Lab 2: The Challenge

Jonathan Harijanto

January 26, 2017

CS 373: Defense Against the Dark Arts - Winter 2017

Abstract

The purpose of this blog is to describe the observation from a given forensic case called `Mayflower`. This blog will also provide answers to all the questions given for the challenge.

I. Blog

A. What you looked at:

For this week, each student received a challenge to investigate a raw image from a USB-stick. This image is in the form of a split file called `Image_USB_Mayflower.001`. By pretending to be a forensic investigator for a day, I have a task to analyze the files contained in the Mayflower disk.

B. How you looked at it AND what you found:

The first thing that I need to do was to retrieve the required files from the disk. Thus, I ran my forensic imaging software called FTKImager, clicked on the "Add Evidence Item" button and selected the `Image_USB_Mayflower.001` disk as an Image file. Inside the disk, I found a partition called 'Partition 1' which contained a directory called root. And inside this directory, I found various files named in Korean. Without hesitation, I selected all these files and exported to a new directory in Desktop called 'MyEvidence'.

Since I did not have a single clue about the Korean language, I decided to use Google Translate Picture to identify the name of the files. The results were impressive; I did not expect that some of the file names are very obvious in English. Apparently, the binary file (.bin) is called Rootkit (literally). For the batch file (.bat), the English name is Target. And the English name of the zip file is Targetlist. Thanks to the obvious naming system, I finally had a clue for what to do next.

The next thing I did was to investigate a JPG file called "don't tell mrs Il Ung" because Christiaan said that the zip file password was hidden there. The way I analyzed the JPG file was to open it using a software called FileInsight. Essentially, it is a more-advanced hex editor software used to analyze a file or URL. Without taking too much time, I saw a string embedded in the image that says "pwd: infected123!".

Since I already found the password, I extracted the zip file and entered "infected123!" as the password. It turns out there was a csv file inside the zip called 'Targetlist'. I opened that file using FileInsight and found the answer to challenge question number 1. This csv file contains complete information of the cyber-targets. Apparently, the attacker is planning to attack two different refineries called 'S-Oil Onsan' and 'GS Caltex Yeosu' in South Korea. I was amazed when I noticed that the attacker also listed the name of the IT support manager and the CEO of each company. Furthermore, I also saw a list of IP addresses such as 'S-Oil Infrastructure - 125.135.116.39, Ubiquoss L2 Switch'. Based on my observation, those are the malware targeted IP addresses.

Following the next hint from Christiaan, I examined the binary file (Rootkit.bin) using FileInsight because it contains an embedded malware. In FileInsight program, I used a built-in plugin called "Embedded EXE Extract" to carve the file and display only the executable malware section. In order to analyze what's the malware doing, I needed to apply another plugin named "Strings" in the newly carved file. What "String" did was extracting all the available strings from a file. Here are some of the important strings extracted from the malware:

1) `cmd.exe /q /c net share shared$=%SystemRoot% /GRANT:everyone,FULL`
2) `shared$\system32`
3) hwrcompsvc64.exe
4) diskpartmg16.exe
5) `admin$\system32`
6) taskhosts64.exe
7) KERNEL32.dll
8) SHLWAPI.dll
9) DestroyWindow

By looking on some of these strings, I could already predict the malware's behavior. The command line string gave me a clue that the malware will grant itself a root access. Furthermore, the string 'system32' indicated that the malware would attack that directory. I also noticed that the malware is aiming for a 'KERNEL32.dll' file, which is one of the most important files in Windows to handle memory management.

Lastly, there's also a string 'DestroyWindow' which is a function in Windows to destroy Windows menu and flush all thread message. Clearly, this malware is a destructive malware.

The final hint that Christiaan gave us was to open a skeleton jpg file and use the acronym to find the list of usernames/passwords in the binary file. From this hint, I re-opened the Rootkit.bin using FileInsight and used a plugin called XOR Text Search. The keywords that I tried to XOR search were 'SPED', 'sped', 'SPE', and 'sped'. Among these four, only 'SPE' keywords that yields the most reasonable result. I saw there were four different usernames and passwords listed in the binary file.

