ID: 756299
Sample Name: file.exe
Cookbook: default.jbs
Time: 00:13:28
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

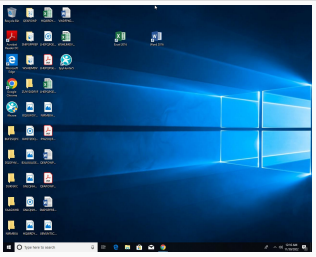
Windows Analysis Report

file.exe

Overview

General Information

Sample Name:	file.exe
Analysis ID:	756299
MD5:	2816bacd01b0d8..
SHA1:	474ae88d9cf093..
SHA256:	637720ba1437fd..
Tags:	exe
Infos:	



Detection

BrowserHistorySpy Tool, Quasar

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	20%

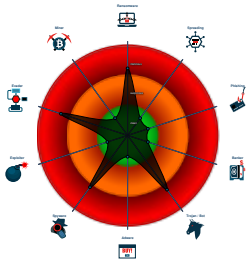
Compliance

Score:	50
Range:	0 - 100

Signatures

- Malicious sample detected (through…
- Yara detected Quasar RAT
- Query firmware table information (lik…
- Changes security center settings (n…
- May drop file containing decryption …
- Writes many files with high entropy
- Yara detected BrowserHistorySpy T…
- Uses 32bit PE files
- Creates files inside the driver directo…
- Queries the volume information (nam…
- Yara signature match
- Drops PE files to the application pro…
- Contains functionality to check if a d…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox

Sample has a GUI, but Joe Sandbox has not found any clickable buttons, likely more UI automation may extend behavior

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")

Process Tree

- **System is w10x64**
- file.exe (PID: 5244 cmdline: C:\Users\user\Desktop\file.exe MD5: 2816BACD01B0D8C48F1D8714C6AA6F0F)
  - sc.exe (PID: 680 cmdline: C:\Windows\System32\sc.exe create EsgShKernel start= demand binPath= "\"C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe\"" DisplayName= "SpyHunter 5 Kernel" MD5: D79784553A9410D15E04766AAAB77CD6)
    - conhost.exe (PID: 5508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 5640 cmdline: C:\Windows\System32\sc.exe description EsgShKernel "SpyHunter 5 Kernel" MD5: D79784553A9410D15E04766AAAB77CD6)
    - conhost.exe (PID: 4080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 5744 cmdline: C:\Windows\System32\sc.exe create ShMonitor start= demand binPath= "\"C:\Program Files\EnigmaSoft\SpyHunter\ShMonitor.exe\"" DisplayName= "SpyHunter 5 Kernel Monitor" MD5: D79784553A9410D15E04766AAAB77CD6)
    - conhost.exe (PID: 5752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 5852 cmdline: C:\Windows\System32\sc.exe description ShMonitor "SpyHunter 5 Kernel Monitor" MD5: D79784553A9410D15E04766AAAB77CD6)
    - conhost.exe (PID: 5784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 1788 cmdline: C:\Windows\System32\sc.exe config ShMonitor start= auto MD5: D79784553A9410D15E04766AAAB77CD6)
    - conhost.exe (PID: 6140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 6020 cmdline: C:\Windows\System32\sc.exe config EsgShKernel start= auto MD5: D79784553A9410D15E04766AAAB77CD6)
    - conhost.exe (PID: 6060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - regsvr32.exe (PID: 2108 cmdline: C:\Windows\System32\regsvr32.exe /s "C:\Program Files\EnigmaSoft\SpyHunter\ShShellExt.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - EsgInstallerDelay__0.exe (PID: 64 cmdline: C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__0.exe -exec OpfXySN2sIJfRn7kaByo3fAgnhU5bFC+1YK5gktB214= -args MHLPvv2eVF5BDDAj57kaKhLIRzVl3TCPBu81sCtfDvA= -wait 300 MD5: EDCE372DE488AA221DA7DB7544C09B3E)
    - conhost.exe (PID: 1332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - sc.exe (PID: 5312 cmdline: C:\Windows\System32\sc.exe start EsgShKernel -tt_on MD5: D79784553A9410D15E04766AAAB77CD6)
  - EsgInstallerDelay__1.exe (PID: 2348 cmdline: C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__1.exe -exec OpfXySN2sIJfRn7kaByo3fAgnhU5bFC+1YK5gktB214= -args hOGTiE/QHFPjrWqL1njGygtJtFEVLgswO/2BlkHQX4U= -wait 300 MD5: EDCE372DE488AA221DA7DB7544C09B3E)

- conhost.exe (PID: 3624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- sc.exe (PID: 5100 cmdline: C:\Windows\System32\sc.exe start ShMonitor MD5: D79784553A9410D15E04766AAAB77CD6)

- svchost.exe (PID: 5288 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1556 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 684 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5540 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1360 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 3384 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 868 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3460 cmdline: c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2080 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 2364 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 2680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ShKernel.exe (PID: 5400 cmdline: C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe MD5: F2F6BF33561C9EF8FE3310D46A3C8A25)
  - SpyHunter5.exe (PID: 5688 cmdline: "C:\Program Files\EnigmaSoft\SpyHunter\SpyHunter5.exe" /hide MD5: 096FA37EA53BB15959E9EEF9FD3F2745)
- ShMonitor.exe (PID: 4792 cmdline: C:\Program Files\EnigmaSoft\SpyHunter\ShMonitor.exe MD5: F9FA9D3B5957F0C365A20DE5C71EC214)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe	MALWARE_Win_EXEPWSH_DLAgent	Detects SystemBC	ditekSHen	• 0xd946f8:$pwsh: powershell • 0xd35b48:$s2: User-Agent: • 0x10069f8:$s4: LdrLoadDll • 0xc35367:$v6: start • 0xc3d08b:$v6: start • 0xc468ae:$v6: start • 0xc468c6:$v6: start • 0xc63dac:$v6: start • 0xc653d0:$v6: start • 0xc6c3d7:$v6: start • 0xc6c417:$v6: start • 0xc6c457:$v6: start • 0xc6ca7c:$v6: start • 0xc6e627:$v6: start • 0xc9b9fc:$v6: start • 0xc9ba30:$v6: start • 0xc9bc43:$v6: start • 0xc9bc72:$v6: start • 0xca2efc:$v6: start • 0xca2f30:$v6: start • 0xca30d9:$v6: start

Memory Dumps

Source	Rule	Description	Author	Strings
0000001C.00000002.583150850.000001D380AA5000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
0000001C.00000003.422519867.000001D3F58C0000.00000004.00000020.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x16da4:$x1: AsyncRAT • 0x1af72:$x1: AsyncRAT
0000001C.00000003.422727533.000001D3F4225000.00000004.00000020.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x16d24:$x1: AsyncRAT • 0x1aef2:$x1: AsyncRAT
0000001C.00000003.422306773.000001D3F5841000.00000004.00000020.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x15d2c:$x1: AsyncRAT • 0x19efa:$x1: AsyncRAT
0000001C.00000003.478164990.000001D3F34BE000.00000004.00000020.00020000.00000000.sdmp	MALWARE_Win_AsyncRAT	Detects AsyncRAT	ditekSHen	• 0x435f7:$x1: AsyncRAT • 0x4372c:$x1: AsyncRAT • 0x43786:$x1: AsyncRAT • 0x437fb:$x1: AsyncRAT

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Yara detected Quasar RAT

Compliance

Uses 32bit PE files

Creates license or readme file

Creates a directory in C:\Program Files

Creates install or setup log file

PE / OLE file has a valid certificate

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

Binary contains paths to debug symbols

E-Banking Fraud

Yara detected Quasar RAT

Spam, unwanted Advertisements and Ransom Demands

May drop file containing decryption instructions (likely related to ransomware)

Writes many files with high entropy

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information

Yara detected Quasar RAT

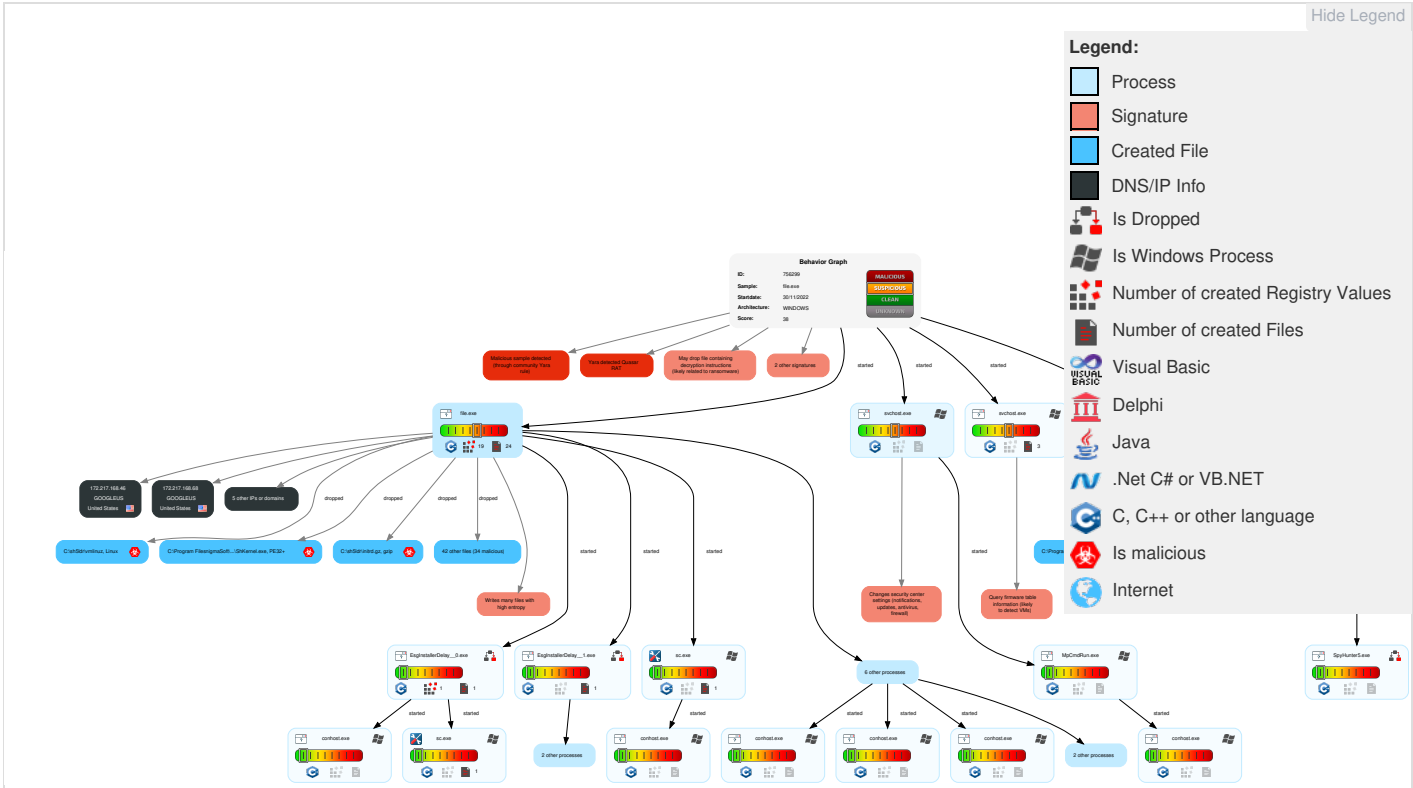
Yara detected BrowserHistorySpy Tool by SecurityXploded

Yara detected Quasar RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	2 1 Windows Service	2 1 Windows Service	3 3 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 Process Injection	1 Disable or Modify Tools	LSASS Memory	1 6 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Service Execution	1 LSASS Driver	1 Registry Run Keys / Startup Folder	1 Modify Registry	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Native API	1 DLL Side-Loading	1 LSASS Driver	1 4 1 Virtualization/Sandbox Evasion	NTDS	1 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 DLL Side-Loading	1 Process Injection	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	3 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Regsvr32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

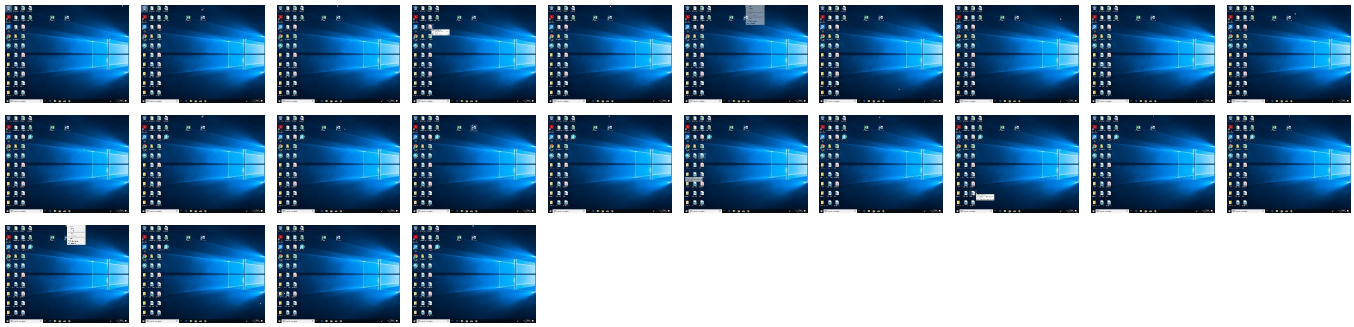
Behavior Graph



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
file.exe	0%	ReversingLabs		
file.exe	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe	2%	ReversingLabs		
C:\Program Files\EnigmaSoft\SpyHunter\ShMonitor.exe	0%	ReversingLabs		
C:\Program Files\EnigmaSoft\SpyHunter\ShShellExt.dll	0%	ReversingLabs		
C:\Program Files\EnigmaSoft\SpyHunter\SpyHunter5.exe	0%	ReversingLabs		
C:\ProgramData\EnigmaSoft Limited\sh5_installer.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__0.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__1.exe	0%	ReversingLabs		
C:\Windows\System32\drivers\EnigmaFileMonDriver.sys	0%	ReversingLabs		
C:\sh5ldr\shldr	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dynamic.t	0%	URL Reputation	safe	
http://installer.enigmas	0%	Avira URL Cloud	safe	
http://https://installer.enigmasB	0%	Avira URL Cloud	safe	
http://wwwigmasoftware.com	0%	Avira URL Cloud	safe	
http://https://api.enigmasoft.nethttps://www.enigmasoftware.comhttps://clicktoverify.truste.com/pvr.php?pag	0%	Avira URL Cloud	safe	
http://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	
http://www.bulla.com	0%	Avira URL Cloud	safe	
http://https://installer.enigmas	0%	Avira URL Cloud	safe	
http://svc-stats.linkury.com/StateStatisticsService.svc/V1/JSON/GetDistributorIdFromNameHttpGet?dist	0%	Avira URL Cloud	safe	
http://https://api.release.cyclonis.net/v1/download?app=cyclonis-backup&os=win	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x64_spyhunter5.exe.ecf)	file.exe, 00000000.00000003.266226833.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268132894.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269928248.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272579170.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267616025.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265041066.0000000004522000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// installer.enigmasoftware.com/sh5/5.13.15.81/sh5_finnish.lng.ecf	file.exe, 00000000.00000003.265023125.00 0000000451A000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.264992574.0000000004509000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.00000000 03558000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.2 67159645.000000000451A000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.265257837.00000000044DE0 00.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000 004519000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 269908904.000000000451A000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.266159498.00000000044E2 000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.000000 0004512000.00000004.00000800.00020000.00 000000.sdmp, file.exe, 00000000.00000003 .266212207.0000000004512000.00000004.000 00800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.000000000451 2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.00000 0000450E000.00000004.00000800.00020000.0 0000000.sdmp, file.exe, 00000000.0000000 3.272560486.000000000451A000.00000004.00 000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265599957.00000000045 0A000.00000004.00000800.00020000.0000000 0.sdmp, file.exe, 00000000.00000003.2681 23380.0000000004518000.00000004.00000800 .00020000.00000000.sdmp, file.exe, 00000 000.00000003.264908780.00000000044ED000. 00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004 517000.00000004.00000800.00020000.000000 00.sdmp, file.exe, 00000000.00000003.265 475931.0000000004509000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http://installer.enigmas	file.exe, 00000000.00000003.265599957.00 0000000450A000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.265475931.0000000004509000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/M	file.exe, 00000000.00000003.267336044.00 00000003525000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.268446523.0000000003528000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268767018.00000000 03528000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.2 70284496.0000000003528000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.268202726.0000000003525000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x64_shmonitor.exe.ecfR	file.exe, 00000000.00000003.268892636.00 00000003513000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http:// https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000005.00000003.309685110 .0000027493E4A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 5.00000002.310476889.0000027493E4C000.00 000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// installer.enigmasoftware.com/sh5/5.13.15.81/sh5_albanian.lng.ecf	file.exe, 00000000.00000003.265023125.00 0000000451A000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.264992574.0000000004509000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000 0451A000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.2 65257837.00000000044DE000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.268295268.0000000045190 00.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266645467.0000000 0044DE000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 269908904.000000000451A000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.267146694.0000000004512 000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.000000 0004512000.00000004.00000800.00020000.00 000000.sdmp, file.exe, 00000000.00000003 .266637598.0000000004512000.00000004.000 00800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450 E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000 0000451A000.00000004.00000800.00020000.0 0000000.sdmp, file.exe, 00000000.0000000 3.265599957.000000000450A000.00000004.00 000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.00000000045 18000.00000004.00000800.00020000.0000000 0.sdmp, file.exe, 00000000.00000003.2655 68181.00000000044DC000.00000004.00000800 .00020000.00000000.sdmp, file.exe, 00000 000.00000003.264908780.00000000044ED000. 00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004 517000.00000004.00000800.00020000.000000 00.sdmp, file.exe, 00000000.00000003.265 475931.0000000004509000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http:// https://purchase.enigmasoftware.com/purchase_spyhunter.php?sid=lav&dc=H2O75	file.exe, file.exe, 00000000.00000003.270258927.00 00000003513000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.269836633.0000000004509000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000 035A6000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.2 68839321.00000000034E4000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.307403176.00000000035A60 00.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.262470538.0000000 0034E3000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 263265975.00000000034E4000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.269812711.00000000044ED 000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270196143.000000 00034E4000.00000004.00000800.00020000.00 000000.sdmp, file.exe, 00000000.00000003 .270153315.00000000035A6000.00000004.000 00800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269586761.000000000455 5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263831490.00000 000034E4000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http:// https://tt.web.enigmasoftware.com/analytics_all/callback_functions/tt_callback.php10-100enigmasoftwa	file.exe, 00000000.00000003.299655855.00 0000000883E000.00000004.00000800.0002000 0.00000000.sdmp, ShKernel.exe, 0000001C. 00000000.400479129.00007FF7094BE000.0000 0002.00000001.01000000.0000000C.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_indonesian.lng.ecf	file.exe, 00000000.00000003.270196143.000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_greek.lng.ecf	file.exe, 00000000.00000003.265023125.0000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/def/2022110703.def.ecf	file.exe, 00000000.00000003.268109273.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_acpdata.dat.ecf6	file.exe, 00000000.00000003.268508936.000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307403176.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270153315.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265217559.00000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_french.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.00000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://wwwigmasoftware.com	file.exe, 00000000.00000003.268360683.000000000045A8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_portuguese_(brazil).lng.ecf	file.exe, 00000000.00000003.267336044.00000000003525000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268446523.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268767018.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270284496.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268202726.0000000003525000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://installer.enigmasB	file.exe, 00000000.00000003.272462882.000000044D9000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269795946.00000000044E5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268644221.00000000044E5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267107205.00000000044E5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_japanese.lng.ecf	file.exe, 00000000.00000003.270196143.000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x86_spyhunter5.exe.ecfD	file.exe, 00000000.00000003.266226833.00000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268132894.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269928248.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272579170.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267616025.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265041066.0000000004522000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// installer.enigmasoftware.com/sh5/5.13.15.81/sh5_acpdata.dat.ecf--	file.exe, 00000000.00000003.265217559.000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_korean.lng.ecf	file.exe, 00000000.00000003.269836633.00000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.0000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268589198.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268109273.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_slovene.lng.ecf	file.exe, 00000000.00000003.268508936.000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.000000000450900.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.000000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307403176.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.000000000451200.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.000000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_finnish.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.0000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265599957.000000000450A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://installer.enigmasoftware.com/sh5/def/latest_def.ecf	file.exe, 00000000.00000003.268508936.000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267137010.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267589014.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265545201.00000000044D3000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268810091.00000000044D5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265243613.00000000035BA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268589198.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268109273.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// installer.enigmasoftware.com/sh5/def.pro/2022080401.def.ecfG	file.exe, 00000000.00000003.268508936.000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307403176.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270153315.00000000035A6000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x86_native.exe.ecf	file.exe, 00000000.00000003.270258927.00000000003513000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268892636.00000003513000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/	file.exe, 00000000.00000003.268508936.000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267336044.0000000003525000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266193979.0000000004501000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268574609.00000000044F2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268091368.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265545201.00000000044D3000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269812711.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268446523.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268810091.00000000044D5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265243613.00000000035BA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272484826.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268767018.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270284496.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268202726.0000000003525000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/shos5/3.18.5/sh5_initrd.gz.ecf.ecf	file.exe, 00000000.00000003.268508936.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307403176.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270153315.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265217559.00000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000005.00000002.310323507.0000027493E2A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_danish.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.0000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.0000000 3.265599957.000000000450A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_slovene.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_chinese_(traditional).lng.ecfDVD	file.exe, 00000000.00000003.267336044.00000000003525000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268446523.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268767018.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270284496.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268202726.0000000003525000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.enigmasoftware.com/support/	file.exe, 00000000.00000003.264261988.00000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307366859.0000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268147686.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263265975.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267393329.0000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270034914.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263198322.0000000003599000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263474019.0000000034F7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263425100.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263666920.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266458249.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263392414.0000000003599000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263138415.000000000355D000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_albanian.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268839321.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266645467.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270196143.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265599957.000000000450A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265568181.00000000044DC000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x64_native.exe.ecf	file.exe, 00000000.00000003.270258927.000000003513000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268892636.000000003513000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.rootca1.amazontrust.com0:	file.exe, 00000000.00000003.263224740.000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.260864313.00000000034E9000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.260814598.00000000034E3000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263633202.0000000003548000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000005.00000003.309542538.0000027493E62000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_portuguese_(brazil).lng.ecfQsTb	file.exe, 00000000.00000003.267336044.000000003525000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268446523.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268767018.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270284496.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268202726.000000000352500.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.enigmasoft.nethttps://www.enigmasoftware.comhttps://clicktoverify.truste.com/pvr.php?pag	file.exe, 00000000.00000003.299655855.000000000883E000.00000004.00000800.00020000.00000000.sdmp, ShKernel.exe, 0000001C.00000000.400479129.00007FF7094BE000.00000002.00000001.01000000.0000000C.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x86_shshellext.dll.ecf	file.exe, 00000000.00000003.266226833.00000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269836633.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268132894.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269928248.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272579170.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266645467.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267616025.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265041066.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.entrust.net/CRL/net1.crl0	file.exe, 00000000.00000003.263224740.00000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.260864313.00000000034E9000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.260814598.00000000034E3000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263831490.00000000034E4000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_croatian.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268839321.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270196143.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265599957.000000000450A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.0000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x64_shkernel.exe.ecf	file.exe, 00000000.00000003.268892636.00000000003513000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268589198.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268109273.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_romanian.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.00000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000005.00000002.310494665.0000027493E50000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x86_spyhunter5.exe.ecf	file.exe, 00000000.00000003.266226833.00000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269836633.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268132894.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269928248.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272579170.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266645467.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267616025.0000000004522000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268892636.0000000003513000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265041066.0000000004522000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/shos5/3.18.5/sh5_shldr.mbr.ecfecf7O	file.exe, 00000000.00000003.268508936.000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307403176.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.0000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270153315.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265217559.00000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000005.00000003.309542538.0000027493E62000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_hungarian.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268839321.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270196143.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.0000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_lithuanian.lng.ecf	file.exe, 00000000.00000003.270196143.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.0000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268589198.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268109273.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_croatian.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265599957.000000000450A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_turkish.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://purchase.enigmasoftware.com	file.exe, 00000000.00000003.269556765.000000045EA000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://purchase.enigmasoftware.com/purchase_spyhunter.php?sid=lav&dc=H2O750x01xDa	file.exe, 00000000.00000003.268839321.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.262470538.00000000034E3000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263265975.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270196143.00000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263831490.00000000034E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/def/latest_def.ecf	file.exe, 00000000.00000003.268508936.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267137010.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267589014.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265545201.00000000044D3000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268810091.00000000044D5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265243613.00000000035BA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000005.00000003.309685110.0000027493E4A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000005.00000002.310476889.0000027493E4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000005.00000003.309685110.0000027493E4A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/latest.ecfH	file.exe, 00000000.00000003.263798085.00000000003539000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_acpwl.dat.ecf/msv0t8	file.exe, 00000000.00000003.265217559.000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_norwegian.lng.ecf	file.exe, 00000000.00000003.268892636.00000000003513000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268589198.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268109273.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://myaccount.enigmasoftware.com/forgot-password/85000.0doc	file.exe, 00000000.00000003.299655855.00000000883E000.00000004.00000800.00020000.00000000.sdmp, ShKernel.exe, 0000001C.00000000.400479129.00007FF7094BE000.00000002.00000001.01000000.0000000C.sdmp	false		high
http://www.bulla.com	ShKernel.exe, 0000001C.00000002.555272712.000001D3807E6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/def.pro/20220 80401.def.ecf	file.exe, 00000000.00000003.272484826.00 000000044ED000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.268177522.00000000035A6000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307522072.00000000 03527000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.2 68767018.0000000003528000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.270284496.0000000035280 00.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272829020.0000000 003527000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 270153315.00000000035A6000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.268202726.0000000003525 000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000005.00000003.309542538 .0000027493E62000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// installer.enigmasoftware.com/sh5/5.13.15.81/sh5_czec h.lng.ecf	file.exe, 00000000.00000003.265023125.00 0000000451A000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.264992574.0000000004509000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000 0451A000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.2 65257837.00000000044DE000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.0000000 00451A000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 266159498.00000000044E2000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.267146694.0000000004512 000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.000000 0004512000.00000004.00000800.00020000.00 000000.sdmp, file.exe, 00000000.00000003 .266637598.0000000004512000.00000004.000 00800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450 E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000 0000451A000.00000004.00000800.00020000.0 0000000.sdmp, file.exe, 00000000.0000000 3.265599957.000000000450A000.00000004.00 000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.00000000045 18000.00000004.00000800.00020000.0000000 0.sdmp, file.exe, 00000000.00000003.2649 08780.00000000044ED000.00000004.00000800 .00020000.00000000.sdmp, file.exe, 00000 000.00000003.266599407.0000000004517000. 00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004 509000.00000004.00000800.00020000.000000 00.sdmp	false		high
http://https://installer.enigmas	file.exe, 00000000.00000003.267369004.00 00000003544000.00000004.00000800.0002000 0.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.enigmasoftware.com/enigmasoft-discount-terms/.	file.exe, 00000000.00000003.264261988.00000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307366859.00000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268147686.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263165543.000000003573000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267393329.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270034914.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263198322.000000000359900.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263425100.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263666920.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266458249.000000000358000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263392414.000000003599000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263138415.000000000355D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.enigmasoftware.com/program-uninstall-steps/.	file.exe, 00000000.00000003.263392414.000000003599000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_romanian.lng.ecf	file.exe, 00000000.00000003.265023125.0000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.00000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_russian.lng.ecf	file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.00000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_portuguese_(portugal).lng.ecf29t	file.exe, 00000000.00000003.267336044.000000003525000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268446523.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268767018.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270284496.0000000003528000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268202726.000000000352500.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/shos5/3.18.5/sh5_vmlinuz.ecf:	file.exe, 00000000.00000003.265217559.000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_french.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.00000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265599957.000000000450A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.release.cyclonis.net/v1/download?app=cyclonis-backup&os=win	ShKernel.exe, 0000001C.00000002.546229449.000001D380054000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_sloven	file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 00000005.00000003.286489874.0000027493E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000005.00000003.286489874.0000027493E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/log_collect.cfgH	file.exe, 00000000.00000003.262458403.00000000003513000.00000004.00000800.00020000.00000000.sdmp	false		high
http://svc-stats.linkury.com/StateStatisticsService.svc/V1/JSON/GetDistributorIdFromNameHttpGet?dist	ShKernel.exe, 0000001C.00000002.555272712.000001D3807E6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.enigmasoftware.com/spyhunter5-special-promotion-terms/	ShKernel.exe, 0000001C.00000002.546229449.000001D380054000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_croatian.lng.ecfiEp	file.exe, 00000000.00000003.268839321.000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270196143.00000000034E4000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_spanish.lng.ecf	file.exe, 00000000.00000003.265023125.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.enigmasoftware.com/sh/license.txt.	file.exe, 00000000.00000003.264261988.00000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307366859.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268147686.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263165543.0000000003573000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267393329.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270034914.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263198322.0000000003599000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263425100.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263666920.000000000355B000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266458249.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.263392414.000000003599000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_swedish.lng.ecfg	file.exe, 00000000.00000003.268508936.000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.000000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307403176.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270153315.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265217559.00000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://installer.enigmasoftware.com/shos5/3.18.5/sh5_vmlinuz.ecffdiyHxtN/	file.exe, 00000000.00000003.268508936.000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307403176.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.270153315.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265217559.000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_chinese_(traditional).lng.ecf	file.exe, 00000000.00000003.265023125.0000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.00000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265599957.000000000450A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high

