**Malware Behavior Analysis on**

**evil.exe**

**Prepared for**

Professor Douglas

CFRS 510

**Prepared by**

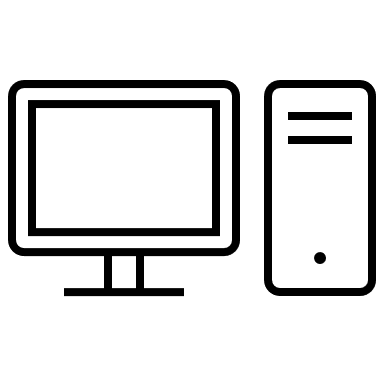
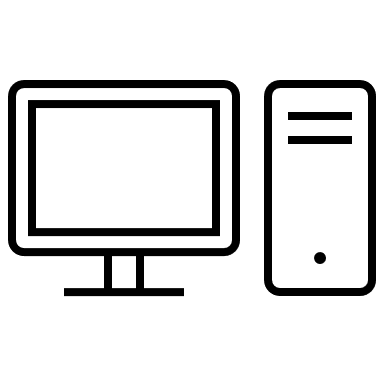
Sofia Sackett

2 May 2020

**Executive Summary**

This report includes the environment setup as well as static and dynamic analysis of the malware evil.exe. Evil.exe is a packed portable executable, approximately 675 KB, and was written for a 32-bit Windows operating system. The malware was examined within a virtual environment consisting of a victim Windows machine and a REMnux virtual machine that acted as a fake DNS and HTTP server. Analysis of evil.exe confirms that it is a malicious piece of code that likely acts as a trojan and sends users to the suspicious domain wike.wikaba.com (**153.249.14.225).**

**Environment**

The evil.exe malware was retrieved from BlackBoard via Professor Brienne Douglas and was downloaded to a victim VM. Evil.exe was run on a victim Windows 8.1 32-bit virtual machine within VMWare Workstation Pro. The victim virtual machine was isolated from the host machine’s network by using a second VM running REMnux 6.0 which acted as a fake DNS and HTTP server for the victim machine. The REMnux box was also configured to act as the victim VM’s default gateway. In this way, all web traffic and DNS name resolution data would be sent to the REMnux VM rather than the Internet.

**OS:** Windows 8.1 32-bit

**IP Address:** 192.168.60.1

**Subnet Mask:** 255.255.255.0

**Default Gateway:** 192.168.60.3

**DNS Server:** 192.168.60.3

**Alternate DNS Server:** 8.8.8.8

**OS:** REMnux 6.0

**IP Address:** 192.168.60.3

**Subnet Mask:** 255.255.255.0

**Network:** 192.168.60.0

**Broadcast:** 192.168.60.255

**Gateway:** 192.168.60.1

**DNS Nameserver:** 8.8.8.8

The tools used to conduct static and dynamic behavior analysis on evil.exe included the strings command, Process Explorer, and Process Monitor from SysinternalsSuite, Regshot to collect VM snapshots before and after analysis, Dependency Walker to identify shared libraries, PEiD, and PeStudio.

|  |  |
| --- | --- |
| Tool | Version |
| Sysinternals strings | 2.52 (June 20, 2013) |
| Process Explorer | 16.21 (May 16, 2017) |
| Process Monitor | 3.50 (February 13, 2018) |
| Regshot | 1.9.0 (July 2, 2013) |
| Dependency Walker | 2.2.1 (October 29, 2015) |
| PEiD | 0.95 (April 24, 2018) |
| PeStudio | 9.05 (April 20, 2020) |

**Static Analysis Results**

Static code analysis was carried out with the help of PEiD, Dependency Walker, the Sysinternals strings command, and PeStudio on evil.exe. First, the MD5 hash (e696b38ac71b23f50ee68da06a004af3) was verified with the help of HxD’s analysis tool. PEiD shows that the malware is a portable executable, specifically a Windows 32-bit .exe file, as well as revealed that the file was compiled on 2013-08-22 15:00:50 + 02:00. Opening evil.exe with PEiD showed the entrypoint (0001D348) and file offset (0001C748), as well as section and subsystem information. PEiD’s Section Viewer shows that there are four main sections within this malware, including .text, .rdata, .data, and .rsrc.

