Malware Behavior Analysis on evil.exe

Prepared for
Professor Douglas
CFRS 510

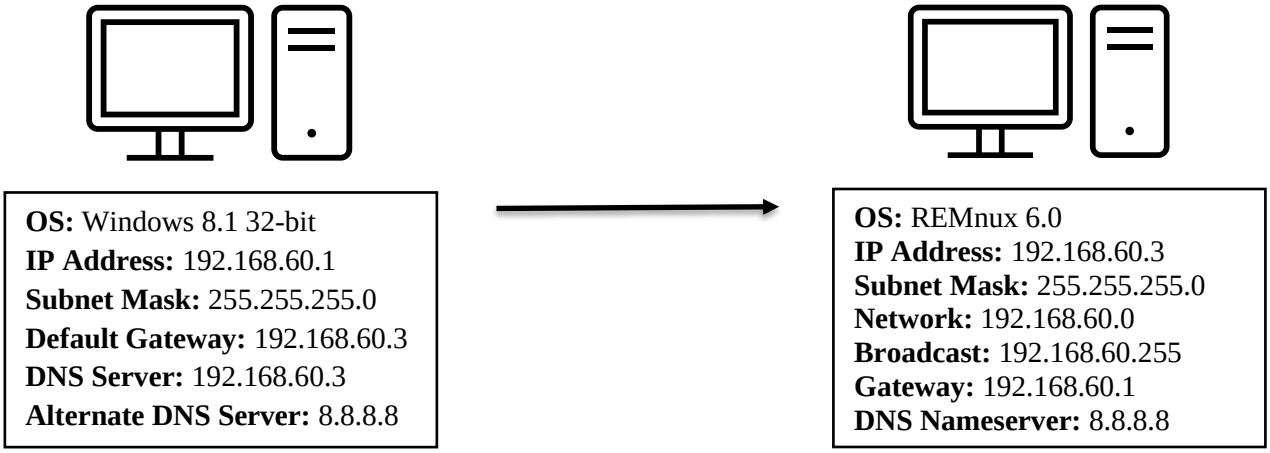
Prepared by
Sofia Sackett
2 May 2020

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.



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.

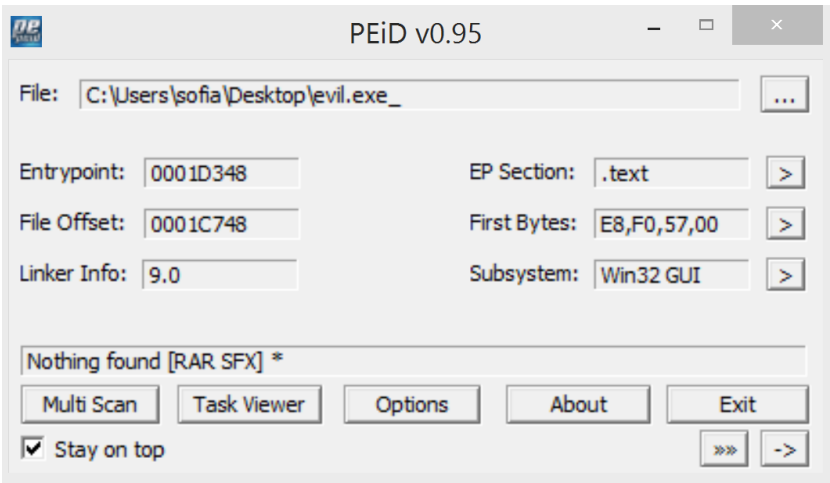


Figure 1 PEiD home screen showing section information, entrypoint, file offset, and subsystem information.