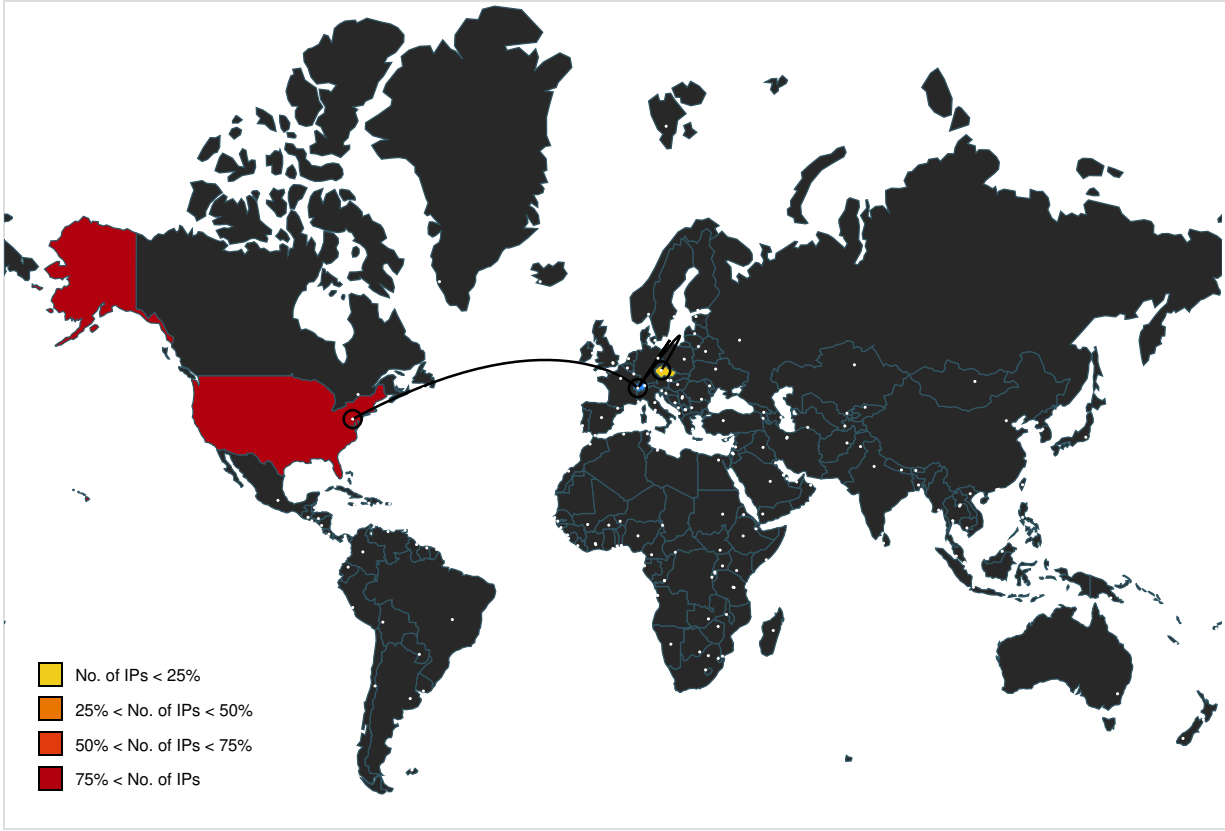
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x86_spyhunter5.exe.ecf	file.exe, 00000000.00000003.269836633.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266645467.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.00000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268589198.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268109273.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.enigmasoftware.com/spyhunter-eula/.	file.exe, 00000000.00000003.263138415.0000000355D000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_acpdata.dat.ecf	file.exe, 00000000.00000003.268508936.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269836633.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265023125.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264992574.0000000004509000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.0000000003558000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267159645.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268295268.0000000004519000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266645467.00000000044DE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269908904.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.307403176.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.00000000044E2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267146694.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.0000000004512000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/	file.exe, 00000000.00000003.268508936.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.267477230.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266193979.0000000004501000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268739494.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268574609.00000000044F2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268091368.0000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265545201.00000000044D3000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269812711.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.00000000035A6000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268810091.00000000044D5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265243613.00000000035BA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272484826.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268177522.00000000035A6000.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_acpwl.dat.ecf1c6	file.exe, 00000000.00000003.265217559.00000000035AC000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.enigmasoftware.com/spyhunter-remover-details/#windows	file.exe, 00000000.00000003.299655855.000000000883E000.00000004.00000800.00020000.00000000.sdmp, ShKernel.exe, 0000001C.00000000.400479129.00007FF7094BE000.00000002.00000001.01000000.0000000C.sdmp, ShKernel.exe, 0000001C.00000002.546229449.000001D380054000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000005.00000002.310439985.0000027493E3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_acpdata.dat.ecf	file.exe, 00000000.00000003.264908780.000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_bulgarian.lng.ecf	file.exe, 00000000.00000003.270196143.000000034E4000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.000000000450E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272560486.000000000451A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265599957.000000000450A000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268123380.0000000004518000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266599407.0000000004517000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265475931.0000000004509000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_x86_shmonitor.exe.ecfR	file.exe, 00000000.00000003.270258927.000000003513000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268892636.0000000003513000.00000004.00000800.00020000.00000000.sdmp	false		high
http://installer.enigmasoftware.com/sh5/def.pro/2022080401.def.ecfp	file.exe, 00000000.00000003.268574609.000000044F2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.268091368.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.269812711.00000000044ED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.272484826.00000000044ED000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000005.00000003.309771847.0000027493E46000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000005.00000003.309723338.0000027493E41000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://installer.enigmasoftware.com/sh5/5.13.15.81/sh5_hungarian.lng.ecf	file.exe, 00000000.00000003.265023125.00 0000000451A000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.264992574.0000000004509000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265090679.00000000 03558000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.2 67159645.000000000451A000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.268839321.00000000034E40 00.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265257837.0000000 0044DE000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 268295268.0000000004519000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.269908904.000000000451A 000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266159498.000000 00044E2000.00000004.00000800.00020000.00 000000.sdmp, file.exe, 00000000.00000003 .267146694.0000000004512000.00000004.000 00800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266212207.000000000451 2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266637598.00000 00004512000.00000004.00000800.00020000.0 0000000.sdmp, file.exe, 00000000.0000000 3.270196143.00000000034E4000.00000004.00 000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265054562.00000000045 0E000.00000004.00000800.00020000.0000000 0.sdmp, file.exe, 00000000.00000003.2725 60486.000000000451A000.00000004.00000800 .00020000.00000000.sdmp, file.exe, 00000 000.00000003.268123380.0000000004518000. 00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.264908780.0000000004 4ED000.00000004.00000800.00020000.000000 00.sdmp, file.exe, 00000000.00000003.266 599407.0000000004517000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http:// installer.enigmasoftware.com/sh5/5.13.15.81/sh5_slovene.lng.ecfPAt	file.exe, 00000000.00000003.268508936.00 000000035A6000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.267477230.00000000035A6000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.273074439.00000000 035A6000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.2 68739494.00000000035A6000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.307403176.00000000035A60 00.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.266526363.0000000 0035A6000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 268177522.00000000035A6000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.270153315.00000000035A6 000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.265217559.000000 00035AC000.00000004.00000800.00020000.00 000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
172.217.168.68	unknown	United States		15169	GOOGLEUS	false
172.217.168.46	unknown	United States		15169	GOOGLEUS	false
34.240.252.91	unknown	United States		16509	AMAZON-02US	false
89.187.165.194	unknown	Czech Republic		60068	CDN77GB	false
108.156.60.5	unknown	United States		16509	AMAZON-02US	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756299
Start date and time:	2022-11-30 00:13:28 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
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:	SUS
Classification:	sus38.rans.troj.spyw.evad.winEXE@46/58@0/7
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 92.6%) • Quality average: 69.1% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Execution Graph export aborted for target file.exe, PID 5244 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKey calls found.
- 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:15:30	API Interceptor	1x Sleep call for process: EsgInstallerDelay__1.exe modified
00:15:30	API Interceptor	1x Sleep call for process: EsgInstallerDelay__0.exe modified
00:15:47	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\EnigmaSoft\SpyHunter\Defs\Rh\full.dat

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	61376
Entropy (8bit):	**7.99721527656712**
Encrypted:	**true**
SSDEEP:	1536:oGRxST1xi3yoeuedpBKgmS0ITGUTdZWz4Hae4:jSTvineonITvT7Wzte4
MD5:	A23943F49D9212F92A2444941A00870B
SHA1:	8E2C8C6A4039A4A83D9294721043E842A48E7893
SHA-256:	3316093484F7F93128B03E4671EAE32B077A022386958E113C329ECEDC3FF3C8
SHA-512:	70B3E388DB46A0430734C783F4248B11E1E86F56AF9F2F4BF3FA288BFCA49AA2EFAE6B9AE297907CCFFBDD1D4117DDF13AF4F89C669C0AFF4CC9C6DF4324C2D
Malicious:	**true**
Preview:	..%.2Z....;r.).1.>3.....Y.....t..r{DRP.....I.)N...J..~.2$....e7L.kW.sOx.....55.>-<!...:...@.(..7.K{..0..$>Ht.e.P8.N(m.z...b3.....,....|MH.:.....r.."Oo....~.9.|...y...S~o...8{fDp....H.u.I.j.....'./.....9J....M...-6.qu.d.n..m.....U....E...:w..@.|.I^.....iH..<.B&)5....#.p.w@...Rc.....%b/f...uDK"....SL.....]..'$.I..e.k=H8.fu.-...d.[..`.r*=...*JAMwC....Zs..,c.aT.4.j.../.."...4-{3._;}2...g2.j."..S...?.A...c...U...]....H.....Nu..>.\O.{.J..P...W.dbz..Z..o.s.....x.._p..W.]...9.>$..._9K.=cXS...n....18.k...h.3....ikS(x.....^fw..(.'J..c .[1T8H..(.0.T.<.....Y.....NF..J.#...lb..r...?..+..S..eS.~..F..k.7,..7..6.".R.V,....;.la./.o....x.g.A..p/RK.....85.p.u.j>..}..x.X.]...5...#$.`...;Bm#.A..`1R....#=...../k.7.yv.#."..M#&...[.w*c.....}p7\...Z<.....'.E...ju.:..S.6.{.D...g]g.E..deR_u;....R..&..^....;....;...G=w...C..b.X.k...n?..kU...EE..&s....rG/ .....t.+...../q..Y..L".B.}&5N._...TNm...j..*.@g....S..$./U...J.].].h>.X.

C:\Program Files\EnigmaSoft\SpyHunter\Defs\full.def

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	1048576
Entropy (8bit):	**7.999801502191134**
Encrypted:	**true**
SSDEEP:	24576:2lmosBfrRo4tk4wUJvBV2nfyI0RCwQWMLR6LdnEWA:GmosBfrRdwUJv72nfK5QWM9sdE3
MD5:	2303D457188A51F3B4489FDA4A2FF611
SHA1:	1D533E082AC8A75417484D94CEF1427A0B91EA37
SHA-256:	ECC9D5C17BBED89660FD22552D51405CB4FDC81C060D026495C3D3EAFFEE8FCD
SHA-512:	31EC5900E2465C0979C229C6ACA7CC3E0AC3D9663FF4040099EB6EEE0C7D4AC0F5A49CEB381E3106DA7E6259A24D0DEC649BA988B64A2078FFB7664952EEC20C
Malicious:	**true**
Preview:	.....x.....4.B.6W.=...t.....,}5;$+j...}K.....,.0Z....4..o8...Qr.Z..'....3x....6.8I..T.d..Y.S..5...V\|..*wXM..p...u..foQ...1..g..rlS+~w.t....nP...M>a...;o7..\....*.....+ .)....s...R.W...n.Z..J..K.,.dG..3#.....F....+K....$..W.....a..e..R...]..."-.PC\P.>L5.v...7.p<eKM.3..LjmiLi@{,..L=.6^.vM..A.@..P.....k..6..E.=.8...Ye.....>...jWA!...z.....%..)Y.P<]H]..^.....8.(.....".Jn|]..+.....VS...f2.....~.GV.I"C)....Hme..M.5F.G.0....{s.&4$.K.X.IX../y.....8k.....e.:...u;/.....:.3m.*....~..'}....+.\|..:....0p.O~h.3....J...3.{m.8I.nH...a.....a-.....L....$...;.@..NQ.....Xv.Q..4../.....:.F.]".Y...B....3....g...._...N.3...].!d.....Qd2P$(b..3.S.o7....H.\1..3...j....2>.'.Et.E.og..<.....n/.'.....t.7.....2S....y.Q*4U...1F..e.p.%7.....?...z .dVpzGU.J;q.....U>jN_...[Y.B..!.5Hw...im.....q..P..%..O5[.1..j..x6.i....mr...o.....Zne.L.Y4...PE...B..~...U75....W..=Q...-..`.o....f.F.....J....`..';x....H.....wS..a....l.d....i

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Albanian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	50848
Entropy (8bit):	**7.995819494658591**
Encrypted:	**true**
SSDEEP:	1536:6Tng6NVUAhysyLo8oo4kDemCWBvLw8+7K5dzO:6Tng6fRhyswo8h4kDemCX8SKba
MD5:	976CB008B4902CA8F7B0FAFD67CC8D7F
SHA1:	B7FB11F06C534EA450EAB52B20B18565211282BE
SHA-256:	C5060390FEBD5CC803490444E7AECCE91E837CCD4ED257BA6CF8F9063450972F
SHA-512:	FD177E34D0C2F8FD5E45674C78F662F62EB7ED471F3E73C3E520B2E9846AA8E548541AB91978BE4AA150489E1C1ABD34E26AA5B3E8F380F2780C5B1FD8E45DD3
Malicious:	**true**

Preview:	.z...V.....&..4.^.y.WH....$.fm".[.c....W...F...d....(...Y.E.....6.l.....S\.....7.?..?Cm.....}...iu..g.8...qA'{....D.y...~*b..3.....|..PF~.<....n.-.....p.[..#...._.....O.".4"|..:.E>....n.f...#..-.....X.....:.....#....5.?.i.....?.....B..A....qZs.AT.9v...L..X...*>.+..1.o.[..G..].u][.C.....^./^.....@..s.3...CY....|H.Q...!I..J.N...4MC..o.. ...D!.%>a').e...K....[._..b.[..DG.(..pi.,.$C T.....o.....{P]./k*F.W....1.a..EE....V]E..H.....aX....C.....F...E$.[.~..c.,=..]d,.I..W.Z.,!.HN.....L.Q*.d...Z.w...=."u?.Se_Y.M.=9.....t.....c....(.6V...Y..\v3n.2.9D9B....q.3....a .|..7....3....G.M.'~.9.2..wH..1.Fv.G....UXe~3C).....!.,.*.DW....k....$.....;.....R.j.F....b^..k.....@.v...~(.... ..7,xG*...?..rTW.J.5..&....3..6.a._IC.....e./.:3....T..5.#w./.....N_..~..l.. ....lq.[.....u...d.#...N{S..)v.U@... fV.Q*.L.... ..h..DX\;\.8.^..U....6..R...s..ZE8.|.Qx.]|...[9..6..|p.....).'.V.l.h....v(#A...x[.....8.]Dy.....

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Bulgarian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	56704
Entropy (8bit):	**7.9966622028475305**
Encrypted:	**true**
SSDEEP:	1536:ASfranQjTDA8Rs1qUTdAjCwW/L5T84SRa:bosPAes1/aewaLJ8xa
MD5:	6618E83905AE4F765661C05EAB36A4FC
SHA1:	3430296DEC76D4B0B94EC96BE8E9B173E5FC17EE
SHA-256:	D63DA339D437AD9254862F9E9A103272E0B7D61A6B2018512E270791F07551AE
SHA-512:	8389B1324506014BAB8D21276ABEF4DCAE4148F21267238FDD814E764A8BF310F677FE6A2103EC2EB1FBB657154B5A625BBEAA13CDC9DFBCB88535A38B961A0B
Malicious:	**true**
Preview:	....:.p.(..$..f,<.W.....H.<.g|...|..F..Wi.....Co...y..[H.....p../.8g.....U..._.HZ.....7...%w0.N.....i.HY.C.....9...!..Q.....4&.....P].g..IO...bs..9.u."..3m{.....[...w.v.8.).a~. d.....e?y!...d.u....(.....-.bj..=Cz%!..:f..$.:c.w..S./...O.z...e .a.....^:.a...'pS%Y....2B..+))'..;...q..].G.....c...B.(w..6'.Q...3[$.1.`.]=.&.1.%...I..F.a....Q._....v..O..yC.....y3.Py..d3.....gj..Z oe...5EZ.c.~e.....o....#_.j.....%.&.Q.:i8...C.!Uz..^Vo..43..Q7..n.5L...f...d._....O.F.xs.:...4q.Ly,E..`...m.y...\.h.+q.C...z#...U....&..uXR.9.{.k.).k.....#.N.0{.19...)u.....`...,....&@.....=.F.q[-.b.....y..Zo0#f..>..p.6'W}....C#...;...8...`...O@).J)....U.j..|.S.0.Y.'...Z^...x.c.....8...|.!.])....L..1.q...y.....\p.H.Y._.=.....u}K..0 Y....y.}R.[..E... ?..H...t.<...G.B..t<m ....sO..7.@.q..y.....t.E.Q.?..c.^.p...A./R...}..>..Gp.....!.. .....kG.!....8.P(.N..5...#R..m.u.-.3..]$.Q..st)v..Y.L5.k..g.h....b0.R.v_:....c.....1w..