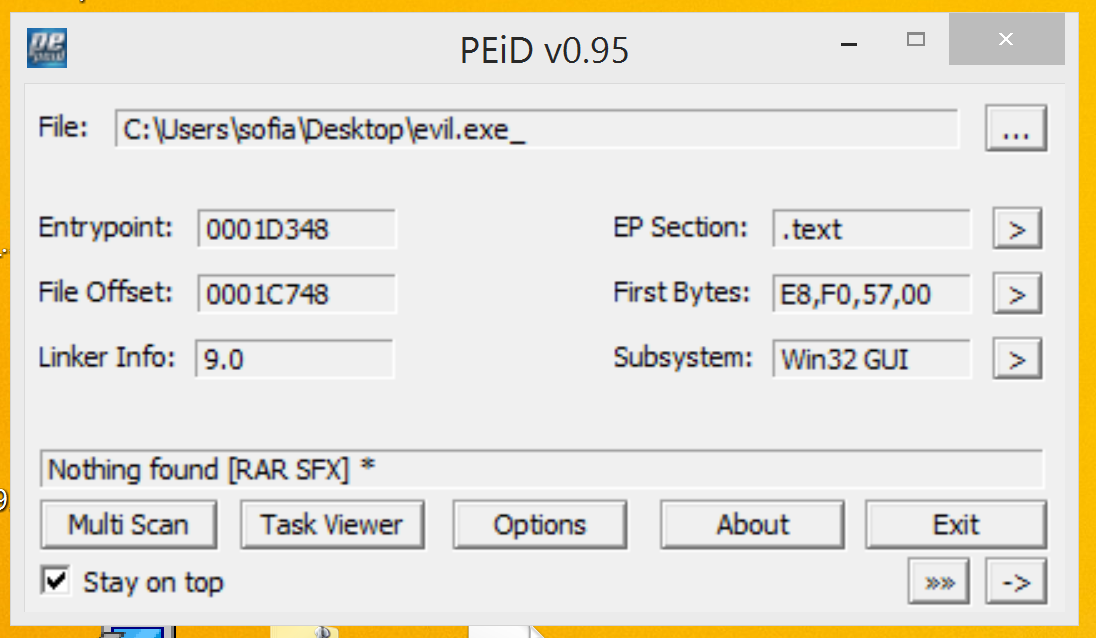


Figure 1 PEiD home screen showing section information, entrypoint, file offset, and subsystem information.

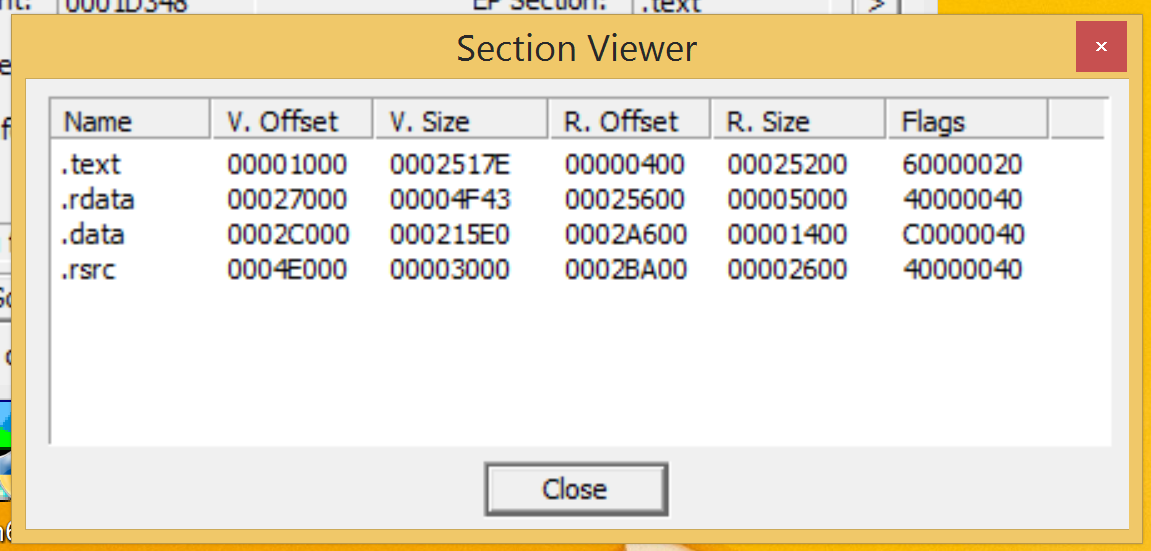


Figure 2 PEiD Section Viewer displaying each section's offset, size, and flags.