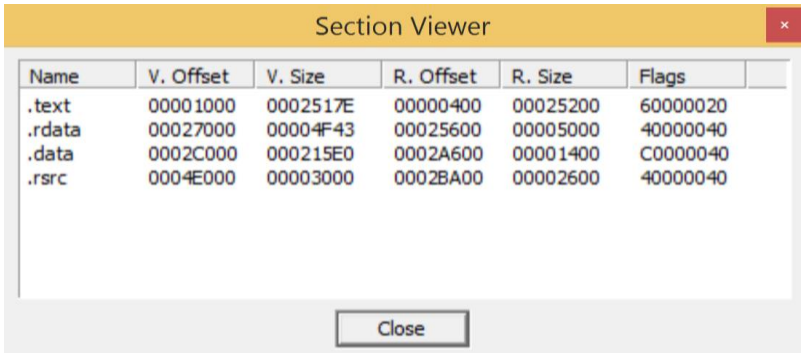


Figure 2 PEiD Section Viewer displaying each section's offset, size, and flags.

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.

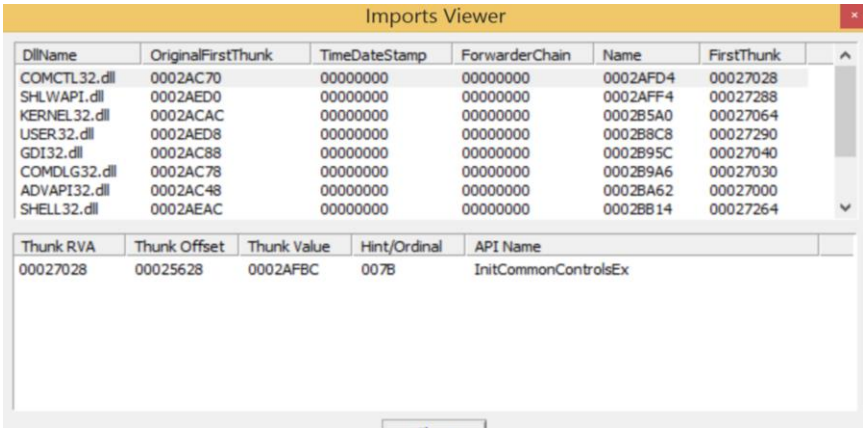


Figure 3 PEiD Imports Viewer showing some of the .dll files imported by evil.exe.

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.

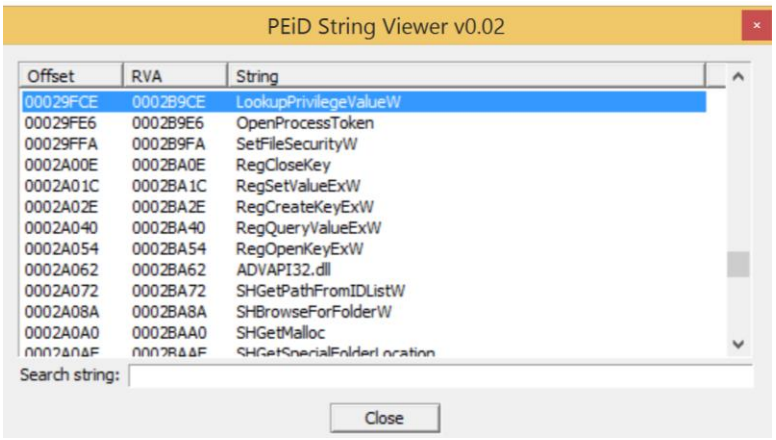


Figure 4 PEiD String Viewer showing suspicious strings.

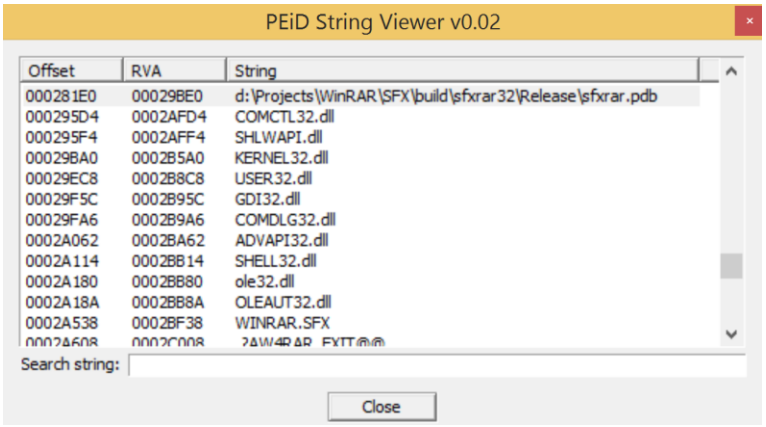


Figure 5 PEiD String Viewer showing the .dlls as well as WinRAR.

