Anaisy Garcia

5734454

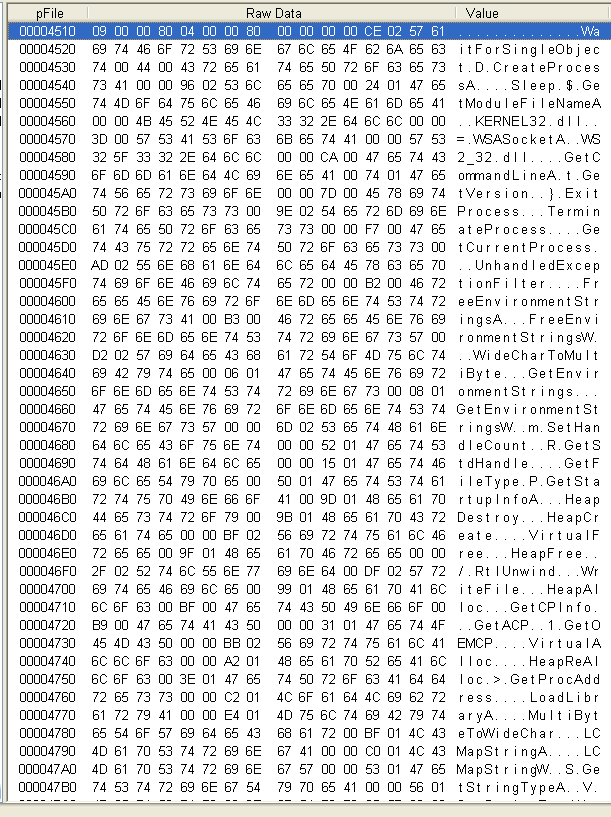
Lab 9-2

Analyze the malware found in the file Lab09-02.exe using OllyDbg to answer the following questions.

Questions

1. What strings do you see statically in the binary?

Imports and string cmd are the only things that can be seen statically in binary.



1. What happens when you run this binary?

When run the program does nothing. It shows up on process monitor and process explorer and immediately leaves.

1. How can you get this sample to run its malicious payload?

The file needs to be renamed ocl.exe before it is run.

1. What is happening at 0x00401133?

A string is being built on the stack. This is what attackers will use to complicate strings.

1. What arguments are being passed to subroutine 0x00401089?

String 1qaz2wsx3edc and a pointer to a buffer of data.

1. What domain name does this malware use?

The malware uses the domain practicalmalwareanalysis.com

1. What encoding routine is being used to obfuscate the domain name?

The program will XOR the programmed DNS name with the string 1qaz2wsx3edc to interpret the domain name.

1. What is the significance of the CreateProcessA call at 0x0040106E?

CreateProcessA is called with cmd as an argument. This means it can create a reverse shell by connecting the socket to the command shell.

Lab 11-1

Analyze the malware found in Lab11-01.exe.

Questions

1. What does the malware drop to disk?

A dll file named msgina32.dll from TGAD.

1. How does the malware achieve persistence?

The program installs mdgina32.dll onto the system and adds it to the registry location HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL. This has it load after a system reboot.

1. How does the malware steal user credentials?

The program can interrupt all user identifications submitted to the system for verification.

1. What does the malware do with stolen credentials?

The stolen credentials are logged onto %SystemRoot%\System32\msutil32.sys with a time.

1. How can you use this malware to get user credentials from your test environment?

Logging out and logging back in shows the identifications on the log file.

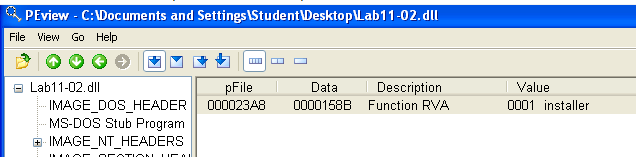
Lab 11-2

Analyze the malware found in Lab11-02.dll. Assume that a suspicious file named Lab11-02.ini was also found with this malware.

Questions

1. What are the exports for this DLL malware?

Installer



1. What happens after you attempt to install this malware using rundll32.exe?

The program copies itself to the windows system directory as spoolvxx32.dll then install itself in AppInit\_DLLs and tries to open Lab11-02.ini.

1. Where must Lab11-02.ini reside in order for the malware to install properly?

Since it cannot open Lab11-02.ini we must put it within %SystemRoot%\System32\ so it can then run.

1. How is this malware installed for persistence?

The program installs itself in the AppInit\_DLLs registry which then loads itself onto anything with User32.dll.

1. What user-space rootkit technique does this malware employ?

The program installs an inline hook of the send function.

1. What does the hooking code do?

Checks if the outgoing packet is an email message that contains RCPT TO:. When found it adds onto it with a malicious email.

1. Which process(es) does this malware attack and why?

The program only attacks things that use email. Therefore, MSIMN.exe, THEBAT.exe, and OUTLOOK.exe.

1. What is the significance of the .ini file?

Contains [billy@malwareanalysisbook.com](mailto:billy@malwareanalysisbook.com) a encrypted email.

1. How can you dynamically capture this malware’s activity with Wireshark?

Running a fake mail server and sending an email then following the TCP stream.