PEiD’s Imports Viewer shows the dynamic-link libraries (DLLs) connected to this malware, including COMCTL32.dll, SHLWAPI.dll, KERNEL32.dll, USER32.dll, GDI32.dll, COMDLG32.dll, ADVAPI32.dll, SHELL32.dll, ole32.dll, and OLEAUT32.dll.

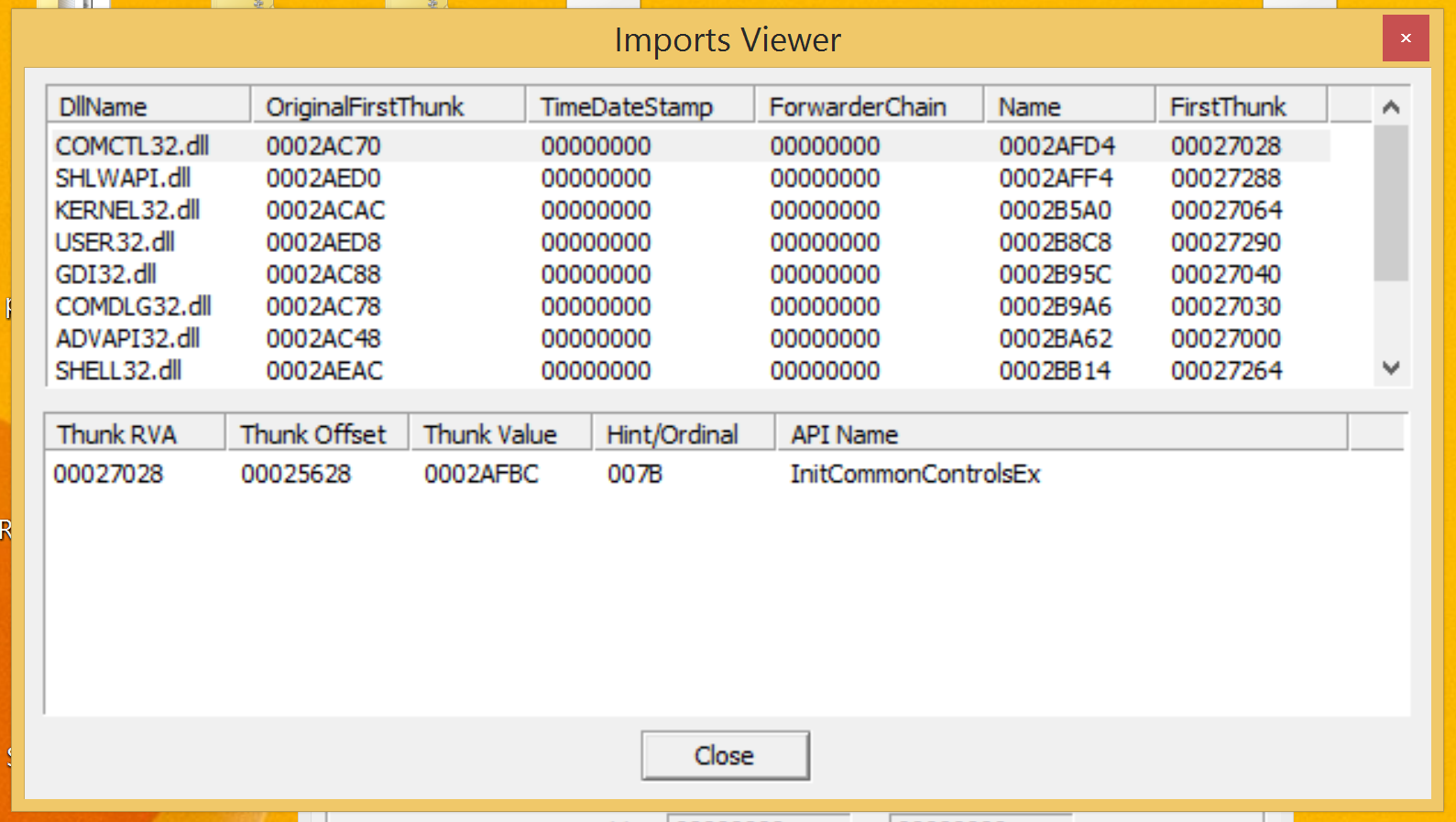


Figure 3 PEiD Imports Viewer showing some of the .dll files imported by evil.exe.