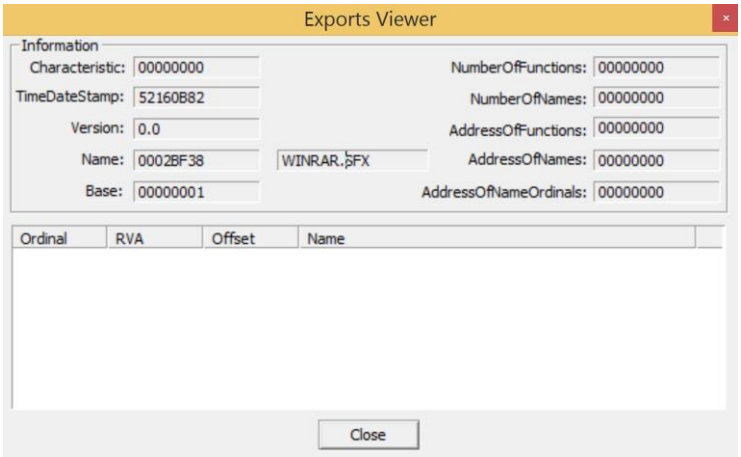


Figure 6 PEiD Exports Viewer displaying WINRAR.SFX, a known unpacking/decompressing tool.

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

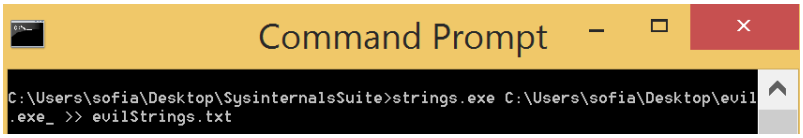


Figure 7 Command prompt executing strings.exe on evil.exe and outputting that data to evilStrings.txt.

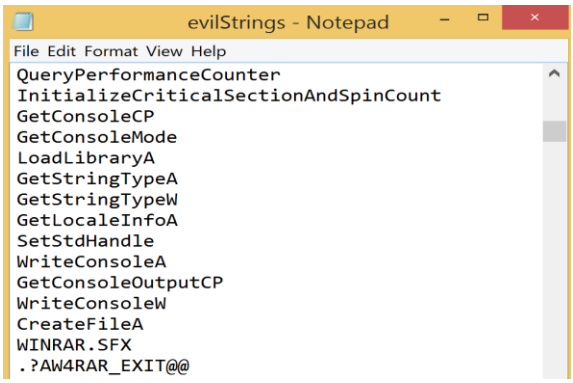


Figure 8 evilStrings.txt

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.