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Chinese (Simplified).lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	44544
Entropy (8bit):	**7.9961564371757055**
Encrypted:	**true**
SSDEEP:	768:08drReUlmrdsecBBjXHOAm2nqkn1ogUKkVc6spAjwZRI3VPjpUIF3oCqSG:71m4jXKk14HPwnC3VLpF3iSG
MD5:	04FCFAA2CAC93ED7A9BE17B254EAA8B7
SHA1:	F7A1DE255EC9639651248095020CEF09ABE883C5
SHA-256:	9A07B678314123FD9750EF745AFD988449AC88B190E358B5658B18A01343DEA4
SHA-512:	CFB2CEF6D9029450A1B5426B6CE28AD858A547DFE5DE7070C1EC9B0EE07E4179D1D14DE5A910B099A30A6ED9C6758CBABFE6E8ADB3BF2BFC3E447889E3B76F8A
Malicious:	**true**
Preview:	[4..n.`.alW.....4..X...A."........g.......G.j..P."$zy'...{.....~Me.y.P...>..k..%...U.g.....<.e@OQo.R....].....".....BGx..Q.l.iI..,..o..(.n...)...P..z.k.Rj.....`Ldx.-...0O....Y..s.S. .xM.1...<..... u.K@....D./.a].....A.1.]@.Lo.,....t...da@'...%.wYj..z.....!$.K4.....jL./:...-..>...~.Z.....|N....M:gI....|H.`.w]. iK.D.....&.o|.2/WXm..J.'...5>.-X}1...et.....LW.m.%<9r.....nn.R..].O ..s.?9.0;u..[.0...z=D..a.|.,!.....g..D.MId..1.%b..O.C..P.m.Ck...5.eJ...X._.,.0....$i.?$...J3vL..;36.<./.p..^...zl..M.v..6l.....3.=.....&....v.....Z.B.'|-1...=.X.r.....w'.B<.\..S|...#.*4.L..#ltYs...C.\.x.8.i<....L.%w.`QIB.G....<^4.gc...V.8...-2.J-.7}...HM;./x<\.B..Q.=.....AT.. !...F.?v...j5-.V.....c.,..4w.....DM..5=.XUJ .*j..#..#o.,....;.h....#.|...f.....4dl..'u..*..dFu...Q.- ....c"T."........+`9.w....f...g.wn...A...W.A.].....Z...>AW.....{...g.....v..4p!:.Cy<..%Dn....K-N.Z.P..|7...'....,...[.M.n%?...I...S.|.~w$t..Pj.y17.6.-..2.}T..>f..R..&....._

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Chinese (Traditional).lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	44960
Entropy (8bit):	**7.996099716929491**
Encrypted:	**true**
SSDEEP:	768:QNsB32GtAfawAkaskx2iJgFQpTxgmPjvXQpy7aSreTcJS+vv1vAOXWQBWfsd:os12yAfT5dg1JhpbPj4w2SreTclv9IOJ
MD5:	0BEF9466525543634O2BE05E41015BBB
SHA1:	93891647EA0CB636541505F9DC045AE8A9D4616C
SHA-256:	EC337520003B26095204172841E21F097C5DFE34C1105097E20E9FA2AB832D5A
SHA-512:	465536C80112FA83235ADF31B8A4E7976030112DC064C4B2681380D962DFD02A16E8BF18F562A60F6F36891060817E29A7323B2E95B834E3C5D0899955521528
Malicious:	**true**
Preview:	.....^.....!..[.\C....>...oo.<.24.~.&..&.?.S..d.c"zI.J.y.....xr.s7....|.....`V..G.....W/.....<...R.8..{..a.....|h.'...4.U..j,..S3|..x5.p..B..7..^.8./@.uL.B,W.....O...g...D..7.X`.....i..... 'fU..GB..i...e..'....`.X&A.@+&..9>6....t....-.".X..b.-...8?u[w.[D/.... ....|.....7..G.....Y...V.T.}.WP.}=...b a.-@X..W}.7u.....N5./.T.>.#N....!.....Y..N.j...!>.xvV!...w.G...tR....U.. ..I.19...?...v...Q9.i.>.8..h\....5..xU.w.9....z.....NifA....~.1..y....z..4.bM..QF..YQ.<.@+..|....]....ziq...-.U...xX.....k....P....$.$!.q....>.n.wQ.....vaZ,.....5;X.*...w.6iO.2....yV.....e. ....;.q..s...Tw.M..F.....561l|c.....iE..Q..I...VA..;O.d.HF<ca.`.x..@..w.!..d....~.f,.pD..H.V...h+.+/d...Z@v\.H..e....2.....L.\...KA.....5..6o....?T4N...x.b.T.p..v..:S..@.D.h3....s.r.8O. E]..H.P.....w`.9,I...De...{.G$.KG.....w.WBwq.g]^.....W.)..gZ...1._..C....6.<T.,...X...].T.5.....g.....#d..I.....s...sH...P4..(..;.m..).Y/X...^..1d=.9Px.@...M`y...cb..k....:....AX.

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Croatian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	OpenPGP Public Key
Category:	dropped
Size (bytes):	49120
Entropy (8bit):	**7.9959514160114304**
Encrypted:	**true**
SSDEEP:	768:BtraZA4guj6hHy/kRqRhiXIWOr4mm36MYwx9AnGytdmtTfew1XQI0NAjNVV8JGCT:Bx42SkqT8IWi4Fvynvtdmx6NAJVVmGCT
MD5:	D36F2FB4D4614620274FB5B6C7B74DBD
SHA1:	C878FBA0B13B820467A3A6DFABBF7685938CCBF1
SHA-256:	4425CC691D8602F9DA0166419D06E945DA46AFC1E7B96573B3AD1FA036816301
SHA-512:	7A0F7343D70E2B6DED9256F5D07501247CB3D48817F081A7EA9303FA4874A8E2B19DB0197C766CD05F0445DBC1C72C929F8451695D64BDA8040078E4E0E9E09
Malicious:	**true**
Preview:	.6.u.O.@.4<.....TCj(.d.k.hb..-..nz..gz[6..G.....H<.@uZ....|..L..,.^`}.e.....{.u...ZEL..y...zg..@.h...w@S.'.2.(..n..C..5C....W4....v...fE...g.Dq.3..~.....:.N-..(*.J.f.\....J(<..j..O.....Z...7.....<S..... W(.T.9X_.....".z....A$.....j.$.6..../L...v..w.2.Mu*?./.e[cf.d.....2x...6z..4....s_"a.?q.p+...o...nr....-.E..M...X...)M... I...l.n.(..).k.X.t.....8.6..t..RA+...*k...Dy...UT...3.!....6.;F..,L.u+...j.d..{.tX..c...|e.6FJb.OI...R.c...pNU../..N...B..={.6..".(s}@.1..iw/r;j....W.Y..U.....e....*.y..x..c.$..K.).y...|.V.y..=..{....6.....{r)t...x.=.5$..o...U].....7.uDE.....\.d.a.,_.....gk.4.9..T...i.f...K...9.+....e2..\..L)Y.....U..blS...\....B.PLOV^.....Yg...G2....h...3.$m.^.|!.s.@.N%.S.w....8[.....E.1.t6g..$...'.....\p.).....t..-]..V.g../E?.`.f...I,> ..@...O.=bh..hR....J.J..F.....{g.N.qz=U..:C.....,.u2'P..B..:y.:..4.Ky...Ty.0>.....3..[.R).v....*.....q.J:?.M...../..z..A..G|.E.x..~0.D>`.....d..t.....&.h..X.4

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Czech.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	51392
Entropy (8bit):	**7.996800787014128**
Encrypted:	**true**
SSDEEP:	1536:p+HtA7Mu2wL/FB99QKYlc7az00MtSHGSS7ot5ZKBP:pZMf2/2c76RG77aKt
MD5:	191C5A8C60F25F69D4F943485B52B787
SHA1:	23827A4424723CA84EBD8AB4F724D8A3F847CD40
SHA-256:	53F153AF1CE3DA8FAEBE4B4D24F50FC460F85438AC4F4DC0BE1BE68B6A9E6BA8
SHA-512:	151B1934F3D1162D5F0111DF4BC8EFD7D34B94C7347AD79AB131FB7986D29BAF0313F8BE3245FEF49F34498A057AD93EA50CD3DCB3483288844D0AB7DD45F428
Malicious:	**true**
Preview:	xlH...<..HgHTb$...`.1.]A@.d..1...a...\r.(.Q.,>....<..w."..dS.....(.<..f..l.....-..1<J..V)..T;(.....<.O..MZ.6..&.....|{....X8..,..Jy.:4..L.2..."..g.gm.GU...Z.k)f.|.,.-...e...c..}Z..b..\....b.V[..7.g.8.$.=/d.....2wO...*.....--.....3W .../.....%.Po..'..s|..:t....A&.`X7.\...>2^.yw.n.....O..%.....G...H.-.....D.(...~olA.L. ..4..g...._..Z....SuK..'.4@.....j".G.^...3.....^.e.Z...p.. ..:,".f8C~.Rb%...).#.....7.....r...q..up.%.+..b9.....z.?.Y-.S...A./...._.L.\...H.S.,... .7i...U.:.....%.:._.'.....6....DJ.....z.`.S...O...?.mD.^|qy@nD.....-.9.\...o..*.{..6.J.=..zj.x.zG..5'....S.....6.o..:..S.G.7^.... ...s.....-.a...@f]...N`.....}E..c.I..H2...Y.|.GD...?...A..L...:...O....."0H.>.....f*...rx..k..q2...x..&.(...tR....B.j...skO.....>sl...7oD..q..qO./QJ....v.VJ....._.en.H...G<`...L.[.....++-..JleJ...s.E.^.....'.....&..*;.)mZh...U.ek.....;.....Qh.&.....fH.^....[.i...kZ..@....

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Danish.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	47136
Entropy (8bit):	**7.99711126287396**
Encrypted:	**true**
SSDEEP:	768:psVmvfwZNnX1uHqX2DXiBwwlT6isbRL9Qiw24aTk2wMcgyON9rexw2oR:WsfwTnqWmQwtNp1bpTiMcTM96CP
MD5:	0985C9DAA23F1700CA990265AE158BC3
SHA1:	C6DA87C9801716989188DFF6F651F01EA3CD5BFF
SHA-256:	C19A7356DD44ADF14C62D253CB88B5E83C11283E7CB57A29FA68AC20F1840EFD
SHA-512:	9F5768270AFA4728B734EB7420A8FF4A82826364A81A53A6DEDDDAB9528EF4DD8748E0C8E0B825AF9F78D3E0EEC99D890FFDCE30B0812F354E0BE2EF5A0FD203
Malicious:	**true**
Preview:	r..We.....>.y.....q6=.E~..i.^..*_}}r,D..x...@Z .OH~.}+WLn6.i...n..'..._.JK..$..E{.7".p..Z.....<....o....9....ULA. .....I.&s..0ZO.AV_..1<..|e..6l...<.-.{.A.q(.09...eg..H...(.....v.WSb&...!a.....{....AK4P.;/.v.h.x.....$.n.w5r.I.....:..^.L0....[..kuM.}iR..D. .2..n...x.c...M..0H...l.lPu...L.F....._q&..pW..$.....&q..h.0<w..q....8..).C...B.t.....L./.....R)RX....c-.lF2\.-..^.g5.n.L.|N\.@>....3....:P.L`...Y'.~...h.!.C.`.Y.N..F.....b....g....@9]...I....gG..e.aW.$X04Ks.@R.!wi..._....`;#1...[9....*pB...1.I:0..._. ....c.Q.<....d*6QoB.<...\.".Qf..S..j...X..Y..2:c.X<.e.>.q....t.7\.y....F.....fB.^.~.\HM7...c....wC....TD83..6..r...PX[V...F.[5.G..F{.6.s..,.Xk..).....j..'..-8..J.[.....S.g..UH.M3.O).1|..F....x..S..l&=.-XC..n.....|e..?....b-.Z..h.c...Q.9..R...{.gfV.o.eaN...^{[7K..y.@.....&|3.....o.....Q>.....m.!.J;.e..D....z...:p[3.u...{I..w`B0..$Q..6.\`u.,xc.0.{.u.,....z....x...q...C....k.jz6..(.2...9![@....U|.....o..."..g!.0J..

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Dutch.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data

Category:	dropped
Size (bytes):	48320
Entropy (8bit):	**7.996230355017293**
Encrypted:	**true**
SSDEEP:	768:dAr9iBSGU9AG6FT6OP348PsKlx72ZN8dOG4DDAIREKMRErUGKJ/:w4BSGU9AG2T6i3dhg8cFD0IR1MR8UGKl
MD5:	7E3368BD8F799DCE730BED0D85BCDC9A
SHA1:	0DFDFE81C81806D9CB5A6BD7913455F4E3A34A9A
SHA-256:	782743FB4BBD79488D1DF851C5A26C01CDE4BEE285B7EB451CF24E063AE723B4
SHA-512:	AC8FDA6F6EF00A15E6371420144EA9F53321493A8F4533ABBEAA9CA24322D9358D81E130EA15C909D687345130F54ADA33BB76BD8C486F2CDF64AD85F475042
Malicious:	**true**
Preview:	.....Uc...#.:.....S..}.~.).E...?/:w<..H.....Tt1$...b..Q.....A1...=.O!.-.1.q..H.W.F.\|v.c9f.gL...~..ZP.@..6..[.>.'..Im.HEAhkh.&.E.).....~..52B...R"...u'...m.H1...,a,5D.E.+&<...$.< ....$...pG..lo...t..z.s..(B=*...._.....2...y.z.>?.....-....Wc.u..p.....pLg2./B>.rS..1.....x.3..,../.4....@.1..p....0e..D^@RM.X....E...k.y.....0..VI...k.S...b.....z.Y...}."I..eG\....{:... .x..*P.q..d..aQ..p.z\|jh=..{.=jU...B@.Se].$.....S>nc.'k./8..9...EY..|..({.....VK..{x.....$.@....._._...L.n..].:K..-..zg.....0z.x.Xov..P15.oW.Kd.R2e0g.X..D.(.>zt..K.z..1.Qz.)..O.F...VPv..q..x5.....V..G..4.....6.."\.....gK%...Z.....v4"+.S{.@./<..\|j.;)4x...r..b.t..[".CB[...z&}u.H...K.3..>>.2..'.....j..t+....v$....2*.T.sCb.NV.....T.Y.D9?9.b.D..sZ"..R.3.Gx.[.... En...xDY..=..j.Wg...a..9ba.?....lu..@R....Us..=#..E0 .K.P.....Mh._..ET'...U.....L.*..^+(.B..:..3..6B.....]....r/;.<...4...`3...%.....l.`m.....Q..$....qes.O..../.y.....*d&a...I....|.-b

C:\Program Files\EnigmaSoft\SpyHunter\Languages\English.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	42784
Entropy (8bit):	**7.995729901452885**
Encrypted:	**true**
SSDEEP:	768:Cv3VkgFj7UnG7+bAkmzx1eWHmVypmUIXOv+4/4t7muef3jOEb:43VbPEG7c5m1RQ1X4mr2b
MD5:	CDC4212F25766779E915F5189862523F
SHA1:	FAF1A8BDCD8F0A460BEF210C7AD72841F6504059
SHA-256:	E2A0515CF459BC2C60D1C849C52ADD6928CEDD0460A1C60E81DFB9966C8A95E0
SHA-512:	D99E0AD932B6E9D2E2881781B3A0B55C67C41C9BD4D184C1B2C29F1F50D1E4D0EE22DCB3F0B9B30CB3D296DE67F5D12D873A9BE729277A6CCB2F87227A488 B2
Malicious:	**true**
Preview:	.E~[.aQ..9k.Q....K....I2.. .>i.(....QBt.o..R.*Y..3.%...P.Z...Gi....."...v.5./....{..c.23.....b.InJ^.C..Oe..w,+..\..|..K.....x.;.....R..#.f.#....Z..vz..ar.....h$....jP=r....q.\|..}j..$.F.9]..$u R.....c.T@.f.....L...k..q44.....<.`.q....t...gc$A....z....7.pVX.y..Be~..I.k.....*.....b.e..F.....% ..6B.k.....P...'$.a3j7.... ...X.[.#6..X...)"r...,"...4..=h6.~.....K.g....cC_...g..... ..h... ..I>.....)..5Bg0..i...;.....d.uS..>W.\|;.;m0E.mO..*.=r.=..^.d\|.^y.&\|...U&.8m.C....;."kAA\.4\4..z.,..*..P..3..f..X.gN.a{..>~Ib...?yVK....K...o.8..z.w1a..2..e...W<^+.e.Fp..&k.8V.\|.... :.....x..7'.s0..<..T..$.6...<.O....hD.K;...I.d.%*a]...#V..rg.....h.5.o..$.....oI...7.&w..i.O..P.....Im.h..t}K$.Y.....`.~.8T....k)I..10`..ss...C.j{...4r.i...k~7Ho.....[...+...N..B..~..(.cd.i..... .@...T=vq.{....8..m..].X~...gj\1@IG...ru:.....O.....W.....#.p.....}.\...MLBP97M.1.x.\...."..O..Q._.....r.....N...8.m..:f..3..S..2..j....?..P{..W.+S.....

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Finnish.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	48512
Entropy (8bit):	**7.996154119133664**
Encrypted:	**true**
SSDEEP:	768:+s+NSaq94nPIAXHyIbHbKKMOxRGUbxAPk/DvKWr3C2TyOf45bWbAvvTat9yHruzq:TXl4AFTmKhGUuPIuWrpya40Avr/GnZi/
MD5:	0B286A1B30CE5C89E2F9300BB8254286
SHA1:	B974D6DFBC5FE1BC89A62AFC86F6DF6948209D54
SHA-256:	610426F80771C20488BEBABA11B69DD0E32B3F7B1CA25EC4714792EE6F48C8F0
SHA-512:	19F56A34676FA176A01917127E7FAA8ABAA20C136B1F120CF0A3855E31D863EDB3CD7287A572E8C78AF2F904C0EBECE906F7BBC04F6D7FFBE833C69DD59A0D 6D
Malicious:	**true**
Preview:	q3..b.o.=_....|...G.....h,.v.>.NT!.w.....L.3....L...T....2.@v4.fu...."..;.....d. .h.....Z...`.X]Z(>>.I}....S.",d..R!.....\..(.;...y.?..q.xo...?K.A.Y.....}.....VC...5?a....4.....,..9.....=...{`.....p.. .!.N...d.y]..sK.+.r.N.r}..qq....G]l.....w{..=.\....u....H.....of.c..Kh'...2...}{.... ...r=.lQ..D.=N....4..!Pt...O...T7.-...b..g.....4t..M....r-.....N.u.t....&(....}0..(...aY..S...r.....F?.I.,H.!..... ...6..0.^W.....=...{..j..E.-/.....z6..6..L:K."A..z....c...uA.:U~[.....!....O..'..f.3...S'..P.n3...9..q.I...O-.....F..,f\..-Y&}Ef..hw..)..8JnS....,....._...(*..V".#...wu....2W7..Ls&....gU{..SifB...- ...yrN5~'...j_..D...d.....=.....Cj.... .v...G...I2M.p....w4...Oa..R...l.W...C.S....j....m.v.....\~.gSe.n.....d...%....A.]9i...C,Q.'.%..I.L...q.6j.u.....m.IQv...u,s.F_I.P.5..r.w.....[. [u$|...h"h.<T.\>X.....a..H.M..v...iH.9...T..b..#.w...?. m.s~.G..\.Q}@.q.(..WG.i..)~.....y?\..X.....[.|.{|...q).{.....r.E!..

C:\Program Files\EnigmaSoft\SpyHunter\Languages\French.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	48224
Entropy (8bit):	**7.9967131332237615**
Encrypted:	**true**

SSDEEP:	768:4mioRiouNLX1LAycAs0i/aNpB+5n1P6Wur90/O96Hv69H9PIQPGfSLlt:Pi4iomXJ3zNpBQmo6N9DG6LX
MD5:	5592FD72F10D4DEA1D0810B2857D8632
SHA1:	4BA8A9BCADF7DFC6B10EAB0F0AD138E5A6C451C6
SHA-256:	516EF58F2C62EB4C2B797586A24869C0A9DFD816E4D80DC79C1DB7E2AA334142
SHA-512:	443C875E496A7A0BCAA87402597F7F69A1196E2D63259E17E8F40589B407039D9762176D2A731B50E26FC4AA99658F0D880459AE19177AF85943C3ABF4A6DF8B
Malicious:	**true**
Preview:	.0.Q...s.n/.x.....:'.:..I.]..@..w0..R\..%3..T.....o.7f#w.....t...m...=.....h....K(I....tTE....L..E..1i...I.....x..hdY.".N....1{..^;....f...G.Y.b.q.+.#s..'..=JN%D.i#2<.....^...J%&vo...O..(.7Q..... j"Ks..{.6Y.8&.'...&^,cl.`.N..N.....aW83...m...*.3...i..n.....Je>.Z.6b.2.x..O...N....I.e.J.G..qK$Y...g.{....i....0.....k...g..hq#<. .k.:....A....I#A?..R.....H.J.k.^...d.0.M.:.....K.xtJl7..7 .@..GoO.....[..*.}.*.TVU3.....j..C..xO{.ST.....3.wnx..e.{a.9w7..n$...7..e.....o...!B4.4...0.).x_...8.?..m.t2S....:...2..t.K..{...2}z...8..P.....2..1Io[.aJ.y..b...H.1.....h...U.\TO... <rw6.)p..L4y....6cs...0.s.N!..P....`.G....^.A.C.C.l9t.... .....!.....c.}.]N.....|F..P....q....._.....u..3.<..6.....&.N.'.w..e&...C...H.}1m..P.F.....;.s.M..h..*.%.`..V/..[.....N.R).]l.`B...<.n S.}xn.6...1n.../.`.....s.#..M..lx.!.....4i..%%,"g.-N.V/..,.....;...{b.9-.....6.Oz..=.!W..=J%...?.F.....D..x.0.KGM.....v..$w.u$.).WY..|cG\

C:\Program Files\EnigmaSoft\SpyHunter\Languages\German.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	49504
Entropy (8bit):	**7.995807513580829**
Encrypted:	**true**
SSDEEP:	768:/Et3lCkAJLjP5t+GavecrMfYAx3jUN4UR+gN8kP1THWt39FA4sXgqpRUcdGHb3m:G3471H5uuZ3oN4eJ8c1jWnEpldArm
MD5:	9FA1C4183C3E9F5849B29483B2685C14
SHA1:	0BE0F1FDE03E1619CA45A014F72779FADE00B804
SHA-256:	BAE08EA9A1C7969161C5CD640266A4D4CFC676DA5F09476A69C2088D0EC62C3B
SHA-512:	0A57DBEA7ED6290C6843C228237991D5A722A8BDBCDC0FE7A93381B16D4265A28C257D8D6C211FD3B7E54B82A0D8985F08C379EBCFF329CCF9D3E930A2009(9
Malicious:	**true**
Preview:	..?#.x.u..D.....Uy#4..(b/.....:.Y..w".d.....K.....Gc.E..GY.$.aH.Biw|....(..We..p.....kqK.X._^..I.Nf.dl..(..Mn-R...a.{.R@...A..lN.pvf.....{..4.H.....p.....L...x..v.B.c.Q..s}:N]D. .....}.1.U..h....'..73.....>Q..L.....i....5..5..p.UJ....D...B.9..{su...)L..q@..\..W...ZM.x^M`v./u.....-.\.O.h...bx.<.e..u..r.B..."...k...4.....).[q..>...NC..5.U.O(..B'.mv|v....mU...dk..I5....C.t H....v".....X.r;;...../.Q.j...U.&'....I...'...ITZ....2E.e.`q...5s.+.....7....4o...*b.>....h6.d....Goq.W.oW...o. mIE.a.....J.M,?.c.`....cH.1aZ...q.[7.....u.W.../.~)2}.k=W.....d..4..H`....9...(... ....)".G<+..JF[....w..b..s.E.-Fz._Q.E^-..hsG.....,.n.Y..m.WI.5.....^d.U..R..0..1.R..e...dj.Y..$....R.....K.;G.....%.g...X.J.....X..../59.i.*..kF}<..jcBv..m|..n.....f...f.!...E6.3;.F..5.I z.jXb...C...Qu.6.S..O..=..nQ.2C.....z.....3..b....y..-.[.....Fn3..pK.....]....|x....n.:@....5.II...S?.3.N..-6.....7..\2..Sy..v.I....zkH...e.9...v'."....

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Greek.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	60096
Entropy (8bit):	**7.997056401458807**
Encrypted:	**true**
SSDEEP:	1536:4NCSRPBRJaHcdxJWn2hF+RHfPrH6KDIk2w08lv5Vy+DQ:8RP0GW2hF+Q0lK+DQ
MD5:	50989BE42BCE3389348A4E9BB0193E77
SHA1:	6F1FE6159CF951D267A6C5714420C45C92FA1A8A
SHA-256:	92E2302F8300B415C33F1EAE6FE51F419FE9411768126C09B216B53EF3208ADF
SHA-512:	ED0BA9FC76FB42A3EE160188419F07942DD0AA44B165A369A49849959AFEA63080B1B571C47D2A95F37575C0F6D72A5B8C061B439EBB9E0A027FA63E6C520D2 1
Malicious:	**true**
Preview:	..cG.x.....w.>...t.V.7:|E.O.E}..`.;y.....s.R..."..'..d.\Mc?.2.+..+p]\..A.A.....%z.W..\.6..R..VGT...x..M..e.....Vm....z...y..Kq.%...-.....a...%.[/..)$..C%.D.W_f.>O.....:.^2.....l .....w.....~..&v.....>a..[*..C.nR..M.....`.']G._?C".....:..l.....B.+.ix...R).]..r,_...Xh"..gE1.I...C. .{.:>]s.}...3...:....F.}.....&$.....".eP.:^../..N....<..l...z@S...C.=d...go].....S-Ik..\.... ..q:.....0.v.g..?....4.m..8..m.T.1.{.l.!..3.x.8.x..dd.z.....U^.;...u.8f...q.9.....L.w9.....t.%6{..H..:).R...?z..z%.....c1...|F...M..m..... .m. ....y`.[..... hd..S..c1p...E:9.T_?.`V.a....9/b. 0..@..-....2.i..v..+...0h.&...(V.....u...;.E.?M.....y.n....bj.&I..C.k6.>....Ob....o.@..ma..o1L....`.ev3.P.....,zLVR.....n..F..}.W.P[..%S.._ ,(.(.....).U'5.-....p9.J.....~U=..Y.x.[..]2.. WEY...L._....P}$.....xFm1..6i.p..i.H.....A}Z....^.x..j..y...o.z\.kd6.3..u...Z..VE..o9.p.#.P.>.3.@.v...9'.~.....zKl...d.8.....}....1..K.L.xk...-._..Z....j..p...