Next, the PEiD Strings Viewer yielded some interesting strings, including those that alter registry keys, create and delete files, and look for sensitive information such as passwords. Finally, there is evidence that the malware may be self-extracting, because the PEiD Exports Viewer and String Viewer show calls to WinRAR as does the Sysinternals strings command.

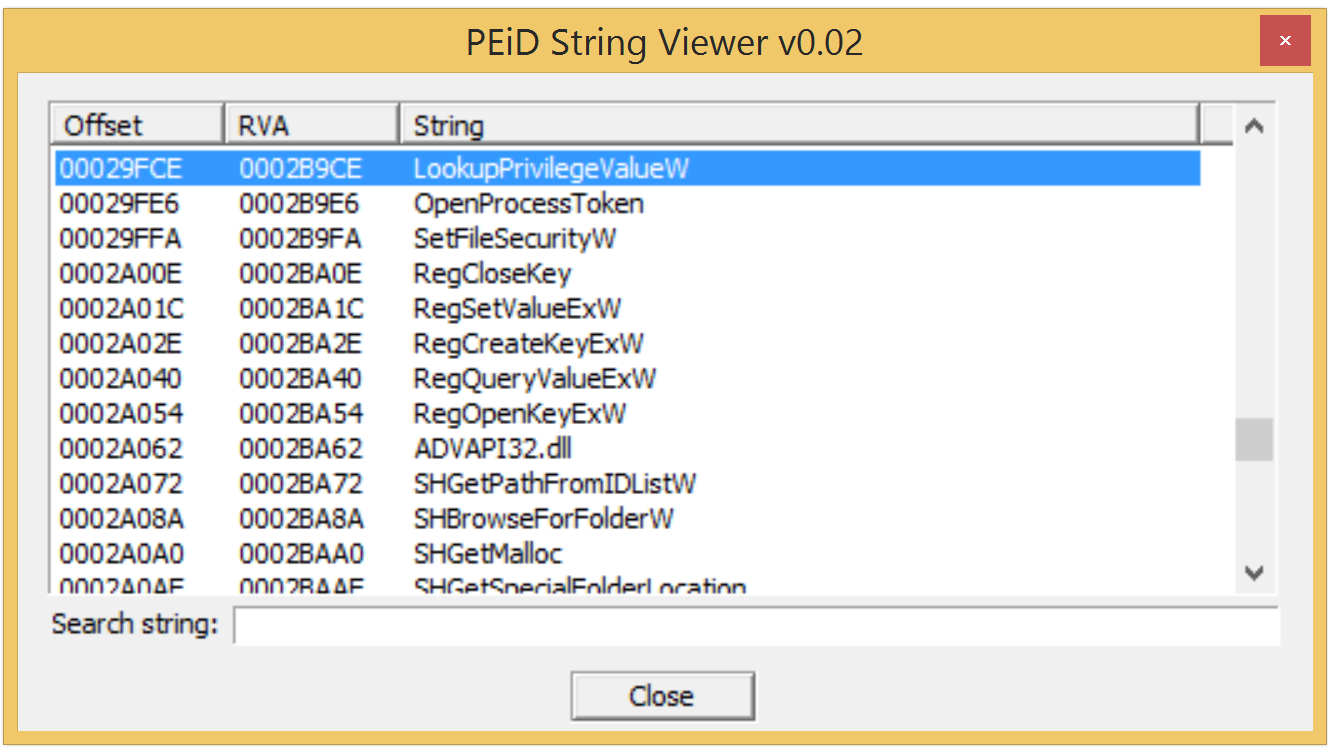


Figure 4 PEiD String Viewer showing suspicious strings.