type (4)	name	file-offset (17)	signature	non-standard	size (8504 bytes)	file-ratio (1.23%)	md5	entropy	language (1)
bitmap	101	0x0004E42C	bitmap	-	2998	0.43 %	5C47...	4.191	chinese-simplified
dialog	ASKNEXTVOL	0x0004EFE4	dialog	-	374	0.05 %	AB3F...	4.701	chinese-simplified
dialog	GETPASSWORD1	0x0004F15C	dialog	-	214	0.03 %	7A93...	3.659	chinese-simplified
dialog	LICENSEDLG	0x0004F234	dialog	-	182	0.03 %	1C2C...	3.264	chinese-simplified
dialog	RENAMEDLG	0x0004F2EC	dialog	-	258	0.04 %	E44D...	3.315	chinese-simplified
dialog	REPLACEFILEDLG	0x0004F3F0	dialog	-	642	0.09 %	183A...	3.801	chinese-simplified
dialog	STARTDLG	0x0004F674	dialog	-	462	0.07 %	65DC...	3.858	chinese-simplified
string-table	7	0x0004F844	string-table	-	184	0.03 %	36090...	5.033	chinese-simplified
string-table	8	0x0004F8FC	string-table	-	202	0.03 %	99137...	5.153	chinese-simplified
string-table	9	0x0004F9C8	string-table	-	214	0.03 %	238C...	5.385	chinese-simplified
string-table	10	0x0004FAA0	string-table	-	116	0.02 %	E383F...	5.111	chinese-simplified
string-table	11	0x0004FB14	string-table	-	642	0.09 %	B7BE...	5.362	chinese-simplified
string-table	12	0x0004FD98	string-table	-	124	0.02 %	800F4...	4.253	chinese-simplified
string-table	13	0x0004FE14	string-table	-	116	0.02 %	41AF...	4.811	chinese-simplified
string-table	14	0x0004FE88	string-table	-	102	0.01 %	55B1...	3.728	chinese-simplified
string-table	15	0x0004FEF0	string-table	-	74	0.01 %	BAC2...	3.875	chinese-simplified
manifest	1	0x0004FF3C	manifest	-	1600	0.23 %	D776...	5.228	chinese-simplified

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

xml-id	indicator (40)	detail	level
1430	The file references string(s) tagged as blacklist	count: 51	1
1525	The file contains another file	type: RAR, location: overlay, offset: 0x0002E000	1
1302	A directory is invalid	type: export-table	1
1236	The file contains resource(s) in a language tagged as blacklist	language: chinese-simplified	1
1266	The file imports symbol(s) tagged as blacklist	count: 43	1
1003	The file-ratio of the overlay is suspicious	ratio: 72.75 %	2
1267	The file references a string with a suspicious size	size: 1688 bytes	2
1262	The file imports anonymous function(s)	count: 1	2
1036	The file checksum is invalid	checksum: 0x00000000	2

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

property	value
md5	C0C1BA24B87928644E1AA4FD9809C2D7
sha1	FD4A0CDC8B524CE9EBF1970E10722AFCFAFFC94C
sha256	EF7C89E10D2ED37914A3EC7E0D0AA0D23F7D655AE0687A73804381AAE9CF6...
entropy	8.000
file-offset	0x0002E000
size	0x0007AC86 (502918 bytes)
signature	RAR
first-bytes-hex	52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00
first-bytes-text	R a r ! .. .. s .. ..
file-ratio	72.75 %