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Hungarian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	51392
Entropy (8bit):	**7.9968985948672096**
Encrypted:	**true**
SSDEEP:	768:gOrpeqUFMgGt03zi+NcYO8VhV1BX8QLpkwhWy6lGbVWEsHwxQaGZ:gOLU2g91Oyz1BX80hAl4l7K
MD5:	E21947E89D81EAA19307098634A1CDA3
SHA1:	990A6AB4CD228298769BE7A6494317F56BCD05DC
SHA-256:	13AF244A480AFCEEF13E6E68D1FD88C3C6640463771B26A01B8EF693F55DB008

SHA-512:	E5D789680077B2C261E9DF1845BAAC9BCFE26BE5A7CA7631DC1438E627277981A2CFBCC056A7A75B9B6B7790347381BCA8EAA39CB2DBDA79DEE954836CA0A464
Malicious:	**true**
Preview:	<.....iB.T2.U..".. .\.p.?-...S{.V..Bg.Qj.....O.N{.vY.....}.$.S.....,{Y1.....8...Ye....y.H.zR^<. ..p._..6.#f~.na...=cz..%.H.=.E^D.._..u.1`).{...z.Y..I.l.4...[.....w .....c.@..R. .1.d..s..Ne.!C%T.[a...C...>....]..o.(..e.....!b..v.H...r.a..y..7....$...*.d.n.IW5...5.....U:..\.....-#.t1O.6|.-}F.G.4.b#...~..#$ X.dQ3vK.J.....r{..=I;8nd.FO.k4..H.t..E..9Z2.\.. .Pg.ZF..._Gva.F..%.~:.;c&.....6r9/..b2E..ui=X.I.PK,...g....."...H.]\..._9.'..z..#FMeT...4.Qu..#.N...7cy.....I.#...iN....8.o....\W..ZiUD.c.g)....p.....C._..(.J*z.I..@.<.-.....z..L4.. (...+...:B....4."Q.$*..3..h..e.....J.*.?.Fg.....s.o.16....%Dk/.....,.....hA,5,..[o.k..`q.9.O.....9.S)6t...a.M....T7.*....u~.~L.D."..;N...1.A..h..)dd..9y..w.3.t.....V./..M.."..5h<?..5... 6YD\.R..r.%gC8s...7.;yiN.3..G@.,U...6.a...W.D.Q.. ..9s.@...a.<pW/.....7.Z...j.C..}\..... ...U.k@:mM)..z..e.h....q.....+.z.OQ.^.)d...(:t.?...RGU.....l.97...p..m_.....

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Indonesian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	45440
Entropy (8bit):	**7.995735152404058**
Encrypted:	**true**
SSDEEP:	768:6J3jbt4FakmnyjdmO2V2CYOsbRhWtE7o4t6t+M9jkCMr5:Y3jhkmyjdzt5lRw4tUjjVQ
MD5:	AFB1C96541A1206C84101DD39633AB07
SHA1:	1B19ED3188A2AE9637165F4B5FF14FA5F97A9111
SHA-256:	37BC59193E038B46894CD3E30D42FA1F941F518FE9EF5CFDB9362B69D1629FC1
SHA-512:	76E1CDBC2741544D8652B659974575AB89BE4D55933BEA54D46F651C611B8F03048897717AA5A5E539FAA1D6E5B725DF6445FFF8C6C5C6B321B87B3378F27D93
Malicious:	**true**
Preview:	.....6...O.....{.jQ....EO..;..bhF*. ...$'.w.-.?.....b.m.u...Ws?...fS...4...c.W&V.....%....}h..."".....%C..L.....==qE.2..O...0<j...3.?..... (.:.../..5< v.O.....V1{.....W}w.EQ_+.<..... `}dF...&.6.V..)#mX.fh..RR.E&=rs7....V.....I...X.)....s..X{.5.....z.....F.....r.b.....GU...]I....P;p.$..1|i...~I.,5T..p.....<5.....E?.2Y..p.R.P&['.c.hRZ.o..b-....d..B.q(.Z..._2.R.p. O..V>Jw.yy..@.....]..9.&u..N..o..YE.3...KM(.]...IQ.....L..8..UE..R.W.....l0..k..o...(.Q.."...}n...@s.x.6.....].....x..R.$ .....,?..._.....:._...(..,....W.h..,O.roFe...=?..,..s.L...Xa ..X.....G^...|.'...nN{..KT...&.-..(....z.|.'.N.d..:....H..#'4.....7..Y.....".CTEB...h.../....tl.f&....R.....t.559a20..p.Hi.N.&..bC....IxH....kM.e.Mxv.u...}.7...N.w.....cDN.....e.....#@.6....9. ...F`h..~... .P..:h....P%SU.p..%#..G..>1C.h....w.P~.Fye.m{.4.d..>..+.....PZ..nA..h*.....!.....<.....<E....k3....n..J...e....a.GI..oZ..w.R..y..~.#.c.i<.$..X]0.....E`@`.....:

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Italian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	48032
Entropy (8bit):	**7.996516407599824**
Encrypted:	**true**
SSDEEP:	768:kHqb6Olqm2afhUwNpJt3Lh1kOYjryiBuCVaOW48dDaaMEc9p97HNod+UMiz0iHpI:kHqeOl3EcbcOgBJaOR8dDaabc3bO+kgz
MD5:	9BABEC3C08A0821FB723C033645FF0F4
SHA1:	8B8F635835FA7C20EC9ACE4079497D46324D4602
SHA-256:	8090349E7F670AC61E1A4FE8DE6FFBCDDEED052314CB32750EE5C954472F7C77
SHA-512:	1DB6FFB564CD0C007E303C0CEE0F02DB7EF9D43AB81544D1C2B136B0B6F3460AE2F7A990290D7CC3908D1CB0E0282BDE6FA512CF14C518C7A6C17A18028B9FA
Malicious:	**true**
Preview:	.6T?].....=.W...;o.l.c{#{.;|)..s.n~/..:...cz6.t|./P...4.-..4....}.BjUoV.H...._2H.<.[.....U..Iq...h.+HF].).z.._..1.....n.#s.|.....m{....`.....LQ.\DJ..>.k.Y..8I.t....Lw.0.=..bq..~...'."...'...)t.uO b+h.i.....]ts|tw.....|bPrX.....*;..%..$L..v.|.3..*:.'gy.._.z5...)n.NU.... U...r.....(.b"y}.C..t,...z5)....(.0..).C..I....E.n.;=...=X..|.9.....|.....o..W0/8.....',W.?;..rr..D.s+./.t.T..7..l...'..8...}.....D ..L...0d.[.....#..%s.}..K.........O@.s...?V...7.f ._.....|.pO~....8:.(I.. ..~K.....5Ry),..|..(.9a..4.w(3._..._...n...x.J..Vf.?i.4'..I1L22.....\-.TX>..x.....|.@.W..?....[I.Jd.....?.{.(.....3d...x 9...`\.-...p.b...p..I...1!.KDN.....:...di..)D...>C.....b,5.....q..L...j..S9/`v..7g.#.%.Q.....#pwkKC..~9....[;.....g....zuLV.)...i0`.@...#...0A&LCMH.&.M.....^'..(Xb.{.`..s'.k ....w7..BUN#6..y.u.....Y^..A\.x....UO).....`.0u.J...1.{.[.U....F.... T.O...0o....a#....s.j0...n.N.....Gy....a..R.@.Y.....L..;....;9..j.P...XG....!

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Japanese.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	50752
Entropy (8bit):	**7.996175639604411**
Encrypted:	**true**
SSDEEP:	1536:jeBnCzg40bF/wWp+JW0PSgMjDUJeKv5qqWRQ:6og4+rAVM3rHQ
MD5:	63740682BD394B8D4D3979C5268C3B7F
SHA1:	7E74D5DA436498C9974A5F70A4100C7975A08529
SHA-256:	3EC5988B0964907BBE6E6110816EE8575F74E13DBA84287B733112EE4654010C
SHA-512:	0A12634F4190FB4F0C6F6D3C837B1FF6F3EAC21AB1765E704D50CDBCE0AD86423529E581457D3C0D391C2F865637B0C59C2DE502D40A7C9500E64AB300D8CA2
Malicious:	**true**

Preview:	7..i.].z&S.....v.4.3...\w.R..x0.6E.N:o...$PB.M.....E...\.Y.\.jJ..<@Y.[F.....S.y>...5..12@....9.;.).`.o2bRa<..s9N....L<O...E.b.s.Q.."U..h-z.{.t.....l.Q$.&..A,..*....P...Yb.=S.*T.... v...R$9.....z.K..,9 .....o?O..;.]...^....{.z...4..-.`..@9.I..>.....Z&..../,-.....].KY.+...|.Q.3p}..N..U.5.....,..h...N.Z.4~.hef#v=.. h..[se.2t....s#V..].|.B.x.fn.;4...D..pqz..'...-....*r,..y... ...7.J..I.8.....j...I...:.y.*0....bF.OS..VpZ..v.&c...2.,.C3k.....@.Y.../.....I..9..$D.;.P.<[h.s4MEG..]=.S*..G....I...V..4.P../..wq...s;..5'x.,.....1:.p.....kdt..*..d...(I..v....Z.I.....K9<2.*. ..o.~.V.do.'R.....^...IK.5.....*..n.D..T..g."8<...+I...3;..C....Qf.C.5".=.4.'..'...._x.7../F..x..O:.....r.........nj.....'....>k.........[.LNN.nX*...Qv. 6%.a..(.....{..x..^.Ih.......)...j#....-.O.^.*...)h..+g.{ ....L.f...M.....I_+.C....m..$....i..:9s.....z.s,..W...zg....$.............i.?..Q.9.d:b.....Om..L.IH..\.<".*.!...4..(m.t,P....:....}&Z....On.5...(H.\D.`...C..2

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Korean.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	OpenPGP Secret Key
Category:	dropped
Size (bytes):	46944
Entropy (8bit):	**7.99693442690835**
Encrypted:	**true**
SSDEEP:	768:wzrYIbPKk6EWhJh49XQo9/BHoRJZ8xSJLG7e4X4d4aSKh0cdtdARp:yrDL6dYN1SdGS4C4aBh0ctAD
MD5:	9B82EDF3F29CD98E20BE6F1F0373083F
SHA1:	795CA4F5A4CC91D59848E0D609D805035AE9EEF7
SHA-256:	1CAB512FB90AB3E6A6F42DFDF648AE7288CA5EF8EB55426C1FA829B292DB55C7
SHA-512:	9770426D8AF8F039FEB5AC949B5F532D816F5CF966536122AF8AEAB832105EA3E90C1A87427808DD1E3E5E7C1FFEFC8E222D427A1D0DB1E667514E1185A71D18
Malicious:	**true**
Preview:	.+..lL.<....%,@\N&....K>..5.,e.H.4....#.p.*..31.8..hp.>..C.]F...b.....$T-M..7.R...=ZEM..P. .q.f..G..*x..`..<j..273.....g..lO..AX.b..X~<.i.....Az.....*#....u..E.b..#-.+....8.....3.:E.e..2. S.s.9.....j@.#G...;[..8J.*..z.c.0..l..(.J.Qr,.60.(..q(...N.)..e..z.y.".q.>.f;.l\.&.E7;z..:hrs...3..=#.....ql9...~.Bs/y....~.....\.h?..Y..my.+.r.KU..I.....a>.....&.y!..M"R$Zb..&v...x....DI...|. ....Z...&..a..p.1}.PF.ga.2V.<.5..t.:.."..uPz3.....=..Z.`..P.:..]L..5../.m.9....Y...U....o...e...qMf....k...{..9q.y.. .a.(~.*YX.-&./...j.....EdQ.P....,.;.;..%... .6.....S>eR.v.....:.$..h..v...m.....N J?.P=B.hJ.,g.....D..%}..0....x;r.....[.u.;.w.sP..g....u.../....,.8.....6..wKr.....d....6.^].^M..._.>.....?..t...p.hKN)[.s...*....a.d...R..*...8m?.(2/#.^d..kdw<.&o...k,3..z.yLA.DH.. .1.n(e....F..._..P..O'~.....(....w.kC..O..G.....M....p..j.+.v...A.....W..r!(....C...1k.|..|..... &3....3n].j.<].z...Kc.d.....8...P"..(.8..b.....0U...2.....C

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Lithuanian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	OpenPGP Public Key
Category:	dropped
Size (bytes):	49856
Entropy (8bit):	**7.996267189250834**
Encrypted:	**true**
SSDEEP:	1536:TLwOaTJnmSTLxnaE7ofsu3kFTQC2TWnjYvXW/abGFM:TLwO4Jn3TLhn2C2TWkvG/8
MD5:	E6A368A35D709E63C7BEA7AC035FEF55
SHA1:	2EBE9159DCF29EADC4CECEB052C78F1E061916E1
SHA-256:	F648CF9D6AB1E7F726CF5822477C09F069C7FF1F5CF752AC03767A896E239478
SHA-512:	D2AA3193A8FE6CB6A7C8053FC615AEF565F0999A147291D3BFD34CADAF85CABACA62787C7D06997DF18402BBD04DB8C95BC6A99164407B5949536160B089F13
Malicious:	**true**
Preview:	......W..D.....A3..u...4..7..<..I.^.....'$.p&'.v=..c.R...Y.T..j.....E9.....~6:.....7.<el...G.)..hO...\Y6b-.3.|N0.@.*)I.....Q.k....u.[.jq;7.c.y.[...3.Lw...P4T....p..H.....b..O.h..E.O.$ t8.....tN.Z<.<.....nF.....h..]...s..)I..%.3.....K..9/#...*..f.V....m@".o..#.....Z`..>.i...a.'.C..2.....Jb~..2...^....u...aC...-.H...d....g1W.=.+../....[.).@..[.!..k<.f.%.FKI...VI.... .t.?.?..J..-.h....F....q.s..<....|+.=L.7..n..HL..S.*.r./....H.5&T.....%5.).....b.xq@I.E(//...yX..x..&....}...n=..T.....J.q.#ko=\ .$...3o.[.q.3..^....gq`..t..I.P...1.qO.....*.F\&.9.C..-.. ..c.M?#'...h.....v..M,.&.....C..x.GU..%....j.2.}?..I./..z.{...$Z%.^.Zj..G!..*.d.;.J.V.7.bN.75.~p...Dg.....>...{..F*...*....#f.....pNi;$8d7.h.....EmAQ.....ne..Y2.K>..%....&n.*..c."Q...,.. (p.a;..+;.. .Du+....I..w../'..I.ssb...(TG....%..(..G..0)7.|Wk.-F..X.:...).?...Z....E...rM_....eWe...^~.....m.....g.K~..`..DW..6%Q"...R....Y.A...

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Norwegian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	45984
Entropy (8bit):	**7.996909164261379**
Encrypted:	**true**
SSDEEP:	768:QdNA/Y1o3lc2skDufiksq1EOv/spccjTl8HYGR0Pv3T5yyet+rd060ydi0OGuEiW:mAg1o3l3DOiW1EOnsycjTl8HFqA66VyX
MD5:	58437B307A946DE05E7D5CF7EF06A134
SHA1:	C93C8397F08976F6D741741F3B9C7F50946CC1B3
SHA-256:	49EF1BF1188AAFDBAB8BA546113B4C5792016386077047CC16BCC30534CE362C
SHA-512:	188D27AF0C86466DBCAF797C92F46C9281A91910384EF061BB8F4AB89062E567489EDAA8FB7C0C06B5B0FD331FEDD24EE25D50F3CF6E2D2D8E78F4D28C583E58
Malicious:	**true**
Preview:	x.#..*f..H.....H.&3.C.-c.!.(.&...^.P..q..aVc.& oQ.Rh..n(d.w..ihc.C...}5l..9..^..-..1...K8.I5...\..'...A&T~R..-s ..V;../Mcls...<.6.....[..!..3.).2#..}z.2.<U."...-Et..Wrh.(..s.$.,.....x... .S..B.`G.....Y&.RmE..M.v..4..V5...&m.....9X-P...H.]..-.G.....Q".....,`...+...@.*....#....j.^K.i.&.R...Y..E.)y.=.+....o^.{.H-.R..T....y7."R....k".'..g..=...]..>.....Fs._.....^..w"C...n. `.`..o...\.i..hW..vd.v.....f....S..o. ...'...n.O..@....^.V..D....R.....6"I.X.).*{....;....".+..%....Z...~%B.....w@...oW%..(x.$z|.C..C...qR.8 ..X...a.U...0...@E's#p...u...."Y.L....~..@aL.G. <~.M....]............jr..{..ok...$.....r.vYJ.h... 3!{...Zf.6l.n..!?....4^.'KY.+...h.NS...#...3...s....;T2.s0lK.L....oQK[..h.(....'gb.Z..';.....yu.5Z.G..@...%.`.".p4..a..\B..-.mP.E@.Q.K. M.#....."'k.>4.n..q.m.....4.....\.t:=..k.....V...."c!...0.3.....?.-...!....m.5}..*b..q....S...ha.H....E..<..%N.a.....h.B.r...9.'m\....=T."+&[CK&*...x.X.T....$..N...A.....v....=....pcL2.2

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Polish.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	OpenPGP Secret Key
Category:	dropped
Size (bytes):	50560
Entropy (8bit):	**7.99635386590933**
Encrypted:	**true**
SSDEEP:	768:qkvdPVG9smQCA1CMo6XJEGGfC4/p4g1EQrVmuLj+yQWCRKj0aaPbZr3z2BdOpypu:qcGs46bF814g1EQrcuLj+3f9VPp+ja
MD5:	85A7A579403177C9E3E60A25987AF90B
SHA1:	E8EFDC66C30DC0C07FB4557C3143F471C9E37053
SHA-256:	1D1E541BF51C145AA6AA6BCBEB7BDCC431B35594AFF6FA2DADDE44E65F733FD1
SHA-512:	3CE754BFF7A3AE082C8F3AF956AB70F508D21254C77EC8005BA02561DA0BA132A96621E2DEC22562D4211044EAD0853FF583F1E76CA8EFAFF4684B6CEBC1C014
Malicious:	**true**
Preview:	..U..}..9.I..K..P...g..D....|..}I./.6...S.9d...H...%.F.c.O.....D5.1Q)....8s.&xj.(..=.gd...Mz.Uv..C-....].`.....U....BJ.6....R.]c..UWh...3..vw....2S...Y...dtG..A .6.].Hh+....G...AE(.F.`..>&..@H[...Fc.8...rL.T7...w....r%.....U..Y.o.....t.gxL.^...0..$MbF.t.(..#..[t..*.....%.y{1.....hz...bl.[#...c\....$.C....$|...w.z...e.3.I...xNq.Us.!.).B.ex...>..... .r..2.@..x..|.C..{..A.[... #}d`..y..iU.6|'8.+...Y.8;...W.....h{...y RV.*....H..C..w.^...T..D....D...% 4....&K.....S.$.?~..+G.D.....O....Zx7..B.)...,..nY..4.>4.G......?...{.....Z....r:.....,. .....1.3..F..tP*.a..o.5|;2..c[. .....r....;.D...7..$...E.L..._...:p....J..rx....W:.S..q.{.k5...o!/..9vO...]@.3DO3.h..=..D....F.R...n"..T .T.^..4_dx"..&.m(.V.S.@E..1|6\{$U.Q.Oz..A*4....`. ...q.....)....o..S.6.....\..p. .?..d.c.u.l.....G.....X.'..Y.....s<.!..xf=...Cs....K..d..;.P.s...u....9_.=R.I..[.xw...i}h.....O.@..x...?.....L.dL..+.C..P.D.}w7>/..*G.6Jp.....D..]vq..A.

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Portuguese (Brazil).lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	47840
Entropy (8bit):	**7.995625621538136**
Encrypted:	**true**
SSDEEP:	768:xTreCxDnt3oiPe36rG4dNoAvUYzCpZdWKyxb2HThB8nEy+zIG3cEvtFch:VeuqiPbG47oAvF+pZdWZx63N1Fch
MD5:	4ACF1F61F613FA0539913AC3DA59825D
SHA1:	9DDFE0769A5D3A8B3BE587FDE36D7CF6AF5281AC
SHA-256:	388AD6F6579A920E3709BA1081EF92DC9B7DAB86AEF82955A6111D9328CAA289
SHA-512:	E60F3C201378101DBB543D5EC2FAEF6A39D06CAE447FA98D31638F06B423AEAF953F27E7638355EEC32C66B13C69A51C9CD9C1B60075D3B2128191D833F149F
Malicious:	**true**
Preview:	='Mfh..f.....a.....].Q0/..k..B.."?\H.=.z..P.I.(Wk...w.f._...b.....1;...L....W.....<..@./+a.m....z.C..S.AY..s..3....|...O...W.V...pAik..1.v.....:c.....6L.....w...t..Rp.nY_..F..7....2...u.a+ .Y..I|W|..#M"[W...q..x%.d.w.'8'...b43..>=.).m...d\ ..;...r....=...LEE.Ci..C....._I~.....n..}....L..h.3T.9...\..b...u..F-q...8...'b{...48.....%.'.3u..W...0Fv.pG2.....Js.....6.<....-A...t.. .q(3@,.....|H...E...BfM'~|A...L.-....Kx...(....;...:.; ...2.....^..(..'.....2ns.....nL\...n..E.D.P..o.+h?...G.....ud..%.37@..5;W|K.j.5....>d..N.....Gqb_..0k.G.{L8.a.IP.M.2.. 0e03c.1Z[.O...|b...?.....v5...%.82.!.....Xxf.s....-....LE..p.u.....$I..}X.".(....9._..}^.>.Kn..#<...&.<8dqdv...!W..B.z.....XAAQ...4.].7_...G7_...t...i.@..-....!...-.D..s.vX..._.....n{ .'.W".h.D...5w-Xh~o..-x.ID=..S..'..8..Szt..M7|...#..rH$d.U..e.v.".*....I>.9..s.H..e.-.O.~j..t..h.f.e;I%.).....".&..}..S(%'h3.SA.[F..... ..%.6f'.'h.L.....X..X,.

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Portuguese (Portugal).lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	48224
Entropy (8bit):	**7.996408622809594**
Encrypted:	**true**
SSDEEP:	768:YgPomgYKM8lAVvoqOkg6s0316391nodXq2h1Ohro+urLYGzlGW3oTM:YXVAVAq46sy163II2h1OhronrLdzlP35
MD5:	5976967D6E02EDFA7283ABE2499FF861
SHA1:	0F88B636CB2D3120B103FD3AD36403B233152CA3
SHA-256:	B9B9FC82173138B02367D022796056C08B9AFFC1F863E4CE6324BAB50FEB831B
SHA-512:	512AD1D35492C97C1628F7A5F2E37000B74E5234D1421AE0E2B4CF2701C7FB47EAB414517103B2FC12ACFA656D156D11F7C9288D24C0616F3ED2F751DD26492
Malicious:	**true**
Preview:	..e.o.@R...8(X...-..m.|...3..[t.>.].....6.i..z...R..~2.....r....-$n....Gr.....L*..P.]...Z..ZiF.cs.>37.I..qB.\+..({c..*.&.+.....q..5...c.)m.eh..f..D..&G....}..Kh&r.%x;..].;...Lu33VR..7.Q.9c. m.=.....a#..Sh.x...6Q.....H.<.$b.I....I .+GV.5...(.w.....\\.yL.>=/.B^Q.5.....%.99.\@.~....M..8|....7.....=.\P....e.;Dz.s.tz..n.t.....m..p.ewZ...$2.N?s.|@fpb...o..$..<v.j...1*.aQ. K-i 58....k...+.....k....-.~7F.S.#...{jS.a...e..x....Q.\..[@{...9....>P..JZ....CL.I.+.?<..r...s0MI....w..E8Q...Wr.....F...g8...b..6....6W|..A!.....g....pn.e.%..~..{...E{.....d..aD...9x.... ..u...\....k...Y..>..E.....e1.y.7..r.;...<Xo...u.K.....h[...Qhy..h..0S.Jo...e]Y..g..=iR-@.B...A.*..u.V.....D.I^%%....}..-+....+. ....M...p.....p:.J.I'...=..[\d...-.... ..U.....R....ma....O p..Jj.c....".D-a. ...~%n%n...Y....)...6c.x..OS..+...I..R"..S.^...I..h...v..."..q.`..g...tb..T...H..$^.....7..N.X.w;....~8R..J..2..W...q..+iB..$..c...T+..~Z...F..ss.st.