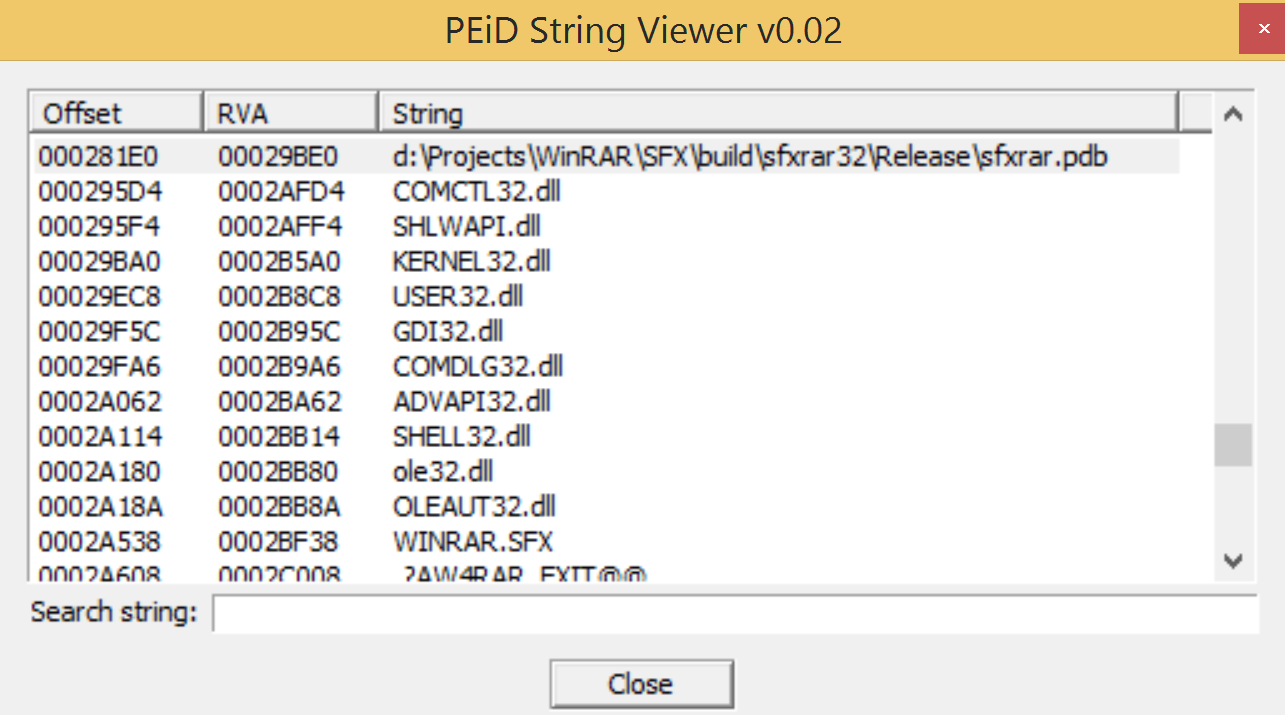


Figure 5 PEiD String Viewer showing the .dlls as well as WinRAR.