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

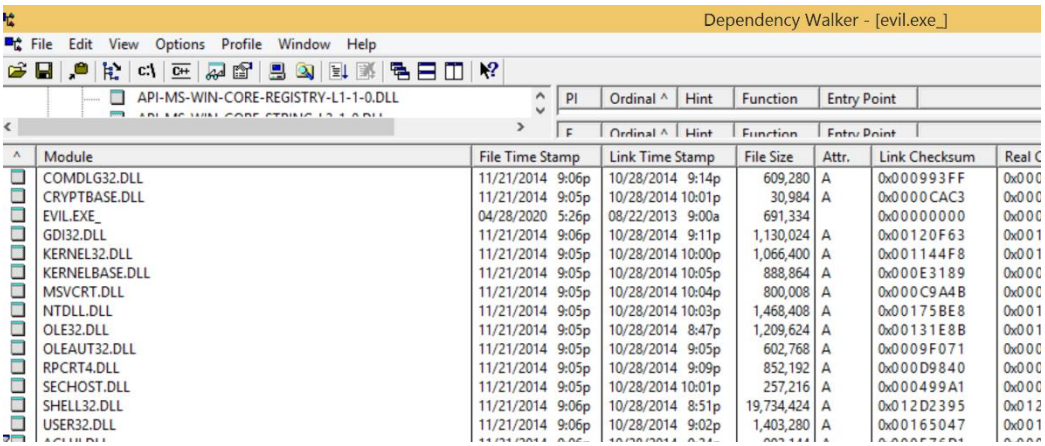
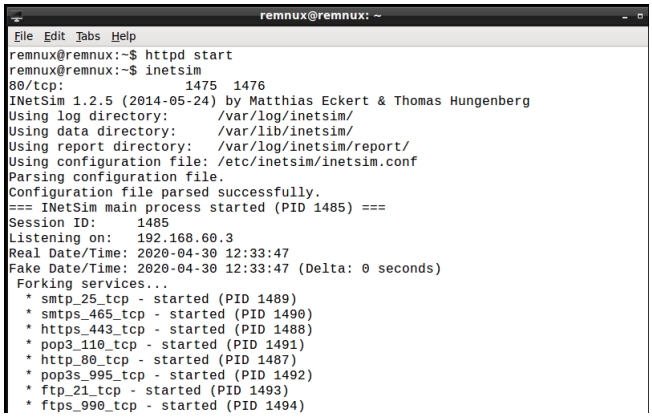
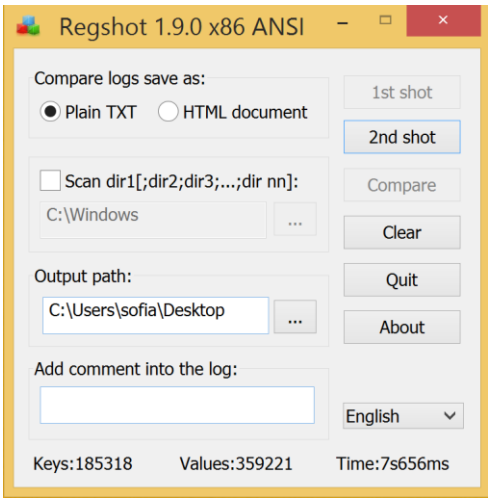


Figure 12 Dependency Walker showing .dll files associated with evil.exe.

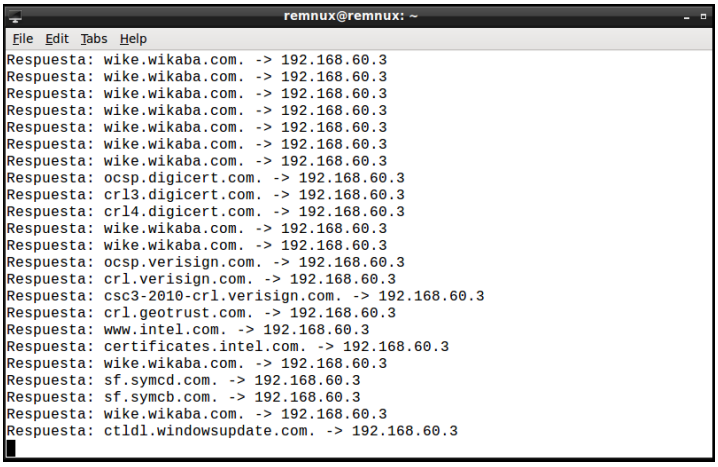
Dynamic Analysis Results

After 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.

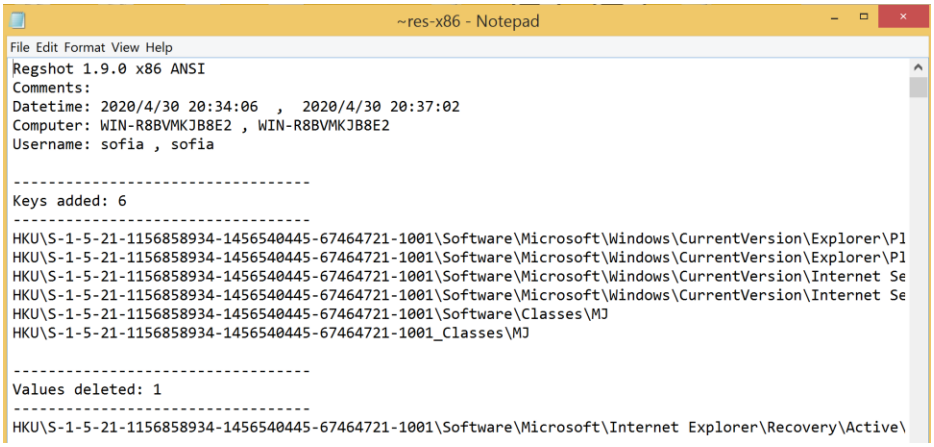




The fake DNS and HTTP servers captured information from the infected Windows machine reaching out to wike.wikaba.com.