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Romanian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data

Category:	dropped
Size (bytes):	49760
Entropy (8bit):	**7.9964153063104035**
Encrypted:	**true**
SSDEEP:	1536:X5n+heipyq7SeJkp2YGzFe7KRYJDcOLW7IQ0:5+xpyq7Se+p2XFpeJLz
MD5:	DC4BABB13A9ADDADCF7EC9272DDEE742
SHA1:	83BB3EE6809E79516EABB38946E5E017B47CD830
SHA-256:	9FA06B1113E8E92F0802C557996B040969F2E5F92D1A8A1950A889E2F35B253A
SHA-512:	29C9869BD6E609B37CDA206A9D2B5370B4DA0F2B987863B4D2B7EDA5002A45D09C8CEF1DD3BFFB0F6F2DED355D758253DB92B6CE346C8A8F56F189E3FE480E8
Malicious:	**true**
Preview:	].)>...?z.....-..s..Xg93.p.....9.....@.. oW.7.GUc.q.jj..=...3....J. ..U:Qa. +....A.Hr.R....Xy.{.V.Y.....-k.m....Hj3).%l.....X...?...S.4$.....)r...g.1.....F.]..j@.~.....!....XP.1..=.t.6Y....QQ..M...".....e.On.....{.....B1o.....V>#...k.k.....)..+.....1.}...g.SM..#.g.,[..X...\...GT5....:..R.B..h"8q.F..je.....|....;....Wq.3.....?.....3....<.6.....h.W.....].t^x..!l.....(S.....;..&...Sq.N..:F;..z....S....l].HI.....>h.2i;.S..S..yWK.....x...1;.j.l.+.....K.Ld vY~0....L.....5....~...&.....<x....k..^.....8%...*..\g.^.H.U...d.G.D.....<...x.3..J.:q..F(.d...T\....h.q...].*..#..... oC-&.2b.....]9u. ..f.....A!m....\.g..*?...7.....vd.~S.z.(.o...,R&.k.:...ud...S..F.....|..'....RN.....!<....u..+.EQ.?.....T3.m.B..%r...P...O.7...{O.k.j..x.b..4....U...:.e7.0.%eC.9.-.../z..._ I...i.r...1..M...=....BN..\..#...fD.~3ph.....h~.....=.G|d...h.r.....]E.....1..0'.!...m..H...h.....:.Y.(.....d4~

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Russian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	56800
Entropy (8bit):	**7.9970102992115475**
Encrypted:	**true**
SSDEEP:	1536:zywOP2/7BSAPayFnIniST+EwdqG3wEgJLxqzOT2xDCvajcwL:e/Ot5FKnikadx3I9AhxDCSwe
MD5:	9F9C51EBFB643D79E2843482F592DD89
SHA1:	108F9AC6A61B9395656FE3069C08360B527EDA7A
SHA-256:	A1871AE3F762E64A18E8A46BD2C175BBE15C40A63C2DDBB2E0CF32FEFFE9775E
SHA-512:	2BE920DACDC2947C4B2F8CC4F2B9CEE9D1BBF6D0C09DF8C2364722D765220ECC4CEC574F80FC95D7D0FB669E10C34FD616EA0432F46212282BEF7BEBD8D826E
Malicious:	**true**
Preview:	.S.D(...A$-..;..F..Y.....E..O.s..[...i..H....4..Z."a....;g(.j.<.+..^a/....6P.....~..^{\`..R.@.....>.B..>...<..p.>.Ir.....cO..?;....6~G>.#.o;./A<....9.....~....D{,c..x..."/..s.0b.....|....[...7`.&.F..!....z..{....n.....r.....T.X(x..@...h.....y#f...;.f...}..0.I.....Y.....6..tt.....n.x..}.E...It.f.).....R.:.....{.....Pf..7).....CQv....1%.Uk.u.o.f.[.,.x..(.x..S9.....#.....q.....`O.g..6.\.#..:..HAGQC.G.P..|...&4...w^..\..O.....Ty.w^.lo.%..../T.LM.u..^.....M..?...XsX.m{.A_3..._I.....P...a...$.Ei...../o.y|N.....Nq.*Z*...r...H..#.....H?.f%e..Y....*..(KR..Q...L.7o.,.Nm.....G....`6...L...B.5.%.M=..v.x..\y.q.L..qK?..B.:R..w."....@&G.}...3.y....<P...*...._....Gn....+..\....*.\...j6.5UA.n....1\.G_....u.C..m.\.9`..... ..D__p.wi..!.....ni}.`y.W..n..k)Ia.]kOi...m.....D+.....Y*.k.N?M`..D$....)..IV=.1.'..$Z.t..8Anw....=.S:B,\D].../.nCo..^..^rB1m..e &. ._....@ fy.[.#.....,...G.\(?.5...n..}9....!....\.B....."Y.D:.Xw.

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Serbian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	50400
Entropy (8bit):	**7.996046989865242**
Encrypted:	**true**
SSDEEP:	768:PEzrJZnyxQpTXXTmkJXJ/HA9myX7KjFK8YdXIQlWw1XA:ej1TN/APX7EFKHBImQXA
MD5:	CAFFCCA11A26F706C9E42A81EF6BDA8F
SHA1:	409F1C47D59CCC025A4341AC4BFABF410DF8CBB5
SHA-256:	82EB2B19911E2C6CBD467CBFE193A8E4B307E4C85124898767D5FCCB25F4FD87
SHA-512:	BD012641EE0CD06BF74C0E2922D7B33CB1782A94CBFBB9C066A6EB39AB3354AC200FFD189B349E6A57A82D79F9D17622F813B1722BB247D0FA8B3DF6463AED43
Malicious:	**true**
Preview:	..D.)..S.x..$...X8...)...\7v.....q...,g.M4.....|.'..w..._..i..EN.P6..E...5~.....F..~}...p0n.Jr.q...tL6.c?.....@..*`.@S..zW.....sx6..'gol...Ek.0Bl ....*K?..h.../..X{.....S[9s...(....2X,#?.A...B....+GD.[..X..>.j.X...e.h.....U.`K.#.....Cj.!..L.C...$E.+8...y.1'.k..3.Gi.nd'U...w.v7..D.k.M..... ... .^.....c1.....ox....Zv.`..g....~5}sm.. 6.(.....H.....v...r?.b.....A...4..V..}....(.lq..mf.g..O..(.)(j..l]. .i..kL...G..{.o.....').e..S.I..\.p.....f.#.....-a.W.....03..Yw[._...c.V..<.F....l.(ou..8*..1.v....5..1g.....:S..#.NW...[.3n'..4..q..fgHg=)Q...jt....@..z.....W.M....S.....v.....xJR.H.....J.H.T.D"..s.]7UwX..5..&.:...$h.)..hp=..E...K..p.....q.q.J.....8....f...3..3.....@.i.h}.B...G..c...3..d.*J.qH....TC.....l.@.CXX-.....ZO2..I.g.x~g..P.....|.>n.sWuZ.o..Wv..$...i.) ...y.5.....Z.....r.....w..PWf Ie.:g...(.]B..z...7..q...5.C..ys.q',{.z..'..'....z..<...W..3/.M)..$.{w.C-&

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Slovene.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	49024
Entropy (8bit):	**7.996060916447486**

Encrypted:	**true**
SSDEEP:	768:2mvkH0KEnIbYjfPMBT4qkj7EYPrtmVMWJCGp58PKUd9RevBSKJ1xOl:+H0DnIMjsBT7y7EymBAjP1dL6Bt1s
MD5:	C9543B7FF82DF905540969271E56A2B1
SHA1:	7452274FE9BBAA09E74FBF41D2357FECD6040A1F
SHA-256:	A7202A0CC59A7A09B8D8EB5A3C6CBB6FBAB785750B0C2291AC8F5CFD4A56C631
SHA-512:	51BC5A8207F1A27E7C8652723ED5D287FC9CA8A81B495E2AA83342D56361A029D0A02ED4893CAEE24487B290FF3CAD6CF4C7566C9DA5717A3D0C506D3059F4 4
Malicious:	**true**
Preview:	RmF....(.F.%<)p...%...XB.f#..[...A^1...ZHhR_.y.(.."........mn..u7.)..2..<..~.........t..4;w ..jV.v...tl..A>b..w"'..h)W2u.C./..$.,.um.Q..#r.Z._p.N..z...%Gr'".....}f...eQq.*...#.........Vb...cx.. ...9...'}.....G..r/.t..9.C....&.6D=Z...#.x.....K.U.;L.anT..>E.4Z....-W}...,:..w...~I.l.4.)%...`qt.....:...I .Ck.Pq....`G.nu.D.....S...P...T....a..l....,.R.....,!.(&~..4].....5..}...,...a....{#A&{ 3_An...f.j'*....wZ...)../f...t..Lf.X.v.S...X...o.S.ny.Hb.....oA.....eu...gbk.a.>w.....F...;B...2....<9A..QM.w..^J..P..|.m.Nl.....PT.....).&.N..;]..y..|o..Hr...mb..x.*.@..t...`..;.E..$.;. Fqd..S..D._..m.....wg.=....Z.+..w..e&..T..'..a....79..1%.....(8%.....m.F[g.G... ..bk...P01^...kn.^%W.".}...q.Bfs....o..F..[.j.....K....w.....y@.n.N..''y...d.#..!...@...K].....bI...cU.|.<. M...*.6.z...j.....\....P....t.s{..<.3+....j$..i.*>."...x....u..<.=..:A...?>g,J...v...OU=.)../.9.6.....t...).(.tv..w.B....0..;.....t..L9Ze$.;U.n...*.....OUWb6:...>./

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Spanish.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	47840
Entropy (8bit):	**7.996383987781172**
Encrypted:	**true**
SSDEEP:	768:K3zwfMYYUfSFDGQUhwktB26yA58bVqd3YXE2PUNCH0g1uZS+COkGheq4FuCzl5XH:K3MBSNmhtVZ8bVqdUE2PUNCHXAZ3bD4h
MD5:	EDC771A651BAEABBD4E5BA0E61166764
SHA1:	6EF66787341CB1050A4559D480BC843B78289A0A
SHA-256:	FCD15C7B0031BE60770428F2A0F40838FE84EF466F2DF17052C1BBA7A5BC3FBE
SHA-512:	1D14535907F33482B72C8131C8FFA2E1B45805991CF60EFB7A05A26D236893CB8F44D10444B551096E4582DDE61A6D5855F1B1C441098CD095C6607EEC2CC2B4
Malicious:	**true**
Preview:	.r.d`.^7.... %...o...@~..=....x...G..@^..Q.T.K...o.Y....u_.<-bxdwF....'..4.|.)....=....V.6.b-?y*.k!..9s.....V.Z.$..b..Lg...og...u_f.W..qb.pk..e..j.T.KyE.`1....'.?2....O\|Y......H.q.\H\|...,A8. ,k.L..5.....-..BV.G.4.K.~Vq..^...E.....)Q.3.tJ....m.=....;.#2....p.....}ho....K.pg8[#B.b..=..`...q".`b...LrC.n..np..L..{X.h...G.a.F.f.....cR....6K...-v.\|n.7.....Tsn7.....#.8$..H..... ..D.u..`).....uA..(gl.|....+.....z..:.H..w..../..m.M..G....To...VGI...Go..bY.o..3.&,e..u..%N....A9....tQ+3p....<;...&...,..E.a.2;4.9$..`&...a..q..!e....!..L...:..._.;.;u.$P....tW...+.6...R. *..@__%i7.4r.......3.C..F.m....2.............+.Ts.9.U...F....V.:*.o.Qy .....P..i.[.^.1P.6.r77.Iff.vt...=..3..!b..gB.......GZi...l.o.T...GFhd.3.*.\7.I.`(..V.5..r.[.m.H..!.|..o.%.._Old.t...*.. ...V.4<^....M.N..s..ZB.@..Wa8.[..%.5.p..c9.w..hjD.....i.,.=+k.D.l..%..q..mD.....9:Gn.Q..4@.)Us.Q.6K...x...$..>/... L.V..4... ..{..J+..y..`...&:h#.g@/.Xm..j.l...O.....NFn..4.1..... {.+)Q..8.. (.

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Swedish.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	47360
Entropy (8bit):	**7.995550966019205**
Encrypted:	**true**
SSDEEP:	768:RxEQKc76f9lm3Gc7u0Re1/nrzGgN/mgoTOmhibA37t96E:PMc76VlmWc7uOU/r7/e5wA37D6E
MD5:	086C30E3A434837B293290032963A7FB
SHA1:	8A21DF3E6FF91DD383C3B373C7B645A4AE3DDA44
SHA-256:	999337F8B71378A31F1D818B4CA5A1CBF2CC01128D7ECC50CA8E234FC52B5AD2
SHA-512:	807D5DF44E1A8412FDBB3C55E06D1D09C84543E6D6942194F6793197D8BA00D9A0F16C2B4F28CB02233D9406DEC37E5610B55058B948E145058DEFAE06B55F7
Malicious:	**true**
Preview:	h...1...r..~v6'.{... LO=..@........).n...u|..<..O.l.[z........G.>.....[.....Rg.....>..xt....4+.....+.....r....$yO..MB...XF...:..z..TR...u.....t'....[FY*h..a.....7.wl.....Q..=...r.w..rs.4"....`..V.7...$.. .L..1...."....'.u.........h..Crq...S."3...2.....G.G...J.U.~.....%.&.p'..l.....e.j#"...8..0.....'...Lf9Zr....@h...]:.....E..qF.~.-..[..=0...^...q5.PSF. ..(=.'.....T.l....2..qM.15[.F..K....fQ.. I:...FF..s..Y6J.9....\5..29.....).'...-...B.\y...+.y...t..^..d..}.@pj.8i.M.g.@.L.....qc...`].z..u...Q..,.....S.h..lr.....f.p...P....v'I..E@5|M.x....J...M.....=...cK.*PA.sv.>e.>....z.....Aj.L ..@.YQJZ0.x.....o`i./oM....cz.a..{.ov..Q..o7E.T;~...K.\.h.#..5...Fp@h.Tu~.Bp..f.<xA.....~..'..Q[b.bM.o..bP.....Y...uE..O},.}.0.5N....M.|mB.....0D.V......"7.o.a..... '..v.N.. C..).....4_.$.gX.....>!..wb...6.\J...&v.</..HN.$.bt.....H:....z.Y.>_NF]..;.>.u. O.....h.-1g..:...TU.h...?...s.).{....I...v..K.x.....}H...P....Vw..

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Turkish.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	48576
Entropy (8bit):	**7.996319364768242**
Encrypted:	**true**
SSDEEP:	768:MXc828+Y7CefJ03GAdEIsH9GkJ68o6nMhnIcIa8+iGmHk8daCP1f8lzRGLpnMn+K:Ms828+oCefJ03TTb8TnMhnIa8+iRHk8S
MD5:	CD0D7648ED08183FE8D4D1E788B16557
SHA1:	930947B114E3EB06543190EB93437CD8F9DB0DE8

SHA-256:	3AF1D3C81E0959E1BF30554472E1E71554F11BB03736471E8158CA21FA0EF271
SHA-512:	9002D56B59F3F58A4EF4CC5BFBC04D05B043845687B60EAC113F32C181F3FB02135BA91264562F0E7C2E9E16EB23C3F5B14A8DEDD658E34F256E779C1BEF4141
Malicious:	**true**
Preview:	.....9....3.W.t.=.3...o.jP.....uP.eH<..0....{(.vHl.s{~.wK..`...b..s....cX..>bu.l..l$.B....7C@...]..9!.+.....r...k./....."...{.+eC..i}..Rt.0q....." FMc..=...!..O]..HY.....P.nd.].S.+W})J... .m.....%N5S..Ey.%A.i.Q..-....y.H....?...V.....8..}X.nN_..o|k>..`..8<[#V0..._.-#.M.:.....=.....V...y+....@.W.m..... .9.....o5..m.^....U.68...K.D..\.....q..2-.....N..o.j...i..4.)....i=dea ~~.aZtd.YK.2A.....zJ.jx...0...>..=.(.U.9.p...w.I...]w.1.0..2..".....#...0K%.^..T..N.7..l.....).)....R".....7Ye.Il[....4FX...W..b..Z.=f(<.....\v{.....f.~.n..56....5..]pp.z,..It..Pp....2... y.....+)K....dpbb.....c8;Q.#[..R*..{.G.E.iJ.....d(.....dR....-..Vs.l.xd...E~..LEi\!=4..M9.z(..>.*C.a.~l.50:..If..-W8..8...%..k}....t..N.R.mG..M...&O>x..Ao[..t`.c..t}x.._.%5...*.+.'.Z...X...@ Dj.`..l.\E.].....M.h.....T.S.k.....X..p)....I.....v)M...}...F...Rf.....l.....-..7..6.....{.@..6D.....(.].p.....DZ.....%...n.`.H.z._.q.....n.1.._t

C:\Program Files\EnigmaSoft\SpyHunter\Languages\Ukrainian.lng

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	56288
Entropy (8bit):	**7.996902131172993**
Encrypted:	**true**
SSDEEP:	1536:uMlhdReDtAraGB5YMM5r9t74N3tlhHH5L9LD:u1hdReDXMM5rT75/L9/
MD5:	D740E315307ADCA0117DC4A12CD88A24
SHA1:	61BF9A0D773F2742BA0A01095F9E4611CA38EEF4
SHA-256:	040F6028A63DC21960DF65066BF14CB38B3A562637EF7716991AA38B97C3168D
SHA-512:	260E5E7180C427ADFFC6DF1DF1308805366CEF219BBE67097281C42AE24157E8758B3AA65EC80A83C65C1207C72F66A0930811E2314DDDF0860222DE22146308
Malicious:	**true**
Preview:	I.....-..A..rQ.a.K...o.FI.@..3...z...n..(....`...V.*.i....>J..!.JL].`.;Z..4.....!...._.a....%3qB.../.?b.....}.MTC...yQ.,g...v.q...KW.$\0K.....E.9.C`....0.....1...rH.v..cJ2...P.=...B....%...y.G.Z.]. 4.O.^i.P..n%-.....J.X.I.J'.D....(8.#d&....`..._.`r.{t?....0.....U@...{c..1..%M\7...A..D.....\)_..<..\...R....m...M.\.g.2;b..E.....z>..3P..k..Q.<...d.:0."`..;.>b]nF.jN.G&~%.....P.... d..a.....2.L.U.....9...Lkk...0>G.I....{`....X...a.%.<#B3s....p.Pan.(.[Y..0....5.?P5.V.C9Y..SI.T.S...jD(..Y3..../Bj~.....g...k&N4,..*.VX..:4.X ...k.N...x...@{...(.fl.k.....v...../..#.#A (.0~3-../&.?7%....3`...s..35....u.....g.....~..:.#.0....!\BD.... ,.$...@..!Sr4.....H..e.ku<..E..3z.....j.k.g.....&..#.t..=.6.tL.^Tb.....%.wE/.l.&kB<.m...M.S.{..k....>T.....%.,....[.P.f&.#..`. .<.R..6.L...r...U....x.W../...l.....V..._.y.\p2...x;.rYw..d^.....z....Lt.....x..Vr)..E+j.....S..=h%...P!.i..F.....H..j.a1.....z~.|..u}..3.R.q...DSR>/.D;...nl#.M.z

C:\Program Files\EnigmaSoft\SpyHunter\Native.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	63464
Entropy (8bit):	6.542288481337166
Encrypted:	false
SSDEEP:	768:96yRcovNvvLkY6CyB1QU59VZtXxznwC2duTmAyVM5DXcE9oPxXWxX74PxWEmP10:9Lcov9TxJKHzTbSuaNC57iPxXW1MPxZ
MD5:	49C446627D85AB0A3C6E731FAB4723A0
SHA1:	554EB949392543B02F553858923B52CB7943F159
SHA-256:	F6540D6953ABE9853744B317341FEB138104A9D78662F08B7136D61A67E5DB4F
SHA-512:	0F2213606329EF81E44CBD2CF1B0A42B7E93C8C8B96597A0B16DF979005F1D1A3566A1CE2B53A220AB06C99B8295203E51B2753E76D699C04500A1A340C2664A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....so..7...7...7...A...4...7.....>v8.5...>v..6...A..6...>v2.2...>v/.6...> v*.6...Rich7.....PE..d...vP|Z.....".....n...@.....@..... .....(.....K..... .....text....m.....n..... ..`.rdata...&.....(...r.....@..@.data.....@....pdata.....@..@.rsrc..... ...@..B.reloc..<.....@..B..... .....

C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	17032680
Entropy (8bit):	6.59177505889633
Encrypted:	false
SSDEEP:	393216:E4DreTdP6z84yCDy5m9eDG2EIPZLOYy2G+Q:E4Didiz84yCDy5m9cBLdXQ
MD5:	F2F6BF33561C9EF8FE3310D46A3C8A25
SHA1:	09761F024FC32B61FA0667BA9DBE8322BC93F0A6
SHA-256:	34EC1126BC2AF019E1226BA114AD38CC6773F9640DC0EE0E5715F5423D47615E
SHA-512:	55407986BF5592A7A9DFFF5B72AF598F2E9660B44B9FF9A60D772BD8560F2D3875BB525E2CA79DF2F93C56FED52C9A39EFFBF9353486A346B7444EF8447ADFC
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_EXEPWSH_DLAgent, Description: Detects SystemBC, Source: C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe, Author: ditekSHen
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%

Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode....$.....qRx."Rx."Rx."...#Ex."...#.x."...#Fx."...#^x."...#\x."...#.x."...#.x."...#.x."4.."]x."...#Px."...#fz."Rx."Lx."...#yx."...#Sx."...#Vx."...#}x."Rx.".z."...##|."..."Sx."Rx\|"Sx."...#Sx."RichRx.".....PE..d.....Rc.....".....fG.....u.....@.....Q.....`.....0.....K...P...%..P'..p.....)..(....'..8.....text...b..... ..`.rdata...Y2.....Z2..@..@.data...Iv...@.....$.....@....pdata.....@..@_RDATA.....p.....@..@.rsrc...0.....@..@.reloc...%...P...&...t.....@..B.

C:\Program Files\EnigmaSoft\SpyHunter\ShMonitor.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	549352
Entropy (8bit):	6.448794633744019
Encrypted:	false
SSDEEP:	6144:p2KqjCl6BatX60NlFxbueeCk7bTkN4vvcrVrp6Ms2srilHVohJgkelZW0:pJq2MkN60RFuLCkgCn0dp6MSD1orgZy0
MD5:	F9FA9D3B5957F0C365A20DE5C71EC214
SHA1:	8E6B91CBA2C323D2BCF29229E69DE5F44F5FC8FE
SHA-256:	CF6B1A1B75B0090A59E8A41A52F7E63C249559407A67F0744AAAB15B210B1FAC
SHA-512:	493B7015027043018A7A8FE9030867889F4AB93621FC3F3E45106490B95CCA8FB95D9447FB3C074C122B86B6C47B24C8ACA3ED134132EFD1DC263ED4120CCF8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....f.j...j...j...1...a...1...x...1.....1...g...j.....8...{...8...`.....h...8...3...1...k...<...O...<...k...j.k...<...k...Richj.....PE..d.....Rc.....".....@.....`.....x.....`.....A.....K..p.....(.....8.....p.....text..... ..`.rdata..Z.....@..@.data..... .....@....pdata...A.....B.....@..@_RDATA.....@..@.rsrc...`.....@..@.reloc.....@..B.....

C:\Program Files\EnigmaSoft\SpyHunter\ShShellExt.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	857064
Entropy (8bit):	6.597191080622984
Encrypted:	false
SSDEEP:	24576:1kCtesF95/4mjZexpz63VIZOWPBA8Jgi1z:B395/DcxBkM2Jx9
MD5:	8863C0F4CC264B818749049F8251D0E1
SHA1:	B95CF183E3955F5E91E9BBAEA436F095E33CDEA5
SHA-256:	538ABE97A7D5B1C301E8EE72E5E8B8CBA58AE74369C567F5F1E6480506C6EC34
SHA-512:	0E6DE997B81195F9517D19A878CB43E87E2915B8236AFB3B430C4A1AE6002FC51888FA96356F49D66BAB7B952DA15C13EE5EBDF32B38BA0E20C588343F3333DA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....<^WG]0.G]0.G]0..53.L]0..55..]0..(4.H]0..(3.M]0../5.E]0..(5..]0..54.\]0..51.V]0.G]1.[\0..56.F]0..(9.I]0..(5.C]0..(4.F]0..(0.F]0..(..F]0.G]..F]0..(2.F]0.RichG]0.....PE..d.....Rc....." .....x.....`.....L.....X.... ...].....K.....`...T.....!..(.....8.....text..... ..`.rdata...P.....R.....@..@.data.....@...(... .....@....pdata...]... ...^...H.....@..@_RDATA.....@..@.rsrc...X.....@..@.reloc.....@..B.....