The last thing to do in this challenge was to retrieve deleted files from the Mayflower disk. In order to accomplish that, I mounted the Mayflower disk into a virtual Drive E using a software named OSFMount. Next, I used Photorec, a file data recovery software, to retrieve any deleted files in Mayflower image (E:). When the recovery process completed, I was able to extract 26 files. Some of these files were the same with ones I extracted to FTKImager. And some of them seemed like fake, or junk, data because the naming was in weird character. The only difference was the recovered folder had a mp4 file and picture of a refinery (.jpg). Also, the Rootkit file was in an executable (.exe) instead of a binary (.bin) extension.

II. Questions

A. Question 1: What is/ are the cyber-target(s) found on the USB-stick?

The cyber-targets found on the USB-stick are S-Oil Onsan and GS Caltex Yeosu. Both of them are a refinery company in South Korea. Besides the name of the targets, the attackers also have other information about these companies such as the IT support manager's name, the CEO's name and the company website.

B. Question 2: Investigate possible malware and describe the working

The behavior of the malware could be predicted just by looking at the extracted strings from the embedded malware. First, there is a string of command that looks like `cmd.exe /q /c net share shared$=%SystemRoot% /GRANT:everyone,FULL`. As can be seen, the malware will try to grant itself a root access at the beginning of the execution. Next, the string 'system32' indicates that the malware would modify that directory. Furthermore, there is a 'KERNEL32.dll' string which means that the malware is aiming for a Windows file that handles memory management. Last but not least, the string 'DestroyWindow' tells that the malware wants to a call a function that could destroy Windows menu and flushes all thread messages. In conclusion, Rootkit.exe is a destructive malware that will destroy the victim's computer memory and operating system.

C. Question 3: Display the list of usernames/ passwords?

1) Username: Dayals - Password: London13!
2) Username: JHKim4 - Password: Tomorrow33
3) Username: KManku - Password: M@nday77
4) Username: MMccLean3 - Password: @Smiley91

D. Question 4: What was the offset-value you find them?

1) At offset value 0x3ebbd, I found both Dayals-London13! and JHKim4-Tomorrow33
2) At offset value 0x3ebd5, I found both JHKim4-Tomorrow33 and KManku-M@nday77
3) At offset value 0x3ebef, I found both KManku-M@nday77 and MMcLean3-@Simley91

E. Question 5: Which relevant files were deleted and can you replicate them?

The software used to replicate (or recover) the deleted files is called Photorec. This software was able to retrieve 26 files from the Mayflower disk. Some of these files are pictures (.jpg and .png), few of them are videos (.mp4), and the rest are fake data in zip files. The only difference between recovered files and the original files is the extension of Rootkit file. In the original files (extracted using FTKImager), the Rootkit has a binary (.bin) extension instead of executable (.exe).

F. Question 6: What strategy would you advice to the target(s)?

Based on clue obtained from the malware file and the picture of a skeleton, I think the attackers are planning to release the victim's critical information on the internet, then wipe out this information from the target's server. If this prediction is somewhat accurate, then some strategies that the target could do are:

1) Performs backup to all critical information in a secure location.
2) Creates a network isolation for any critical systems.
3) Avoids the use of any external devices.
4) Removes any suspicious email attachment.
5) Uses an artificial intelligence security software to guess the next possible action for any possible security bridge.
6) Configures account privilege in the system to prevent any insider attack.

III. Conclusion

I learned a lot of things from this challenging assignment. First, I developed the skill to investigate an unknown file using FileInsight. Honestly, I'm surprised that I could obtain much information from analyzing the hex format only. Second, I discovered how to recover a disk using Photorec. Again, I'm surprised that a retrieval process is not complicated at all. Lastly, I just learned that it is possible to embed an executable file inside a binary file.