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.

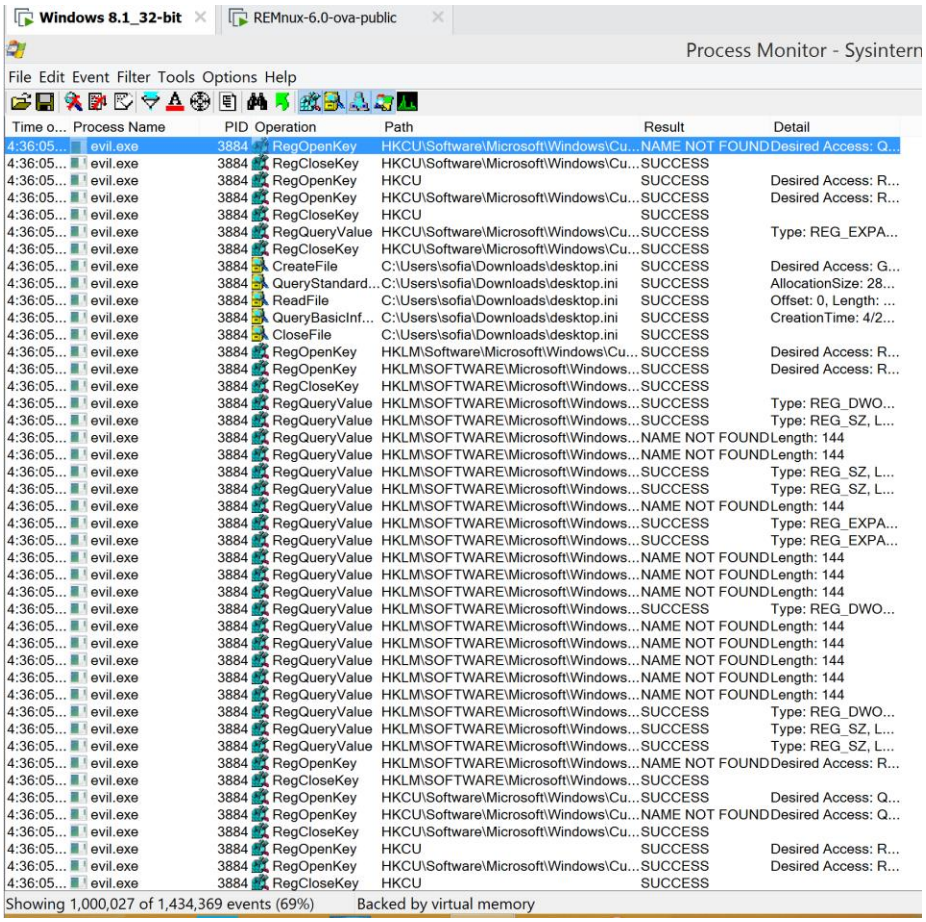


```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2020/4/30 20:34:06  ,  2020/4/30 20:37:02
Computer: WIN-R8BVMKJB8E2 , WIN-R8BVMKJB8E2
Username: sofia , sofia

----------------------------------
Keys added: 6
----------------------------------
HKU\S-1-5-21-1156858934-1456540445-67464721-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Pl
HKU\S-1-5-21-1156858934-1456540445-67464721-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Pl
HKU\S-1-5-21-1156858934-1456540445-67464721-1001\Software\Microsoft\Windows\CurrentVersion\Internet Se
HKU\S-1-5-21-1156858934-1456540445-67464721-1001\Software\Microsoft\Windows\CurrentVersion\Internet Se
HKU\S-1-5-21-1156858934-1456540445-67464721-1001\Software\Classes\MJ
HKU\S-1-5-21-1156858934-1456540445-67464721-1001_Classes\MJ

----------------------------------
Values deleted: 1
----------------------------------
HKU\S-1-5-21-1156858934-1456540445-67464721-1001\Software\Microsoft\Internet Explorer\Recovery\Active\
```

Sysinternals' Process Monitor tool corroborates the information found by Regshot, such as the registry queries conducted by evil.exe.