C:\Program Files\EnigmaSoft\SpyHunter\SpyHunter5.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	18037736
Entropy (8bit):	7.132271432325441
Encrypted:	false
SSDEEP:	196608:ZssPoaV55EByQ6+Lzs2rqIaG7f1GMRlsdGDlOH88KegZkH:Z5AG55EUh+k2rn1GIsMEGnZkH
MD5:	096FA37EA53BB15959E9EEF9FD3F2745
SHA1:	733FA736561BD9FF34B5946D60D0FEB1AFBEF95E
SHA-256:	4F08CAC75CB5A4F5B204986C1F7AC12FD04008E4B10425862A59F0A79512E922
SHA-512:	6B62A2E4DFBD7F2E46F61E52F9AA9DA618C3072D8C17C7784FB9281231A95D8D3E3A1AC2DE7663287F2FB4BC31E87DEB847415629EE173CDC3ACE94CCBE33A63
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....wN].3/3.3/3.3/3.hG0../3.hG6../3.aZ7.'/3.aZ0.?/3..]6.8/3.hG7../3.U@.9/3.hG5.2/3.aZ6.\/3.hG2../3.3/2..-3..]7..-3.3/3.-/3.eZ:..-3.eZ.2/3.3/..2/3.eZ1.2/3.Rich3/3.....PE..d....Rc.....".....`.....P.W.....@.....0.....&....`.....h.....;K.....`.....K.....X.....p.....(...p...8.....p.....text....^.....`..... ..`.rdata.. .+..p....+..d.....@..@.data.....@....pdata..`.....@..@_RDATA.....X.....@..@.rsrc....;K.....<K..Z.....@..@.reloc...X.....Z.....@..B.....

C:\Program Files\EnigmaSoft\SpyHunter\data\CrCache.dat

Process:	C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe
File Type:	data
Category:	dropped
Size (bytes):	1691520
Entropy (8bit):	**7.999886530677001**
Encrypted:	**true**
SSDEEP:	49152:wyfLU+F+AsgxiKGrdRVZaIlpNQc1waWak35AO+iLya:wYwgA3VZ2c1WmO+m
MD5:	E6CA61B636AD315AC46A30E59E3DCF8A
SHA1:	8B091D8823A53EDAAB40BB4AF1B8731C41CE8852
SHA-256:	FE9AACAB975512E6816CCB41D96049A6BD05D22B37E87558DF24A1672A137B8C
SHA-512:	BBBC2D7D5A62228345DDB4CF871D20C7390DB05A471A1E55C06D2FCDC8F0B6BC82A5846095A5E73C65C7F3A8DD59690368D243A64B033936C93DDF00EB4653
Malicious:	**true**
Preview:	:.9....fb.....]...#H...5..>g.U|.....F7..-y.n...{..P!.8_?.Dc....SN'3...Z.]qt.JT...w.b)....>...j}.xe.b)R$..e.#..s2..8v*....^.Y=.?R.5. .I]...s.PZ.nB..u.N>.7.T.....x.t. U/.g2'My...P.. ....~.....1.!}.G.a$2]....O.W8.d...`...5.$.x.w.,.j...*(...*..ri.SyA...,10.....84.BF...S.Gt._...F..k..'9.'F.a/V.g.....".*4.;(M..J.m.....3.\.....Yew.L...."0..$9....1G...8'ZA9.o...V.....f.....=p....!]M..F.$<.1=.YAF+8v..s....t....m#..%&...U=..#..uVl..`4.....N..E....&>.98...2....X..>nT.....Z..9B..!x..|.9.M_&T..=.4.).z....j./Z\.....y..n'....a..K9...V ...u.@..L.!.....d.'$#]....]5Q,.dJ..9.....jl...WZ^\|'.A(..t.....\.2.{.$...4..Sl.Q.....:.M=.$.....$..3.Y.....4.....W.n.....v..,..e.Edy..F.....N...d...5..a..a..Y....?F.<<...qBr1_#.....[...../^L.,....._.....+&.....f9&|BY...@AY..m{#.=.NJb.{N.d:0pH..T.....v(.(.N3.E.....2.k.,... .....l.s.\.;..B#dR,..W.{r..e.s..H.....4.`.w,....>n.. ..i#...../.`.R22.;D.v.Z.."@.....U...&.19..S

C:\Program Files\EnigmaSoft\SpyHunter\data\ScanHistory.dat-journal

Process:	C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	7.813953058985591
Encrypted:	false
SSDEEP:	192:7CReCQiGhtYDjSmBQt28vfRdfz6hUyOszHtNtAP:7CRlFneJvpchUy3zHtNtAP
MD5:	50B3CF60F997870D5354C5A1A15FB649
SHA1:	9D49FA09944C29A5921EB9CF96C918A65EA542E9
SHA-256:	7D5B14443FBE3DF925E21476719999FF6A13B4C6CBD27DD72AE1F3DCDE43A183
SHA-512:	3070CCEDB081C383DBC550332267B9F3B3B7170D3B77C94F0C72E89190716417E54B5E46FDA266F88919AFC35BCFA1AA80CD21CD8F800F8BE1A646651284FFDA
Malicious:	false
Preview:	.... .c.....)....?.Z.....x..@..mk...Bm..m.c..AA.....l...j..|AA"..[.J.w`.2.....>YA..S0..S}rt.e...8.<)..z.....Mr..K..xO`GY..f..0....*`....j.....".%...c9BV@.${~.....b(e.PP.]....g.k...+r.7n.Ni.r..R..$...>K-V9e*ERO.p%.'io_._.-....L..AY...|.ke..Q9..;w./.#...[>..Q~y../^sy.....2..5....."o...a..dPxK...s.:.z.q2.i.S.yq`w....N.k,t,?"FN.5Lx.e.i.F%..l.....k.@...m..w,WH8#qF.x8...(5,....tGdC./.M.....1..(....5....BN..J..zc..2.ue.T.J..f...k..n.q~...5...Y..Z.w..u.}.V...U3.

C:\Program Files\EnigmaSoft\SpyHunter\data\acpdata.dat

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	1440
Entropy (8bit):	7.873396989507999
Encrypted:	false
SSDEEP:	24:pHhWsHQrKrsnxHBHkmPid6N9RJ6yFaoZPb5mflkbtNcrhcIqczH1ZEnyE1UfMqGo:dkKyxHBEmaY/J6yFTZP92yzLIxbgnXU7
MD5:	C022DCA528E122811414BA401861354B
SHA1:	185035A39224FFB8C456C95EB9FB2A8D2C173694
SHA-256:	49E16EFA204072C5068B83C826F5941C376FFE98222BABAB253DA3F8320CB9D7
SHA-512:	8BC83270EBFEAC31FDF732738C9CD3613E7940F01C28DD1DE967D4E3972FFDFAFA97944FD1BCE176DF4C09996CC334DD7092DA5E435F2F7300E42516D1FD19EC
Malicious:	false
Preview:	5.w.%>.....o.m.rh...@..UFdN. ..=..k.\.....(:...e....v.i.....R .4.4i.)..Q..X.8.....U.....+.,.Hg....Fz..v...iV.....n....?....v...^.$.F.z.....0.t.6V..V..e.....N.....q.F.Ts&_.....H...x.}....r.._c.Z.....(@Q.~..j.. .k..h.S..]X$.....WPB.\o...X....b..V.o....H`E.[...;..O.....y..~]....I...x.....w.1..O.t2.&.87.~./.,{...JV...R....(..C.....yC.X.....5....6.O.0.. d.}P.....V..~...b...{R.1.!.&.z....s{2..=..^w....>...B.ZX9o..a.....)...F7.....4..Y..h.q...#...(d.....ua=D..9.@...+....K~..E....W|#.54..$zR..!.Nt..w"...*..&..I?qA.r.....a.....W.....@e."n.s.^1...Z..G..0.F.$.pu$.....y.....T..N.....=..... ...ml..._.Fr1Z.+.ePv.$.....5.-..@.50.F..8pI.#V#.k..^.....p.-yb^....T%r.....+.9.....*._..)4.@..."...K.B..P..;3.X.c.A...Wh[8...8LI.0.....7.cP..N.b\0.C..{]S.0;A.3..JK..k?...=....;$.>...."B.#.....1....j.'..N.r..6g.....U...I.LT.....Y.....^..ll.]....$..n..X.....V.P.....%.Q...W....z..^.C.....Gt.q.k

C:\Program Files\EnigmaSoft\SpyHunter\data\acpwl.dat

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	59520
Entropy (8bit):	**7.996845650623955**
Encrypted:	**true**
SSDEEP:	1536:iT2cwNpgV1w57Ls0wlFDbxeambZsimilRWFw/1/JIqwjF:iqcOpywVQ0w3dweilRn1/mJ
MD5:	F8294ADDA1A1FDF38BED854604B67A2B
SHA1:	2E1766B3B2A9F2B848F8FF57E68C7F154E95CFC6
SHA-256:	D4A9CEB2B406964D95777D9C2DC46363701D9CC96365C77D4A661FF256969109
SHA-512:	B50C1BB9401C69BB1ED4D0CF3C1731C102618A5D83EAC82AA22F2CC02ADB0B34365CED25BAE695BB05D183C4935A70D6F1335603824BE6FDF5390B6DD0B6FC52
Malicious:	**true**
Preview:	......7.=Hu..'..wo7..&t.F.D. .....u.XDb...H...7..F....9...{....y(..e3.I.Z[?Z.a..a.i.W..n7.,]h.../.[.........B.."5....XI..A%...:.{....(..tUC../.-.._....M....'H.sD.`....zvq.]..."#.n....g.....v.....y&..U.....=..G~..Y.S...Z.[..;...b:..I..LZ<....6.4..J..vxu...Y.h66A._ ...F...V7.ys.&..g$k..yzM...8`L.u.,.....}...P.C~w#4:.....\n....:..k....7V\.....(r&..^...ks...$..aW..X.I.....iuT.....v.I.....0.fi.:...n_...Ef.c.G...0.g...h.O...zb..u...2t...W.6....B.?..~xQ...-...C.h.&...3..^,J.]e..}...6.....;.y4|.}...p>....Q..KM]....?.W.~Y.W.....V.g.s.i^n..n..O4{....:N..j.I...Qh...M.1.-...R.0W..E...KmAs.h.WC.0k.X.4.V..1.a.]..$*B.....P@.Q..C.t..EU.b.HyX.(.K..y<...<..Ya..r..).rq.$...;A.W..P.a(.2.D..N.....0.qg...:...Aos.F3c.....-V.!Mh.6.d.]."..V..6.*Q..=.....@9.....Q.i.u.{.....EK...a.Y.$...O.q.....e.*...G..2.&V.`'.4.....>.....@W.m.D.I\..lgy..5V.~.l.5..y...,...t.B..]+/....D..]...PG.)...=....T.32.R.|.u.W..gr.v.-<..M.....J.

C:\Program Files\EnigmaSoft\SpyHunter\license.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	Unicode text, UTF-8 text, with very long lines (1644), with CRLF line terminators
Category:	dropped
Size (bytes):	107716
Entropy (8bit):	5.2003181449234575
Encrypted:	false
SSDEEP:	3072:FjNLzj07ABLuLmxJJcHj9KIyvLBPjvlXjAjRU0eFljo73FT6TlN5Z7jw769MVDZk:7ZxJJchby6FdT5hgK
MD5:	66507057FFDF4CAF36C3061C80D2D08F
SHA1:	281F661AEA3D9042A1147BC29769537BFADD6219
SHA-256:	A80E70A5E036EAC0C75354D4EE0E4147D606DEBBDDB704435C96CF2DE2C8C777
SHA-512:	B00FABA46CFAE27CFE9B92A5211EFACB315EC98C752EE9E022F1F2D5CDEC12477D228C0CE45ADFBD973C3AAAF50292F53C7A06C8516D96317D674E73B85B5737
Malicious:	false
Preview:	SpyHunter 5 and SpyHunter for Mac - Additional Terms & Conditions....==========....COPYRIGHT NOTICE..... 2017-2022 EnigmaSoft Ltd. All rights reserved.....Third party code may be aggregated or distributed with EnigmaSoft's proprietary and copyrighted software. The copyright notices and license terms for such third party code are detailed below.....==========....SOURCE CODE DISTRIBUTION....Certain third party licenses may require distribution of the corresponding source code. ....You may obtain the complete corresponding source code from us for a period of three years after our last provisioning of this product by sending a money order or check for .5 to:....EnigmaSoft Ltd...Attn: GPL Compliance Offer..1 Castle Street..Dublin D02 XD82..IREL AND....Please write "GPL Compliance Source" in the memo line of your payment. This offer is valid to anyone in receipt of this information.....==========....LIST OF COMPONE

C:\Program Files\EnigmaSoft\SpyHunter\purl.dat

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	128
Entropy (8bit):	6.613204882778696
Encrypted:	false
SSDEEP:	3:1caYq43OVKCoPADbaVotoQISUbuFLS1PN5to3qIm:1cmXQcaVMoQIKxG1L
MD5:	C13C63D7C052C923DCAE07E181EE5F3F
SHA1:	6C7B36F191BF16F1531C4351705117B28DA1C1A9
SHA-256:	A09417F649A518F5171C055BCDAFF7928AD855E9D4921D1373D51499B27262FA
SHA-512:	36766A6C39054E4E32CF63EE9C28512CC3BB927998DA4037DCEFB6C3B988C55046A2B230C85F3AD992D2F27577938DF80F9318FF21B5779AADFFEA56D81253B
Malicious:	false
Preview:	.T....3.?..K.....bn...._k'./...0'.I.....D.....C.7.y..}.V.m. :ec:x.....sg.fb. n%'<.k.D.9">...=....\...k.....w.....V.

C:\ProgramData\EnigmaSoft Limited\sh5_installer.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	6881256
Entropy (8bit):	7.120994762388773
Encrypted:	false
SSDEEP:	98304:Hh/MyJC5zMggmeTN1YBi9MCL8e7Wf7teFSiFMMrFDnl9KMBlcbhHEjZD:HXGAggm48/y8e7Wf7tYFM99HEp
MD5:	2816BACD01B0D8C48F1D8714C6AA6F0F
SHA1:	474AE88D9CF093DCB9789CB7B79513E0DBD38388
SHA-256:	637720BA1437FD6DEA873E56A6A1D7BB3C663E490ABC4E406E3817DD2EB82C4F
SHA-512:	8BC78E625A8BE14DC54185E1CDD63F4CF85B5FDCD32EA532FC00E2F805EF9D241D2B3E89E582779B167113CA7B4DABEE60B56F3EACDF4BDC4B5F56C15C82AC2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....C.o.....X.1....X.....X. ....d.....J.....!.....&.....7.....Rich.....PE..L.....Qc.....dC..L%.....(.....C...@.....i.....#i...@.....Q.T.... U.0\.....h..K..f..D...IN.p.....IN.....pIN.@.....C.H.....text....cC.....dC..... ..`.rdata..D.....C.....hC.....@..@.data.....@R.....R.....@....gfids.....U.....T.....@..@.tls.....U.....T.....@....rsrc...0\... U..^....T.....@..@.reloc...D....f..F...ne.....@..B.....

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\EnigmaSoft\Uninstall.lnk

Process:	C:\Users\user\Desktop\file.exe
File Type:	MS Windows shortcut, Item id list present, Has Description string, Has Relative path, Has Working directory, Has command line arguments, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	699
Entropy (8bit):	3.0819274522482916
Encrypted:	false
SSDEEP:	12:8Ul0g0i/kdjHLolgpROXG62MmolgdqP62ib7olgr3wS:8UlFIvOgXJ7RZ
MD5:	C08C660064F10A88A1276AB26D020D20
SHA1:	75C99ED08455B1A570CDCD95BE856C3249904A11
SHA-256:	31FCA4C6FADB51AADAB22AE9C3E81D7BD85346F42B5DA1825E1C72CD9B3829C9
SHA-512:	F6C07FEBBEFFAAA26966FD882092E35E8B4457E70363E2641442B4B2412E881B0AAB3F75E2D0AC192722F422EC8EB3FF865834898ADBAC2314EF223C75EC90DD
Malicious:	false
Preview:	L.....F.....}....P.O. .:i.....+00.../C:\.....b.1.....ProgramData.H.....P.r.o.g.r.a.m.D.a.t.a.....x.1.....EnigmaSoft Limited..V.....E.n.i.g.m.a.S.o.f.t. .L.i.m.i.t.e.d...".t.2.....sh5_installer.exe.T.....s.h.5._.i.n.s.t.a.l.l.e.r...e.x.e.. .....R.e.m.o.v.e. .S.p.y.H.u.n.t.e.r.3.....\.....\.....\.....\.....\.E.n.i.g.m.a.S.o.f.t. .L.i.m.i.t.e.d.\.s.h.5._.i.n.s.t.a.l.l.e.r...e.x.e.!.C.:\.P.r.o.g.r.a.m.D.a.t.a.\.E.n.i.g.m.a.S.o.f.t. .L.i.m.i.t.e.d...-.r. .s.h.5. .-.l.n.g. .E.N.....

C:\ProgramData\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines (2494), with no line terminators
Category:	dropped
Size (bytes):	2494
Entropy (8bit):	5.252849377001231
Encrypted:	false
SSDEEP:	48:cAn/TLtfGgzmQLeUp/B8H+OaBSkC9+TcR6Ks:pTLtf9zmQR4k6kKs
MD5:	20FDB39B527CAE9749852CF3DCA99993
SHA1:	E400F7EC756C26F962B490510C1124BFED0A666F
SHA-256:	449286F631EF1524C2EE769AE40EA7EC5AB7E63858DBDCBCE48FC3B6F8C1C555
SHA-512:	255BAF621E33C9AA3BF3DA4F775BB82E1359E2639B330C37A6056BEB84B7C78BA5AC20859BEBB45B01876C24317EC5F64A3159E6A5840428D32D61944E13A6EA
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService dataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataType="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399969272148706</FirstScanAttemptTime><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399969272304939</LastMeteredScanTime><LastScanAttemptTime dataType="21">132399969272148706</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType="21">133051593686244000</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines (2494), with no line terminators
Category:	modified
Size (bytes):	2494

Entropy (8bit):	5.252849377001231
Encrypted:	false
SSDEEP:	48:cAn/TLtfGgzmQLeUp/B8H+OaBSkC9+TcR6Ks:pTLtf9zmQR4k6kKs
MD5:	20FDB39B527CAE9749852CF3DCA99993
SHA1:	E400F7EC756C26F962B490510C1124BFED0A666F
SHA-256:	449286F631EF1524C2EE769AE40EA7EC5AB7E63858DBDCBCE48FC3B6F8C1C555
SHA-512:	255BAF621E33C9AA3BF3DA4F775BB82E1359E2639B330C37A6056BEB84B7C78BA5AC20859BEBB45B01876C24317EC5F64A3159E6A5840428D32D61944E13A6EA
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService dataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataType="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399969272148706</FirstScanAttemptTime><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399969272304939</LastMeteredScanTime><LastScanAttemptTime dataType="21">132399969272148706</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType="21">133051593686244000</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__0.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	369512
Entropy (8bit):	6.2987418401396384
Encrypted:	false
SSDEEP:	6144:cVRijf0pLl3/W5FBNoRIa9G+iLBZ0OSxqxu1GUhH++Lf1M131s4E:PTkLl3/W5FBNoOac+pxqM1Lhe+pjX
MD5:	EDCE372DE488AA221DA7DB7544C09B3E
SHA1:	E684BE09C22E93B12AF9F78508E5422B83CBE0FC
SHA-256:	DBC0B0AFEAE1E33F3F8FA2384BBBFD2F787ACA1C75BF2E5372812B3DA33A7EFE
SHA-512:	89A21C8C4D4963B02E36CD887B071B866CEBAFC1F8E04AAB6CF043746AADB37799644E41FA3B1DDB1E297593B0035693E151B9B5ECF95041E0796BF47174E6E1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y...8s..8s..8s..j...8s..@.8s..@...8s..@..8s..@...8s..@.8s..8r.J8s..@...8s..@.8s..@.8s.Rich.8s.....PE..d...y.4\.....".....|.....H.....@.....V.....@.....d.....h.....h:...n..h5.....H.....\..(.....h.....text...,..... ..`.rdata..T.....@..@.data...0.....,.....@....pdata..h:.....<.....@..@.tls.....R.....@....rsrc...h.....T.....@..@.reloc.....`.....@..B.....

C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__1.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	369512
Entropy (8bit):	6.2987418401396384
Encrypted:	false
SSDEEP:	6144:cVRijf0pLl3/W5FBNoRIa9G+iLBZ0OSxqxu1GUhH++Lf1M131s4E:PTkLl3/W5FBNoOac+pxqM1Lhe+pjX
MD5:	EDCE372DE488AA221DA7DB7544C09B3E
SHA1:	E684BE09C22E93B12AF9F78508E5422B83CBE0FC
SHA-256:	DBC0B0AFEAE1E33F3F8FA2384BBBFD2F787ACA1C75BF2E5372812B3DA33A7EFE
SHA-512:	89A21C8C4D4963B02E36CD887B071B866CEBAFC1F8E04AAB6CF043746AADB37799644E41FA3B1DDB1E297593B0035693E151B9B5ECF95041E0796BF47174E6E1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y...8s..8s..8s..j...8s..@.8s..@...8s..@..8s..@...8s..@.8s..8r.J8s..@...8s..@.8s..@.8s.Rich.8s.....PE..d...y.4\.....".....|.....H.....@.....V.....@.....d.....h.....h:...n..h5.....H.....\..(.....h.....text...,..... ..`.rdata..T.....@..@.data...0.....,.....@....pdata..h:.....<.....@..@.tls.....R.....@....rsrc...h.....T.....@..@.reloc.....`.....@..B.....

C:\Users\user\AppData\Local\Temp\esg_setup.log

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	modified
Size (bytes):	64482

Entropy (8bit):	3.6903364002980066
Encrypted:	false
SSDEEP:	1536:X5AKcAVmmsReFuYuuplhkKOMjNSUUyKGu8dhEvoqwbt7SLPsKa5LUkBRx0WKiOxL:Jm
MD5:	F21C271ECED0E1CD2EE569E956C4EF70
SHA1:	B8302FE4A7390D8024FDB227CDD34ED495808E47
SHA-256:	DA16C8670DD4476CCC03158230E47E70960BCC8A3F09B4D566F199BC2915FAD1
SHA-512:	1595AFF765C92C4365300F2971FFF89A6A57D501B2CF28189E9F04C406500CA2B14D50A0E5D73EE15675993637FECECF11195EC2EF16401EB69CBB7682A5B313
Malicious:	false
Preview:	[.1.].[.0.8.:.1.4.:.2.9...7.4.2.].[.0.0.5.2.3.6.]. .(.2.9.3.). .I.n.s.t.a.l.l.e.r. .3...0...8.1.9...5.0.5.0. .(.0.7.0.8.4.9.6. .:. .4.d.d.d.8.7.2.4.). .i.n.i.t.........[.1.].[.0.8.:.1.4.:.2.9...7.8.9.].[.0.0.5.2.3.6.]. .(.2.9.6.). .H.W.I.D.[.4.3.1.7.7.b.1.f.9.0.4.4.f.0.3.a.6.6.5.7.5.c.a.f.3.e.b.9.e.0.0.6.]. .H.a.s.h.:.[.2.8.1.6.b.a.c.d.0.1.b.0.d.8.c.4.8.f.1.d.8.7.1.4.c.6.a.a.6.f.0.f.].....[.1.].[.0.8.:.1.4.:.2.9...7.8.9.].[.0.0.5.2.3.6.]. .(.2.9.9.). .O.S. .v.e.r.s.i.o.n.:. .W.i.n.d.o.w.s. .1.0. .P.r.o.,. .1.0...0...0...0...1.7.1.3.4.,. .6.4.b.i.t. .=. .1.....[.1.].[.0.8.:.1.4.:.2.9...7.8.9.].[.0.0.5.2.3.6.]. .(.3.0.4.). .A.r.g.s.:. .8.3.8.8.8.9.3.....[.1.].[.0.8.:.1.4.:.3.1...0.3.9.].[.0.0.3.5.2.0.]. .(.3.2.3.). .[.s.h.5.]. .5...1.3...1.5...8.1. .(.W.e.b.).....[.0.].[.0.8.:.1.4.:.3.1...6.3.3.].[.0.0.3.5.2.0.]. .(.5.2.). .F.i.l.e. .R.C. .r.e.g.i.s.t.e.r.e.d.[.1.].[.5.0.8.4.8.].[.9.7.6.c.b.0.0.8.b.4.9.0.2.c.a.8.f.7.b.0.f.a.f.d.6.7.c.c.8.d.7.f.].:. ./.s.h.5./.a.l.b.a.n.i.a.n...l.n.g.....