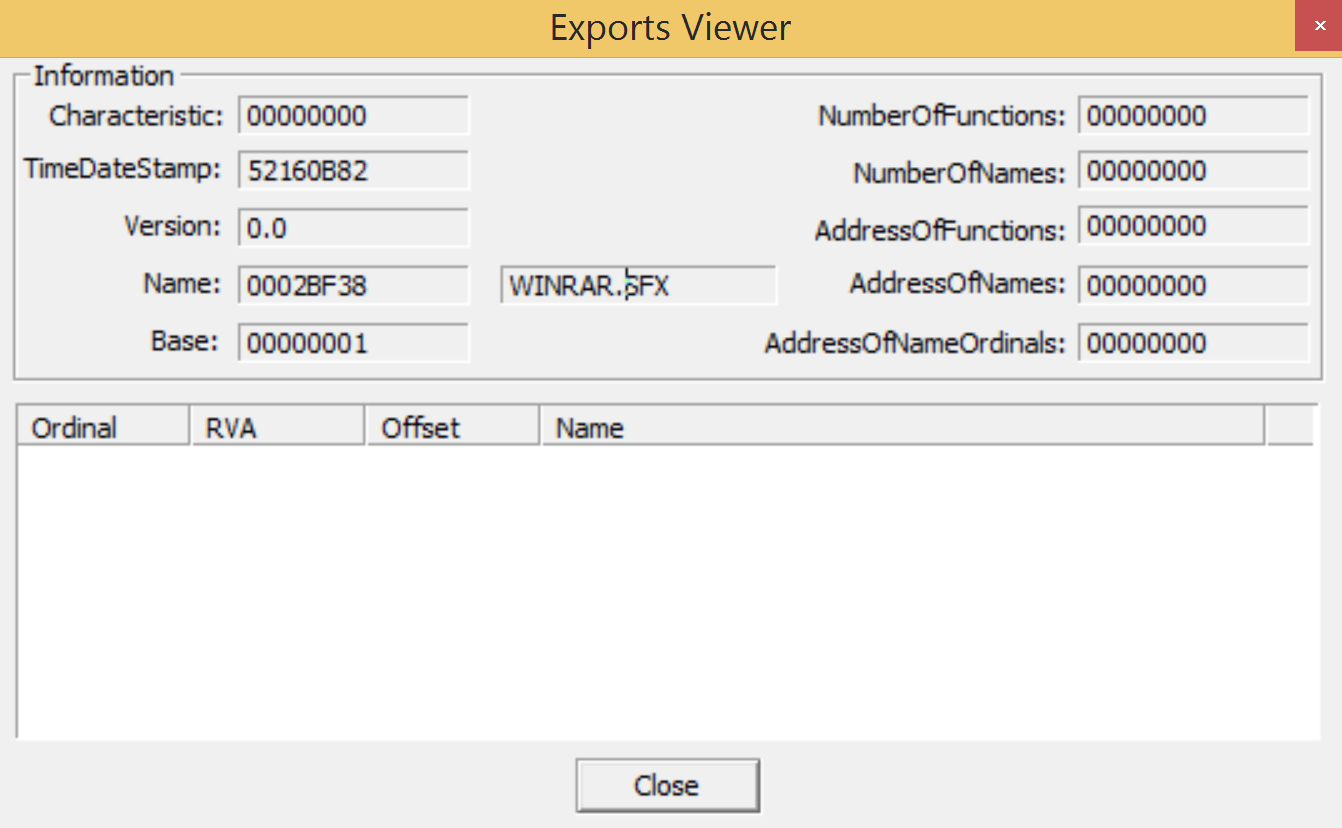


Figure 6 PEiD Exports Viewer displaying WINRAR.SFX, a known unpacking/decompressing tool.

The strings command was executed from the command line and the output was saved to a text file, evilStrings.txt.

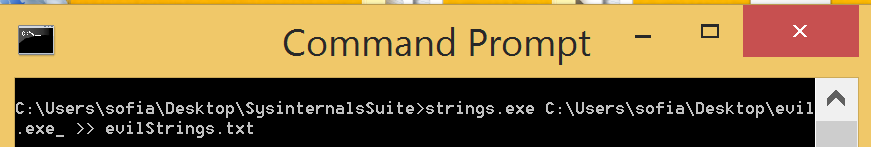


Figure 7 Command prompt executing strings.exe on evil.exe and outputting that data to evilStrings.txt.