Time o...	Process Name	PID	Operation	Path	Result	Detail
4:36:05...	evil.exe	3884	RegOpenKey	HKCU\Software\Microsoft\Windows\Cu...	NAME NOT FOUND	Desired Access: Q...
4:36:05...	evil.exe	3884	RegCloseKey	HKCU\Software\Microsoft\Windows\Cu...	SUCCESS	
4:36:05...	evil.exe	3884	RegOpenKey	HKCU	SUCCESS	Desired Access: R...
4:36:05...	evil.exe	3884	RegOpenKey	HKCU\Software\Microsoft\Windows\Cu...	SUCCESS	Desired Access: R...
4:36:05...	evil.exe	3884	RegCloseKey	HKCU	SUCCESS	
4:36:05...	evil.exe	3884	RegQueryValue	HKCU\Software\Microsoft\Windows\Cu...	SUCCESS	Type: REG_EXPA...
4:36:05...	evil.exe	3884	RegCloseKey	HKCU\Software\Microsoft\Windows\Cu...	SUCCESS	
4:36:05...	evil.exe	3884	CreateFile	C:\Users\sofia\Downloads\desktop.ini	SUCCESS	Desired Access: G...
4:36:05...	evil.exe	3884	QueryStandard...	C:\Users\sofia\Downloads\desktop.ini	SUCCESS	AllocationSize: 28...
4:36:05...	evil.exe	3884	ReadFile	C:\Users\sofia\Downloads\desktop.ini	SUCCESS	Offset: 0, Length: ...
4:36:05...	evil.exe	3884	QueryBasicInf...	C:\Users\sofia\Downloads\desktop.ini	SUCCESS	CreationTime: 4/2...
4:36:05...	evil.exe	3884	CloseFile	C:\Users\sofia\Downloads\desktop.ini	SUCCESS	
4:36:05...	evil.exe	3884	RegOpenKey	HKLM\Software\Microsoft\Windows\Cu...	SUCCESS	Desired Access: R...
4:36:05...	evil.exe	3884	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Desired Access: R...
4:36:05...	evil.exe	3884	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_DWO...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_SZ, L...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_SZ, L...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_SZ, L...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_EXPA...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_EXPA...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_DWO...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Length: 144
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_DWO...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_SZ, L...
4:36:05...	evil.exe	3884	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	Type: REG_SZ, L...
4:36:05...	evil.exe	3884	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Desired Access: R...
4:36:05...	evil.exe	3884	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows...	SUCCESS	
4:36:05...	evil.exe	3884	RegOpenKey	HKCU\Software\Microsoft\Windows\Cu...	SUCCESS	Desired Access: Q...
4:36:05...	evil.exe	3884	RegOpenKey	HKCU\Software\Microsoft\Windows\Cu...	NAME NOT FOUND	Desired Access: Q...
4:36:05...	evil.exe	3884	RegCloseKey	HKCU\Software\Microsoft\Windows\Cu...	SUCCESS	
4:36:05...	evil.exe	3884	RegOpenKey	HKCU	SUCCESS	Desired Access: R...
4:36:05...	evil.exe	3884	RegOpenKey	HKCU\Software\Microsoft\Windows\Cu...	SUCCESS	Desired Access: R...
4:36:05...	evil.exe	3884	RegCloseKey	HKCU	SUCCESS	

Showing 1,000,027 of 1,434,369 events (69%)   Backed by virtual memory

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.