C:\Windows\Logs\waasmedic\waasmedic.20221130_081446_547.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.736344290343422
Encrypted:	false
SSDEEP:	48:j1Rr52UBmb7kUYb7kEyb7klnb7kdb7kbIl9lvb7k0tpl3b7kSb7klb7kwDb7k9O:52Uw0UY0F0h0d0U9R0Cl30S0l0A09O
MD5:	3EF309A9EE17AE9D3922E7FD37AC6B0C
SHA1:	5288E02BAE015066BD153FB5CBE78C6F1489455F
SHA-256:	557AD0B3B40823C2A4523252E8825DA816B0A7844180B17D52DA7BC916CB7EEE
SHA-512:	30318705D2175F4BBA6011FA08A608C8A648B949F07E7951F403F2524E86E8D0D28FCCC8AB4B75C0CC8577385EBAAEA5A712C949A755F5185773A66A604175F0
Malicious:	false
Preview:	....!..........................x.......F......................B.......y.....Zb....... ....@.t.z.r.e.s...d.l.l.,.-.2.1.2.. ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..WW...... .....w..............E.C.C.B.1.7.5.F.-.1.E.B.2.-.4.3.D.A.-.B.F.B.5.-.A.8.D.5.8.A.4.0.A.4.D.7...C.:.\.W.i.n.d.o.w.s.\.l.o.g.s.\.w.a.a.s.m.e.d.i.c.\.w.a.a.s.m.e.d.i.c...2.0.2.2.1.1.3.0._.0.8.1.4.4.6._.5.4.7...e.t.l............P.P.x.......F..9.B.F. .....17134.1.amd64fre.rs4_release.180410-1804...........5.@.F......OYo."(.s..O........WaaSMedicSvc.pdb... ....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	10874
Entropy (8bit):	3.166085046821439
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z5+6I3+zJ9+i:j+s+v+b+P+m+0+Q+q+q+73+zj+i
MD5:	9658A663F2DFBC67E0B56BEFC1C7594F
SHA1:	6E1255D582A2F94F7DE4C4E2D7F18C55D9728A85
SHA-256:	DB8E1DE3403925115F4653FA8F125F7C6F0B69714F45E735E32DD170E91737CC
SHA-512:	04B62023F203E363080EC3E57391C52AEC454D3F2C24C6C588BC1DDFBBC2EFEA5896E30ACAC0DCD4778B422C059D84BBF73AA52EADCA510DB4D55FA8A7C5 C803
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

C:\Windows\System32\drivers\EnigmaFileMonDriver.sys

Process:	C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83992
Entropy (8bit):	6.272239054005574
Encrypted:	false
SSDEEP:	1536:dg3dQYWSNxlINp9BNsrxwpu0jV0IWsyAtZZKltYdjxzzs:dg3dQYWaxmNNNsD0jGIWs33oltu0
MD5:	6BED4CEE4117F47E2EF797DA56935C04
SHA1:	34EBF65A197F4BD8FFFE891130A0B0CB903F75F6

SHA-256:	0BF9F7247339C1676F6F59EE4647A6266DAEFA74CA00C7F1ED608BDC3A0EF693
SHA-512:	8FAF611DCE276B4877463847248BC7A4F41AA1032C679DE55F650536858993C9EC4A8B834017C0C23A5D20E7EFB0EB63AADCF94B1DF49BD2541413F4448F1EA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PG.i.&.:.&.:.&.:.T.;.&.:.T.;.&.:.T.;.&.:.&.:g&.:.S.;.&.:.S&:.&.:.S.;.&.: Rich.&.:.....PE..d...d].b.....".....8.....l.....@.....t....A.....K..P....`.....  ...(...p.....p...8..... .....8.....text.....  ..h.rdata..$.....@..H.data.....@....pdata.....@..HPAGE.....!.... ...".....  ..`INIT....N....@..... ..b.rsrc.....`.....@..B.reloc.....p.....@..B.....

C:\sh5ldr\initrd.gz

Process:	C:\Users\user\Desktop\file.exe
File Type:	gzip compressed data, was "newinitrd", last modified: Fri Feb 9 17:19:34 2018, from Unix, original size modulo 2^32 4180998130
Category:	dropped
Size (bytes):	1048576
Entropy (8bit):	**7.9952417172698125**
Encrypted:	**true**
SSDEEP:	12288:M6bKggdUNSAChsS7CalpLtMGclsPz0Nvn8WCOrkct9ces20Y8/EiaDrsnLr3PN1U:bKgoU0N2lw0KWhkcDce2uYfmjr
MD5:	356054D8D017B1CD5C7130D30ACB1FAA
SHA1:	536BF38B34297D48D24A0DD58A9C20E3DCD9CB69
SHA-256:	2F9A0353058B4F0A11B531819A48D85CEF0D8B343F33910D77EE33549F3DE857
SHA-512:	FC99CDCFE0B115A3ED388C116E7C6360FCEBA372EAEDA63DA91FD8451645BF8B41828D6C902E131D13C6DA98DF2A5E6A990B7C3C5E310AE7F520E74CCB7CB489
Malicious:	**true**
Preview:	....&.}Z..newinitrd..Z{p\Wy?.7..y..)....D.-iwe).K.....$.QY...{W...n.+Y....&...v`...1..04.i..v.Ny.Q.B..3!...fj&.....{%..C..j..~.{..u...Yg....e.....,>}..a..F.7...`.....s}..O.....~....|..j..... ..7...?.._....h...q.....u.9..3.Jn^..!.....?.co..y....L...1o.#78x...#...L...v.[7.{A.L!6..5....f.C.S.g.....3..W...2.[..@.....LY..B.(....d%o.....S"...:.... .p.....{zl.k.3M.`Q..]r.HCw0}.....; ...l8...A..*N..X...J>iG...A9f:..Y.T.!.....13.....s$..FI..P.9.B....K.0.S,...X.V...ul.#k.$..I.Ll..ul.....K.a..[.5...E.X.{...@+...~p..i98.|dprrpb..]....l....d..E..a..;..T...F&.>.....}..A.9 :>=125%G.O.Ay`prz|..}.....Fz..2I).....G....n.}e.c....yi..&.j.....^O..3.Id!h...%.t.K.z6..).Z....C^..Hw.....1j. ~..^..r.....\.....S.=I..z....N....9..L.....B.W.j...3y,.:.e.M.....tG...m. ..2..:..0pFv..`.:%gw..N.....k....).5x..FR!.....M...V2.0E.....\..`'Cu.....].....M.X..:d..,j..\.4.LA.LI.^6!.UY.R(.).]....T....M.<o.S..u..lg^V.H0r

C:\sh5ldr\shldr

Process:	C:\Users\user\Desktop\file.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	270476
Entropy (8bit):	6.649640171668803
Encrypted:	false
SSDEEP:	6144:AHvZF0wXVHGMvtxkRhmB2xB4+AINF4/KaigfHvU:AHv4MiiB2xB4+A1Ki/s
MD5:	D4FBD43D0BA1237AC37545E278D0414B
SHA1:	55E05CE5F96B9891547E6248BC6972847271707A
SHA-256:	1D458FE14A87DA3249766163996359A2BCEF33ECEE15501A52A81F8B03FE04BA
SHA-512:	ED084E82A7AB6280C724AA40A45E603AC66F11A2662093F299CDBD07FB7C20FE90573F9E4E69607F48896DF83A59234A3DF2634A3AF171CEBFA862B8C2B53ED6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	.>.. 9.....1.....[..K.....Sj[...A..f.>.....y.f.>..X..u..@.h. .....K.....QS..[Yr.....1.1.....f.GRU.f9.u..... ..f9.uJ.r;.....$?t.....h. ..1.`.2.as.`1..).aOu...y.w/.....r.w...1.....1.....RVWU...]_^Z.....f`.....`.. ....".....f1.f1.f..$...f.....$.."....1.V..|W..V.....f..... ....fa...h.....<.u....Missing helper.....X.. ...P....r0.>..U.u(.....Kj@.....;.f1.1..D..u.8T.u.f.D.E.s.....[.....".....1.1...f.t<..t.1.f1.f@u.....U....f.....D... .\.f.D.f.D.....f`.B._.fa.fP.[...f@.....fXf.>X.....u.....[.....S.....Q.....u.9.t... .r;.....1.1.....h1..... ...1.1.....Ku..+....p.. x.....-....-....Ku..1.....f1.6..f..... .N.....1.... ...../menu.lst.....

C:\sh5ldr\shldr.mbr

Process:	C:\Users\user\Desktop\file.exe
File Type:	DOS/MBR boot sector
Category:	dropped
Size (bytes):	9216
Entropy (8bit):	6.64401103615787
Encrypted:	false
SSDEEP:	192:19tH9JfvwQkeDDL1IjmK2YbfknoZusHC1jIKYBSZV:TTJf4QxDiCK2QknyHHC1jIKYBSn
MD5:	2B0B4E8E51E7B754A9E3F086BBC1D98C
SHA1:	CC133E92C2206552D7C0BD6DC77811FEB45431B1
SHA-256:	8F6293B3DD067EFE6AD19CD5CB9201871FA3AE865F55D23DC5A1BF428BC4C5E0
SHA-512:	26771424BADF099614554113E1525DB3B5522B95540E34A1EED15FA5E0955CD5B6655F1A5B00F233F37CA91C7BB3658C6FEADFD67744A663909ED2322D426084

Malicious:	false
Preview:	.^.. 9.....1.....[..k.....Sj}.h. .....K.....QS..[Yr.....1.1.....f..M.f9.u..9..... ..f9.t(f`.....s.u.faf9.uM.....&....r3 .....$?t.....h...1..K.s.u...\.....r.w...1....1.....M.....RVWU...]_^Z..... ....fa....`PSQ.....Y[Xr...u.as.`1...aO.....<.u....Missing MBR-helper..... .....U..... .....

C:\sh5ldr\vmlinuz

Process:	C:\Users\user\Desktop\file.exe
File Type:	Linux kernel x86 boot executable bzImage, version 3.18.5ESGi (enigma@enigma-mindo-xdev) #3 SMP Wed Feb 4 13:13:25 EET 2015, RO-rootFS, swap_dev 0X2, N ormal VGA
Category:	dropped
Size (bytes):	1048576
Entropy (8bit):	**7.998369627630954**
Encrypted:	**true**
SSDEEP:	24576:iANSKABQg2hQTjn83uRq5E8p5g5GSfWatSU/alzP/eg:FAehQTz8U2Jp7Sfb/awg
MD5:	EE6BEB0699A62B528A6927A13672E1A2
SHA1:	5E47E0D14246ED311BB8CE774426898A53E8DFE8
SHA-256:	87AA518948A8BE0BCAAB8E9694E29EDE2AD87D4742A5B702F35014D91EB31A7D
SHA-512:	5617275FE4920F387A48BF4C8DB1A40CBE291E9B8F76558D6996B9865E8205D44A517A5BB009BF6E873EF0453AE8F4260476CC1506720D973A817E01CB6495AC
Malicious:	**true**
Preview:	.....1....-.. .t.....1.....Use a boot loader....Remove disk and press any key to reboot..... .....c. .....U..fHdrS.....1.....P.....y.....'.....m.....9..t...P.....t...$.....s.1...u.....f.....h...f.>.=U.ZZu...=..Pf1.).....f.f..+..f.....f.....8...t.....f.....f`..,.. ....f.fa.....f...f.....f`.f.....g.|$D!.t.....f...,fa....f.f.fVfSf..4f..f...u.f.....f.....gf.D$.f.!...g.D$...g.D$...g.D$!.g.\$ f1.gf.T$.f.....f.J...f...Pf..t!f.....gf.Q.. u.fNt....f...f....f..4f[f^f.fSf...f..gf.....t .fCf.Z.....f...f[f..No setu

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.120994762388773
TrID:	• Win32 Executable (generic) a (10002005/4) 98.81% • Windows ActiveX control (116523/4) 1.15% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	6881256
MD5:	2816bacd01b0d8c48f1d8714c6aa6f0f
SHA1:	474ae88d9cf093dcb9789cb7b79513e0dbd38388
SHA256:	637720ba1437fd6dea873e56a6a1d7bb3c663e490abc4e406e3817dd2eb82c4f
SHA512:	8bc78e625a8be14dc54185e1cdd63f4cf85b5fdcd32ea532fc00e2f805ef9d241d2b3e89e582779b167113ca7b4dabee60b56f3eacdf4bdc4b5f56c15c823ac2
SSDEEP:	98304:Hh/MyJC5zMggmeTN1YBi9MCL8e7Wf7teFSiFMMrFDnl9KMBlcbhHEjZD:HXGAggm48/y8e7Wf7tYFM99HEp
TLSH:	D666DF12B641C171E5A302B2997EAFBF987CED200B2458C7E3D45E7D4E702E26637B52
File Content Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....C.o.....X..1....X.....X.. ....d.....J.....!.....&.....7.....

File Icon

Icon Hash:	f8b6b45971a6ee70

Static PE Info

General

Entrypoint:	0x68a7d4
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x63510DF3 [Thu Oct 20 08:59:31 2022 UTC]
TLS Callbacks:	0x689cd0
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fa3740f07f6d2725edcaa42e6d766d63

Authenticode Signature	
Signature Valid:	**true**
Signature Issuer:	CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 6/18/2020 5:00:00 PM 6/13/2023 5:00:00 AM
Subject Chain	• CN=EnigmaSoft Limited, O=EnigmaSoft Limited, L=Dublin, C=IE, SERIALNUMBER=597114, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=IE
Version:	3
Thumbprint MD5:	C1CA2DE9B1FC80CB6991C5E96BFDBB56
Thumbprint SHA-1:	9B7616BF6F93FFDEB04A6998A944512C1C753015
Thumbprint SHA-256:	5F5216C99F6851AC1FF36BECDE318E5ECF54222D051E2D4EB142165657C7630F
Serial:	0D52114AABA1B5E4B4B1ACE58C319E4E

Entrypoint Preview
Instruction
call 00007FB4ACAECBB5h
jmp 00007FB4ACAEBD03h
int3
int3
push ecx
lea ecx, dword ptr [esp+04h]
sub ecx, eax
sbb eax, eax
not eax
and ecx, eax
mov eax, esp
and eax, FFFFF000h
cmp ecx, eax
jc 00007FB4ACAEBE7Eh
mov eax, ecx
pop ecx
xchg eax, esp
mov eax, dword ptr [eax]
mov dword ptr [esp], eax
ret
sub eax, 00001000h
test dword ptr [eax], eax
jmp 00007FB4ACAEBE59h
int3
int3
int3
push ecx
lea ecx, dword ptr [esp+08h]
sub ecx, eax
and ecx, 0Fh
add eax, ecx

Instruction
sbb ecx, ecx
or eax, ecx
pop ecx
jmp 00007FB4ACAEBE2Fh
push ecx
lea ecx, dword ptr [esp+08h]
sub ecx, eax
and ecx, 07h
add eax, ecx
sbb ecx, ecx
or eax, ecx
pop ecx
jmp 00007FB4ACAEBE19h
int3
int3
int3
int3
push esi
mov eax, dword ptr [esp+14h]
or eax, eax
jne 00007FB4ACAEBE9Ah
mov ecx, dword ptr [esp+10h]
mov eax, dword ptr [esp+0Ch]
xor edx, edx
div ecx
mov ebx, eax
mov eax, dword ptr [esp+08h]
div ecx
mov esi, eax
mov eax, ebx
mul dword ptr [esp+10h]
mov ecx, eax
mov eax, esi
mul dword ptr [esp+10h]
add edx, ecx
jmp 00007FB4ACAEBEB9h
mov ecx, eax
mov ebx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
mov eax, dword ptr [esp+08h]
shr ecx, 1
rcr ebx, 1
shr edx, 1
rcr eax, 1
or ecx, ecx
jne 00007FB4ACAEBE66h
div ebx
mov esi, eax
mul dword ptr [esp+14h]
mov ecx, eax
mov eax, dword ptr [esp+10h]
mul esi

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x51fda0	0x154	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x552000	0x115c30	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x68b400	0x4be8	.reloc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x668000	0x344b0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x4e6c00	0x70	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x4e6ccc	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4e6c70	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x438000	0x948	.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	0x4363cc	0x436400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x438000	0xeb144	0xeb200	False	0.41603846856725146	data	5.84204624071673	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x524000	0x2bee1	0x1ea00	False	0.12552614795918368	Matlab v4 mat-file (little endian) \334, rows 8, columns 8, imaginary	4.35694874016997	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.gfids	0x550000	0x9b8	0xa00	False	0.3890625	data	4.1212839696841	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0x551000	0x9	0x200	False	0.033203125	data	0.020393135236084953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x552000	0x115c30	0x115e00	False	0.9782669815564552	data	7.982123610094004	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x668000	0x344b0	0x34600	False	0.6026486053102625	data	6.676291391323307	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x553ff0	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0x554658	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x554940	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_ICON	0x554a68	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x555910	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x5561b8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States
RT_ICON	0x556720	0x9a5e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x560180	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x562728	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x5637d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x563c38	0x34	data	English	United States
RT_DIALOG	0x563c6c	0x34	data	English	United States
RT_DIALOG	0x563ca0	0x34	data	English	United States
RT_DIALOG	0x563cd4	0x34	data	English	United States
RT_RCDATA	0x563d08	0x60	data	English	United States
RT_RCDATA	0x563d68	0x480	data	English	United States
RT_RCDATA	0x5641e8	0x60	data	English	United States
RT_RCDATA	0x564248	0x3b60	data	English	United States
RT_RCDATA	0x567da8	0x37c0	data	English	United States
RT_RCDATA	0x56b568	0x38e0	data	English	United States
RT_RCDATA	0x56ee48	0x3b80	data	English	United States
RT_RCDATA	0x5729c8	0x39c0	data	English	United States
RT_RCDATA	0x576388	0x3d40	data	English	United States
RT_RCDATA	0x57a0c8	0x4180	data	English	United States
RT_RCDATA	0x57e248	0x6960	data	English	United States
RT_RCDATA	0x584ba8	0x3dc0	data	English	United States
RT_RCDATA	0x588968	0x41c0	data	English	United States
RT_RCDATA	0x58cb28	0x3c00	data	English	United States
RT_RCDATA	0x590728	0x5fe	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x590d28	0xa0	data	English	United States
RT_RCDATA	0x590dc8	0x7c0	data	English	United States
RT_RCDATA	0x591588	0x340	data	English	United States
RT_RCDATA	0x5918c8	0x18fa0	data	English	United States
RT_RCDATA	0x5aa868	0x7a0	data	English	United States
RT_RCDATA	0x5ab008	0x2e0	data	English	United States
RT_RCDATA	0x5ab2e8	0x260	data	English	United States
RT_RCDATA	0x5ab548	0x280	data	English	United States
RT_RCDATA	0x5ab7c8	0x360	data	English	United States
RT_RCDATA	0x5abb28	0x240	data	English	United States
RT_RCDATA	0x5abd68	0x280	data	English	United States
RT_RCDATA	0x5abfe8	0x260	data	English	United States
RT_RCDATA	0x5ac248	0x2a0	data	English	United States
RT_RCDATA	0x5ac4e8	0xf3e0	data	English	United States
RT_RCDATA	0x5bb8c8	0xa40	data	English	United States
RT_RCDATA	0x5bc308	0x280	data	English	United States
RT_RCDATA	0x5bc588	0x2c0	data	English	United States
RT_RCDATA	0x5bc848	0x280	data	English	United States
RT_RCDATA	0x5bcac8	0x280	data	English	United States
RT_RCDATA	0x5bcd48	0x360	data	English	United States
RT_RCDATA	0x5bd0a8	0x2a0	data	English	United States
RT_RCDATA	0x5bd348	0x2c0	data	English	United States
RT_RCDATA	0x5bd608	0x260	data	English	United States
RT_RCDATA	0x5bd868	0x280	data	English	United States
RT_RCDATA	0x5bdae8	0x520	data	English	United States
RT_RCDATA	0x5be008	0x2c0	data	English	United States
RT_RCDATA	0x5be2c8	0x280	data	English	United States
RT_RCDATA	0x5be548	0x2a0	data	English	United States
RT_RCDATA	0x5be7e8	0x2a0	data	English	United States
RT_RCDATA	0x5bea88	0x360	data	English	United States
RT_RCDATA	0x5bede8	0x140	data	English	United States
RT_RCDATA	0x5bef28	0x2a0	data	English	United States
RT_RCDATA	0x5bf1c8	0x2a0	data	English	United States
RT_RCDATA	0x5bf468	0x2a0	data	English	United States
RT_RCDATA	0x5bf708	0x260	data	English	United States
RT_RCDATA	0x5bf968	0xd460	data	English	United States
RT_RCDATA	0x5ccdc8	0x2a0	data	English	United States
RT_RCDATA	0x5cd068	0x340	data	English	United States
RT_RCDATA	0x5cd3a8	0x2c0	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x5cd668	0x2c0	data	English	United States
RT_RCDATA	0x5cd928	0x22180	data	English	United States
RT_RCDATA	0x5efaa8	0x221a0	data	English	United States
RT_RCDATA	0x611c48	0x27000	data	English	United States
RT_RCDATA	0x638c48	0xc20	data	English	United States
RT_RCDATA	0x639868	0xd20	data	English	United States
RT_RCDATA	0x63a588	0xd80	data	English	United States
RT_RCDATA	0x63b308	0xc80	data	English	United States
RT_RCDATA	0x63bf88	0xca0	data	English	United States
RT_RCDATA	0x63cc28	0xcc0	data	English	United States
RT_RCDATA	0x63d8e8	0xd00	data	English	United States
RT_RCDATA	0x63e5e8	0xd60	data	English	United States
RT_RCDATA	0x63f348	0xca0	data	English	United States
RT_RCDATA	0x63ffe8	0xc60	data	English	United States
RT_RCDATA	0x640c48	0xcc0	data	English	United States
RT_RCDATA	0x641908	0xf40	data	English	United States
RT_RCDATA	0x642848	0xd60	data	English	United States
RT_RCDATA	0x6435a8	0xca0	data	English	United States
RT_RCDATA	0x644248	0xe40	data	English	United States
RT_RCDATA	0x645088	0xca0	data	English	United States
RT_RCDATA	0x645d28	0xca0	data	English	United States
RT_RCDATA	0x6469c8	0xca0	data	English	United States
RT_RCDATA	0x647668	0xd20	data	English	United States
RT_RCDATA	0x648388	0xfe0	data	English	United States
RT_RCDATA	0x649368	0xc20	data	English	United States
RT_RCDATA	0x649f88	0xd20	data	English	United States
RT_RCDATA	0x64aca8	0xd20	data	English	United States
RT_RCDATA	0x64b9c8	0xc40	data	English	United States
RT_RCDATA	0x64c608	0xd40	data	English	United States
RT_RCDATA	0x64d348	0xd40	data	English	United States
RT_RCDATA	0x64e088	0xee0	data	English	United States
RT_RCDATA	0x64ef68	0xd20	data	English	United States
RT_RCDATA	0x64fc88	0xd40	data	English	United States
RT_RCDATA	0x6509c8	0xe60	data	English	United States
RT_RCDATA	0x651828	0xd00	data	English	United States
RT_RCDATA	0x652528	0xbc0	data	English	United States
RT_RCDATA	0x6530e8	0x840	data	English	United States
RT_RCDATA	0x653928	0x80	data	English	United States
RT_RCDATA	0x6539a8	0x760	data	English	United States
RT_RCDATA	0x654108	0x820	data	English	United States
RT_RCDATA	0x654928	0x940	OpenPGP Public Key	English	United States
RT_RCDATA	0x655268	0xac0	data	English	United States
RT_RCDATA	0x655d28	0x1060	data	English	United States
RT_RCDATA	0x656d88	0xac0	data	English	United States
RT_RCDATA	0x657848	0x920	data	English	United States
RT_RCDATA	0x658168	0xaa0	data	English	United States
RT_RCDATA	0x658c08	0x7a0	data	English	United States
RT_RCDATA	0x6593a8	0x820	data	English	United States
RT_RCDATA	0x659bc8	0x8a0	OpenPGP Public Key	English	United States
RT_RCDATA	0x65a468	0x8c0	data	English	United States
RT_RCDATA	0x65ad28	0x16c0	data	English	United States
RT_RCDATA	0x65c3e8	0x7c00	data	English	United States
RT_RCDATA	0x663fe8	0xa0	data	English	United States
RT_RCDATA	0x664088	0xa0	data	English	United States
RT_RCDATA	0x664128	0xa0	data	English	United States
RT_RCDATA	0x6641c8	0x2c0	data	English	United States
RT_RCDATA	0x664488	0x460	data	English	United States
RT_RCDATA	0x6648e8	0x2e0	data	English	United States
RT_RCDATA	0x664bc8	0xc20	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x6657e8	0x19e	PNG image data, 15 x 60, 8-bit gray+alpha, non-interlaced	English	United States
RT_RCDATA	0x665988	0x28c	PNG image data, 30 x 120, 8-bit gray+alpha, non-interlaced	English	United States
RT_RCDATA	0x665c14	0x31d	PNG image data, 30 x 180, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x665f34	0x31d	PNG image data, 30 x 180, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x666254	0x5cf	PNG image data, 30 x 180, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x666824	0x5cf	PNG image data, 30 x 180, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x666df4	0xe9	PNG image data, 15 x 60, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x666ee0	0x152	PNG image data, 30 x 120, 8-bit/color RGBA, non-interlaced	English	United States
RT_GROUP_ICON	0x667034	0x92	data	English	United States
RT_VERSION	0x6670c8	0x348	data	English	United States
RT_MANIFEST	0x667410	0x820	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (2020), with CRLF line terminators	English	United States