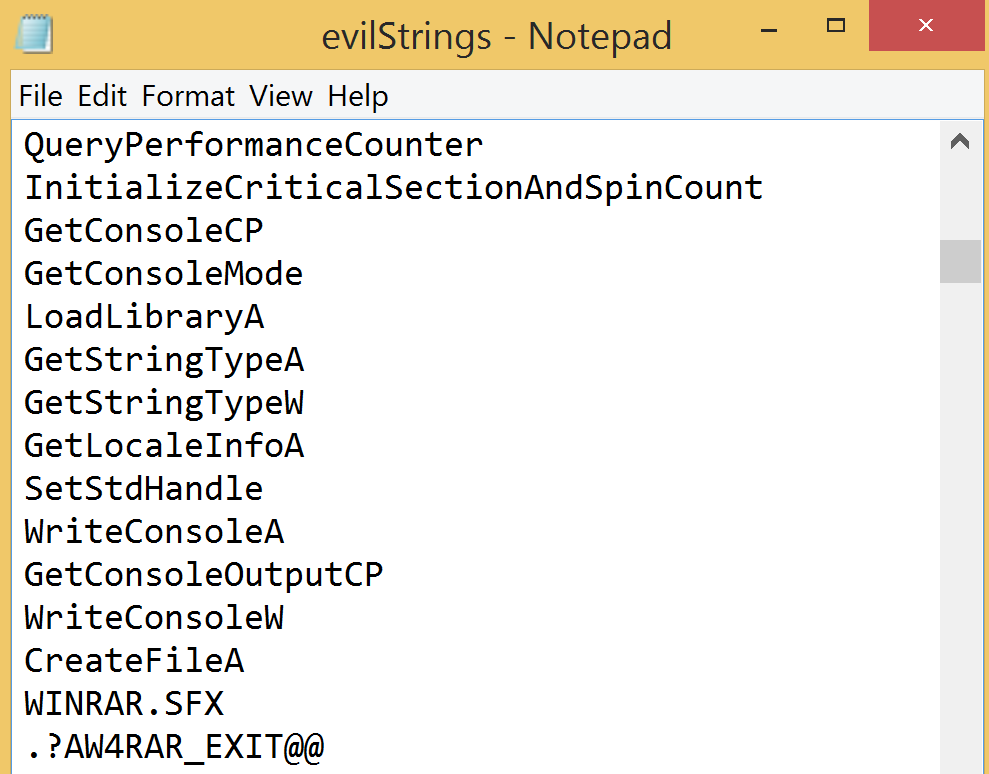


Figure 8 evilStrings.txt

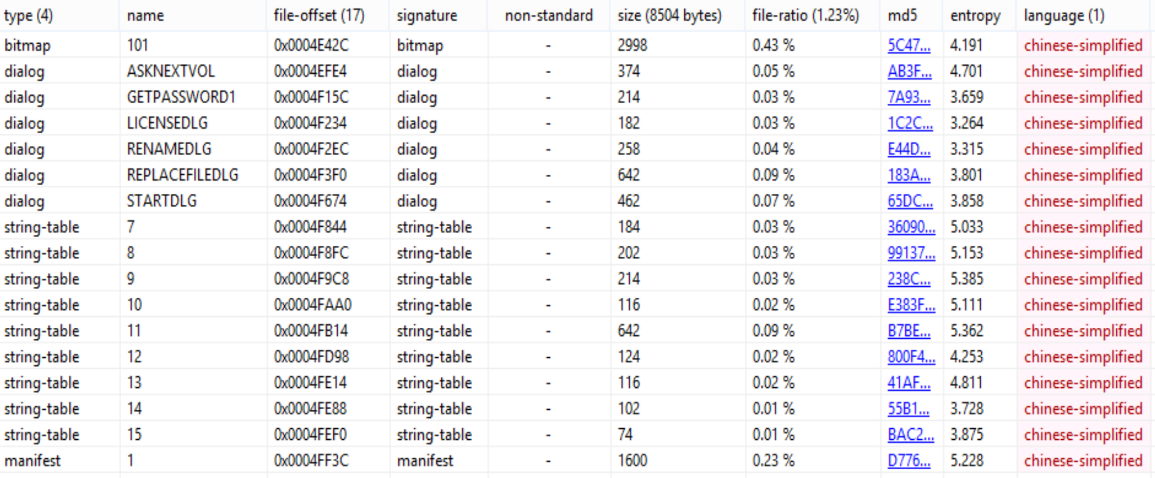
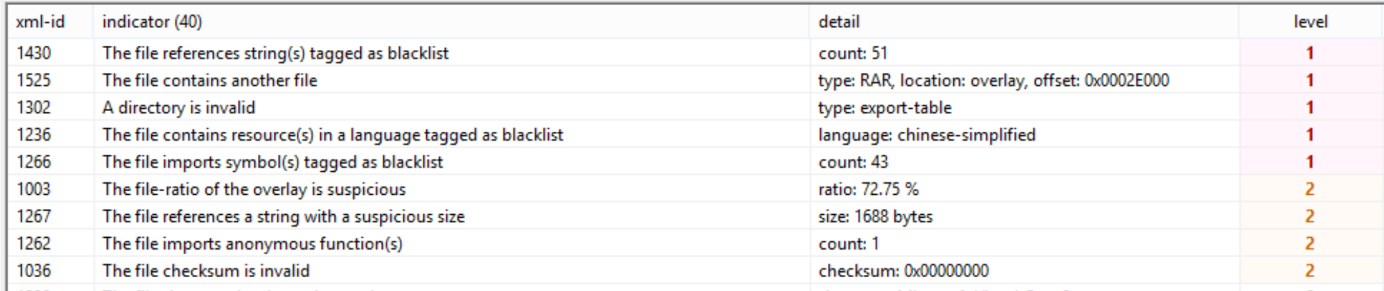
The data collected from PEiD was bolstered by PeStudio, including compilation date and time, system information, strings, and DLLs. However, PeStudio also provided new information, including the unpacked hash value of evil.exe, that the malware contained Chinese characters, as well as categorized indicators of compromise by threat level. Finally, the DLLs were checked with the Dependency Walker tool, which showed the same information as PeStudio and PEiD.

Figure 9 PeStudio tool showing the threat levels of indicators in evil.exe.

Figure 10 PeStudio showing that some of the malware was written using Chinese-simplified characters.