Imports

DLL	Import
gdiplus.dll	GdipCreatePath, GdipCreateRegion, GdipSetClipRegion, GdipSetInfinite, GdipGetClip, GdipDeleteRegion, GdipDeleteGraphics, GdipGetImageHeight, GdipCreateFromHDC, GdiplusShutdown, GdiplusStartup, GdipImageRotateFlip, GdipGetImagePixelFormat, GdipCreateHBITMAPFromBitmap, GdipCreateBitmapFromResource, GdipCreateBitmapFromStream, GdipClosePathFigure, GdipAddPathArcI, GdipResetPath, GdipDeletePen, GdipDrawPath, GdipSetPenDashStyle, GdipCreatePen1, GdipSetPixelOffsetMode, GdipSetInterpolationMode, GdipSetCompositingQuality, GdipSetCompositingMode, GdipFillRectangleI, GdipDeleteBrush, GdipCreateTextureIAI, GdipSetImageAttributesColorKeys, GdipSetImageAttributesWrapMode, GdipDrawImagePointRectI, GdipGetImageGraphicsContext, GdipCreateBitmapFromScan0, GdipDrawImageRectRectI, GdipDisposeImage, GdipCloneImage, GdipAlloc, GdipFree, GdipCreateBitmapFromHBITMAP, GdipSetImageAttributesColorMatrix, GdipDisposeImageAttributes, GdipCreateImageAttributes, GdipDeletePath, GdipCombineRegionPath, GdipSetSmoothingMode, GdipGetImageWidth
USP10.dll	ScriptStringAnalyse, ScriptStringOut, ScriptStringGetLogicalWidths, ScriptStringGetOrder, ScriptStringXtoCP, ScriptString_pSize, ScriptString_pcOutChars, ScriptStringFree, ScriptString_pLogAttr, ScriptStringCPtoX
CRYPT32.dll	CryptDecodeObject, CryptMsgClose, CryptQueryObject, CryptMsgGetParam, CertGetNameStringW, CryptHashCertificate, CertGetCertificateContextProperty, CertCloseStore, CertEnumCertificatesInStore, CertOpenSystemStoreW, CertFreeCertificateContext, CertGetEnhancedKeyUsage, CertGetIntendedKeyUsage, CertDuplicateCertificateContext, CertFindCertificateInStore, CertOpenStore
VERSION.dll	GetFileVersionInfoW, VerQueryValueW, GetFileVersionInfoSizeW
WS2_32.dll	WSAIoctl, closesocket, WSASetLastError, getpeername, getsockname, socket, ntohs, connect, getsockopt, htons, setsockopt, send, recvfrom, listen, accept, bind, shutdown, getaddrinfo, htonl, gethostname, recv, WSAGetLastError, WSACloseEvent, WSACreateEvent, WSAEventSelect, WSAResetEvent, WSAWaitForMultipleEvents, WSAEnumNetworkEvents, WSACleanup, WSAStartup, select, __WSAFDIsSet, ioctlsocket, freeaddrinfo, getnameinfo, sendto
PSAPI.DLL	GetProcessMemoryInfo, GetModuleFileNameExW, EnumProcessModules, GetProcessImageFileNameW

DLL	Import
KERNEL32.dll	CreateEventA, GetLastError, MoveFileExW, InitializeCriticalSectionAndSpinCount, RaiseException, DecodePointer, DeleteCriticalSection, DeleteFileW, Sleep, GetCurrentProcess, SetLastError, EnterCriticalSection, LeaveCriticalSection, GetCurrentThreadId, GetTickCount, CreateFileW, HeapFree, QueryPerformanceFrequency, GetProcessHeap, lstrcmpiW, QueryPerformanceCounter, FindResourceW, GetUserDefaultLCID, GetDiskFreeSpaceExW, LoadLibraryW, HeapAlloc, GetProcAddress, CreateMutexW, WaitForSingleObject, ReleaseMutex, GetCurrentProcessId, GetLocalTime, ReadFile, GetFileSizeEx, WriteFile, RemoveDirectoryW, GetFileAttributesW, SetFileAttributesW, GetExitCodeProcess, EnumResourceNamesW, SizeofResource, InterlockedDecrement, GetModuleFileNameW, MultiByteToWideChar, LoadResource, GetModuleHandleW, InterlockedIncrement, SetDllDirectoryW, LoadLibraryExW, FreeLibrary, FileTimeToSystemTime, SystemTimeToFileTime, TerminateProcess, OpenProcess, OpenMutexW, GetSystemDirectoryW, SleepEx, InitializeCriticalSection, WideCharToMultiByte, VerSetConditionMask, VerifyVersionInfoW, FormatMessageW, GetEnvironmentVariableA, GetStdHandle, WaitForMultipleObjects, PeekNamedPipe, GetFileType, CompareFileTime, GetSystemTimeAsFileTime, GetEnvironmentVariableW, GetConsoleMode, SetConsoleMode, ReadConsoleA, ReadConsoleW, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetModuleHandleExW, SwitchToFiber, DeleteFiber, CreateFiber, LoadLibraryA, ConvertFiberToThread, ConvertThreadToFiber, FindClose, FindFirstFileW, FindNextFileW, GetSystemTime, WaitForSingleObjectEx, MulDiv, ExpandEnvironmentStringsW, GetLongPathNameW, CreateDirectoryW, CopyFileW, DeviceIoControl, LocalFree, GetSystemInfo, GetNativeSystemInfo, LocalAlloc, ProcessIdToSessionId, GetVolumeInformationW, lstrcpyW, lstrcatW, CreateProcessW, CreatePipe, SetHandleInformation, HeapReAlloc, GetComputerNameW, GetCurrentThread, GetLogicalDriveStringsW, GetDriveTypeW, GetModuleHandleA, GlobalAlloc, GlobalLock, GlobalUnlock, GlobalFree, GlobalSize, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, FindFirstVolumeW, GetVolumePathNamesForVolumeNameW, QueryDosDeviceW, FindNextVolumeW, FindVolumeClose, lstrlenW, CreateFileMappingW, MapViewOfFile, UnmapViewOfFile, SetFilePointer, MoveFileW, SetFilePointerEx, GetTimeFormatW, GetDateFormatW, LockResource, GetLogicalDrives, DeleteVolumeMountPointW, DefineDosDeviceW, GetVolumeNameForVolumeMountPointW, SetVolumeMountPointW, GlobalMemoryStatusEx, GetLocaleInfoW, CreateEventW, CreateNamedPipeW, GetLocaleInfoA, CreateTimerQueue, DeleteTimerQueueEx, CreateTimerQueueTimer, lstrcmpA, FileTimeToLocalFileTime, lstrcpynW, RemoveVectoredExceptionHandler, SetUnhandledExceptionFilter, AddVectoredExceptionHandler, IsBadReadPtr, VirtualQuery, FreeResource, GetFileSize, CreateSemaphoreA, DuplicateHandle, ReleaseSemaphore, CloseHandle, SetEvent, GetStringTypeW, EncodePointer, CompareStringW, LCMapStringW, GetCPInfo, ResetEvent, WaitForMultipleObjectsEx, OpenEventA, SetWaitableTimer, ResumeThread, CreateWaitableTimerA, FormatMessageA, UnhandledExceptionFilter, IsProcessorFeaturePresent, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, OutputDebugStringW, InterlockedPopEntrySList, InterlockedPushEntrySList, FlushInstructionCache, VirtualAlloc, VirtualFree, LoadLibraryExA, GetStringTypeExW, LCMapStringA, GetStringTypeExA, RtlUnwind, GetModuleFileNameA, WriteConsoleW, GetACP, GetFileAttributesExW, SystemTimeToTzSpecificLocalTime, CreateThread, ExitThread, FreeLibraryAndExitThread, SetConsoleCtrlHandler, ExitProcess, GetCommandLineA, GetCommandLineW, GetConsoleCP, HeapSize, IsValidCodePage, GetOEMCP, IsValidLocale, EnumSystemLocalesW, GetCurrentDirectoryW, GetFullPathNameW, SetStdHandle, FlushFileBuffers, GetTimeZoneInformation, SetEnvironmentVariableA, SetEnvironmentVariableW, FindFirstFileExW, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEndOfFile, GetTempPathW, GetVersionExW, CreateProcessA
USER32.dll	OpenClipboard, EmptyClipboard, SetClipboardData, CloseClipboard, IsClipboardFormatAvailable, GetClipboardData, EnableWindow, SetTimer, KillTimer, SetWindowRgn, IsCharAlphaNumericA, ScreenToClient, UpdateLayeredWindow, SetCaretPos, SetActiveWindow, GetKeyState, DestroyCaret, ClientToScreen, CreateCaret, ShowCaret, HideCaret, InsertMenuW, TrackPopupMenu, MessageBoxW, GetSystemMetrics, LoadAcceleratorsW, LoadStringW, GetClassInfoW, DispatchMessageW, PeekMessageW, RegisterClassW, CharNextW, TranslateMessage, UpdateWindow, SetForegroundWindow, LoadImageW, GetWindow, MonitorFromWindow, EndDialog, GetWindowInfo, LockSetForegroundWindow, MapWindowPoints, EnumWindows, GetWindowDC, SetWindowTextW, InvalidateRect, GetDC, ReleaseDC, GetFocus, RegisterClassExW, IsWindowEnabled, SetRect, GetClassInfoExW, InflateRect, IsZoomed, DrawTextW, IsIconic, GetCapture, TrackMouseEvent, SetFocus, SetCapture, ReleaseCapture, GetCursorPos, PostMessageW, ShowWindow, RedrawWindow, GetDlgItem, GetWindowLongW, DefWindowProcW, AdjustWindowRectEx, CallWindowProcW, GetWindowRect, DestroyWindow, IsWindowVisible, SetWindowPos, EnumChildWindows, CreateWindowExW, SendMessageW, IsWindow, OffsetRect, LoadCursorW, SetCursor, SetWindowLongW, GetClientRect, GetParent, PtInRect, BeginPaint, EndPaint, UnregisterClassW, ExitWindowsEx, GetMessageExtraInfo, wsprintfW, GetUserObjectInformationW, GetProcessWindowStation, FindWindowExW, GetWindowTextLengthW, GetMenuItemInfoW, MessageBeep, CreatePopupMenu, GetActiveWindow, IsDialogMessageW, DestroyMenu, BringWindowToTop, TranslateAcceleratorW, LoadIconW, TrackPopupMenuEx, RemoveMenu, AllowSetForegroundWindow, MonitorFromPoint, GetMenuItemCount, MoveWindow, LoadStringA, AppendMenuW, PostQuitMessage, DialogBoxParamW, GetMessageW, GetMonitorInfoW, LoadMenuW
GDI32.dll	TextOutW, GetTextMetricsW, StartPage, EndPage, GetBkColor, SetTextAlign, GetTextColor, GetDeviceCaps, CombineRgn, GetDIBits, ExtCreatePen, LineTo, MoveToEx, ExtTextOutW, CreateFontW, GetObjectW, SetBrushOrgEx, SetStretchBltMode, GetTextExtentPoint32W, CreatePen, Rectangle, SelectClipRgn, IntersectClipRect, SetBkColor, CreateSolidBrush, SetTextColor, SetBkMode, BitBlt, CreateCompatibleBitmap, SaveDC, SelectObject, CreateCompatibleDC, DeleteDC, SetViewportOrgEx, ExcludeClipRect, RestoreDC, DeleteObject, CreateRectRgn, ExtSelectClipRgn
ADVAPI32.dll	CloseServiceHandle, CryptSignHashW, OpenServiceW, OpenSCManagerW, GetNamedSecurityInfoW, GetExplicitEntriesFromAclW, InitializeAcl, SetEntriesInAclW, SetNamedSecurityInfoW, QueryServiceStatusEx, ControlService, LookupAccountNameW, RegSaveKeyExW, RegEnumValueW, OpenProcessToken, RegQueryValueExW, InitializeSecurityDescriptor, SetSecurityDescriptorOwner, RegSetKeySecurity, AddAccessAllowedAce, SetSecurityDescriptorDacl, ConvertSidToStringSidW, LookupPrivilegeValueW, GetTokenInformation, GetLengthSid, RegDeleteValueW, RegOpenKeyExW, RegSetValueExW, RegEnumKeyExW, RegCreateKeyExW, RegDeleteKeyW, RegQueryInfoKeyW, RegCloseKey, DeregisterEventSource, RegisterEventSourceW, ReportEventW, CryptAcquireContextW, CryptReleaseContext, CryptGenRandom, CryptDestroyKey, CryptSetHashParam, CryptGetProvParam, CryptGetUserKey, CryptExportKey, CryptDecrypt, CryptCreateHash, CryptDestroyHash, AccessCheck, IsValidSecurityDescriptor, CryptEnumProvidersW, AdjustTokenPrivileges, GetUserNameW, DuplicateToken, FreeSid, OpenThreadToken, AllocateAndInitializeSid, SetSecurityDescriptorGroup
SHELL32.dll	SHOpenFolderAndSelectItems, SHParseDisplayName, ShellExecuteW
ole32.dll	CreateStreamOnHGlobal, CoInitializeEx, CoTaskMemRealloc, CoCreateInstance, CoUninitialize, CoInitialize, CoTaskMemFree, CoTaskMemAlloc
OLEAUT32.dll	VariantInit, SysAllocString, VariantClear, VarUI4FromStr, SysFreeString
SHLWAPI.dll	StrCmpNIW, StrCmpIW
COMCTL32.dll	
MSIMG32.dll	AlphaBlend

DLL	Import

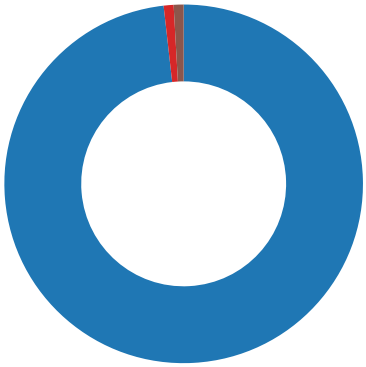
Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- file.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- svchost.exe
- sc.exe
- conhost.exe
- sc.exe
- conhost.exe
- sc.exe
- conhost.exe
- sc.exe
- conhost.exe
- sc.exe
- conhost.exe
- sc.exe
- conhost.exe
- regsvr32.exe
- EsgInstallerDelay__0.exe
- conhost.exe
- EsgInstallerDelay__1.exe
- conhost.exe
- sc.exe
- ShKernel.exe
- sc.exe
- ShMonitor.exe
- MpCmdRun.exe
- conhost.exe
- SpyHunter5.exe

Click to jump to process

System Behavior

Analysis Process: file.exe PID: 5244, Parent PID: 3452

General

Target ID:	0
Start time:	00:14:27
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0xd80000
File size:	6881256 bytes
MD5 hash:	2816BACD01B0D8C48F1D8714C6AA6F0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Registry Activities

Analysis Process: svchost.exe PID: **5288**, Parent PID: **580**

General

Target ID:	1
Start time:	00:14:39
Start date:	30/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **1556**, Parent PID: **580**

General

Target ID:	2
Start time:	00:14:39
Start date:	30/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **684**, Parent PID: **580**

General

Target ID:	3
Start time:	00:14:39
Start date:	30/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5540**, Parent PID: **580**

General

Target ID:	4
Start time:	00:14:40
Start date:	30/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Analysis Process: svchost.exe PID: **1360**, Parent PID: **580**

General

Target ID:	5
Start time:	00:14:40
Start date:	30/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: **3384**, Parent PID: **580**

General

Target ID:	6
Start time:	00:14:45
Start date:	30/11/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff65cb30000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **868**, Parent PID: **580**

General

Target ID:	7
Start time:	00:14:45
Start date:	30/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: **3460**, Parent PID: **580**

General

Target ID:	8
Start time:	00:14:46
Start date:	30/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **2080**, Parent PID: **580**

General

Target ID:	9
Start time:	00:14:46
Start date:	30/11/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: sc.exe PID: **680**, Parent PID: **5244**

General

Target ID:	10
Start time:	00:15:24
Start date:	30/11/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\sc.exe create EsgShKernel start= demand binPath= "\"C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe\"" DisplayName= " SpyHunter 5 Kernel"

Imagebase:	0x7ff676710000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5508, Parent PID: 680

General

Target ID:	11
Start time:	00:15:24
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5640, Parent PID: 5244

General

Target ID:	12
Start time:	00:15:24
Start date:	30/11/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\sc.exe description EsgShKernel "SpyHunter 5 Kernel"
Imagebase:	0x7ff676710000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4080, Parent PID: 5640

General

Target ID:	13
Start time:	00:15:25
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **5744**, Parent PID: **5244**

General

Target ID:	14
Start time:	00:15:25
Start date:	30/11/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\sc.exe create ShMonitor start= demand binPath= "\"C:\Program Files\EnigmaSoft\SpyHunter\ShMonitor.exe\"" DisplayName= "SpyHunter 5 Kernel Monitor"
Imagebase:	0x7ff676710000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5752**, Parent PID: **5744**

General

Target ID:	15
Start time:	00:15:25
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **5852**, Parent PID: **5244**

General

Target ID:	16
Start time:	00:15:26
Start date:	30/11/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\sc.exe description ShMonitor "SpyHunter 5 Kernel Monitor"

Imagebase:	0x7ff676710000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5784, Parent PID: 5852

General

Target ID:	17
Start time:	00:15:26
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 1788, Parent PID: 5244

General

Target ID:	18
Start time:	00:15:26
Start date:	30/11/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\sc.exe config ShMonitor start= auto
Imagebase:	0x7ff676710000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6140, Parent PID: 1788

General

Target ID:	19
Start time:	00:15:26
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **6020**, Parent PID: **5244**

General

Target ID:	20
Start time:	00:15:27
Start date:	30/11/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\sc.exe config EsgShKernel start= auto
Imagebase:	0x7ff676710000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6060**, Parent PID: **6020**

General

Target ID:	21
Start time:	00:15:27
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: **2108**, Parent PID: **5244**

General

Target ID:	22
Start time:	00:15:27
Start date:	30/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /s "C:\Program Files\EnigmaSoft\SpyHunter\ShShellExt.dll"
Imagebase:	0x7ff65a000000

File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: EsgInstallerDelay__0.exe PID: 64, Parent PID: 5244

General

Target ID:	23
Start time:	00:15:29
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__0.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__0.exe -exec OpfXySN2sIJfRn7kaByo3fAgnhU5bFC+1YK5gktB214= -args MHLPvv2eVF5BDDA j57kaKhLIRzVl3TCPBu81sCtfDvA= -wait 300
Imagebase:	0x7ff6980f0000
File size:	369512 bytes
MD5 hash:	EDCE372DE488AA221DA7DB7544C09B3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__0.exe	success or wait	1	7FF6980F19C1	MoveFileExW

Analysis Process: conhost.exe PID: 1332, Parent PID: 64

General

Target ID:	24
Start time:	00:15:29
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: EsgInstallerDelay__1.exe PID: **2348**, Parent PID: **5244**

General

Target ID:	25
Start time:	00:15:29
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__1.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__1.exe -exec OpfXySN2sIJfRn7kaByo3fAgnhU5bFC+1YK5gktB214= -args hOGTiE/QHFPjrWqL1njGygtJtFEVLgswO/2BlkHQX4U= -wait 300
Imagebase:	0x7ff7a56d0000
File size:	369512 bytes
MD5 hash:	EDCE372DE488AA221DA7DB7544C09B3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__0.exe	\??\C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__0.exe\??\C:\Users\user\AppData\Local\Temp\EsgInstallerDelay__1.exe	success or wait	1	7FF7A56D19C1	MoveFileExW

Analysis Process: conhost.exe PID: **3624**, Parent PID: **2348**

General

Target ID:	26
Start time:	00:15:30
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **5312**, Parent PID: **64**

General

Target ID:	27
Start time:	00:15:30
Start date:	30/11/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\sc.exe start EsgShKernel -tt_on
Imagebase:	0x7ff676710000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: ShKernel.exe PID: **5400**, Parent PID: **580**

General

Target ID:	28
Start time:	00:15:30
Start date:	30/11/2022
Path:	C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe
Imagebase:	0x7ff7088d0000
File size:	17032680 bytes
MD5 hash:	F2F6BF33561C9EF8FE3310D46A3C8A25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000001C.00000002.583150850.000001D380AA5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000001C.00000003.422519867.000001D3F58C0000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000001C.00000003.422727533.000001D3F4225000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000001C.00000003.422306773.000001D3F5841000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 0000001C.00000003.478164990.000001D3F34BE000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_BrowserHistorySpy, Description: Yara detected BrowserHistorySpy Tool by SecurityXploded, Source: 0000001C.00000003.509274290.000001D3F5D31000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_EXEPWSH_DLAgent, Description: Detects SystemBC, Source: C:\Program Files\EnigmaSoft\SpyHunter\ShKernel.exe, Author: ditekSHen
Antivirus matches:	• Detection: 2%, ReversingLabs

Analysis Process: sc.exe PID: **5100**, Parent PID: **2348**

General

Target ID:	29
Start time:	00:15:30
Start date:	30/11/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\System32\sc.exe start ShMonitor
Imagebase:	0x7ff676710000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ShMonitor.exe PID: **4792**, Parent PID: **580**

General

Target ID:	30
Start time:	00:15:30
Start date:	30/11/2022
Path:	C:\Program Files\EnigmaSoft\SpyHunter\ShMonitor.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\EnigmaSoft\SpyHunter\ShMonitor.exe
Imagebase:	0x7ff7a72d0000
File size:	549352 bytes
MD5 hash:	F9FA9D3B5957F0C365A20DE5C71EC214
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs

Analysis Process: MpCmdRun.exe PID: **2364**, Parent PID: **2080**

General

Target ID:	31
Start time:	00:15:47
Start date:	30/11/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff610f30000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2680**, Parent PID: **2364**

General

Target ID:	32
Start time:	00:15:47
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: SpyHunter5.exe PID: **5688**, Parent PID: **5400**

General	
Target ID:	33
Start time:	00:16:11
Start date:	30/11/2022
Path:	C:\Program Files\EnigmaSoft\SpyHunter\SpyHunter5.exe
Wow64 process (32bit):	
Commandline:	"C:\Program Files\EnigmaSoft\SpyHunter\SpyHunter5.exe" /hide
Imagebase:	
File size:	18037736 bytes
MD5 hash:	096FA37EA53BB15959E9EEF9FD3F2745
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs

Disassembly

No disassembly