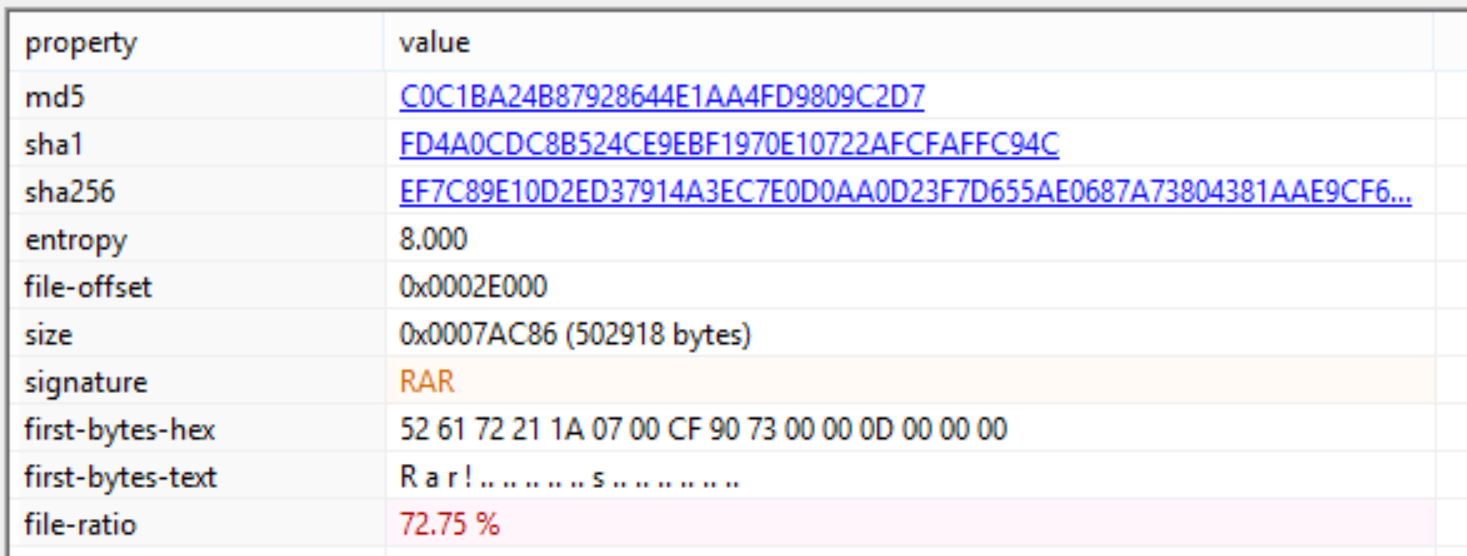


Figure 11 PeStudio showing unpacked hash values as well as the file ratio.

A screenshot of a social media post

Description automatically generated

Figure 12 Dependency Walker showing .dll files associated with evil.exe.

**Dynamic Analysis Results**

A screenshot of a cell phone

Description automatically generatedAfter completing static code analysis and setting up the sandbox as described in the environment section, the REMnux virtual machine was configured to act as a fake DNS and HTTP server. Using Regmon’s Regshot, a snapshot of the Windows virtual machine was taken before and after the malware was executed. In this way, we can compare the two snapshots and determine what system changes occurred due to evil.exe.

A screenshot of a cell phone

Description automatically generated

The fake DNS and HTTP servers captured information from the infected Windows machine reaching out to wike.wikaba.com.

A screenshot of a cell phone

Description automatically generated

The comparison of the first and second snapshots in Regshot was saved to a text file which include alterations to registry keys and values, some of which can be seen below.

**A screenshot of a social media post

Description automatically generated**

**A screenshot of a cell phone

Description automatically generated**Sysinternals’ Process Monitor tool corroborates the information found by Regshot, such as the registry queries conducted by evil.exe.

**Conclusion**

The malware evil.exe is a portable executable written for a 32-bit Windows system. The malware is believed to be dangerous because it is hiding its true intentions with a packer and it is altering registry keys. Some of the registry alterations include changes to the Windows error reporting registry key as well as scheduling tasks based on specific triggers which indicate a self-deletion mechanism. The malware also attempts to connect to a suspicious web domain, wike.wikaba.com which resolves to the Japanese IP address **153.249.14.225. Therefore, it is very likely that evil.exe is a type of Trojan that sends the user to a dangerous website that may downloads more malware such as spyware or ransomware.**