Anaisy Garcia

PID 5734454

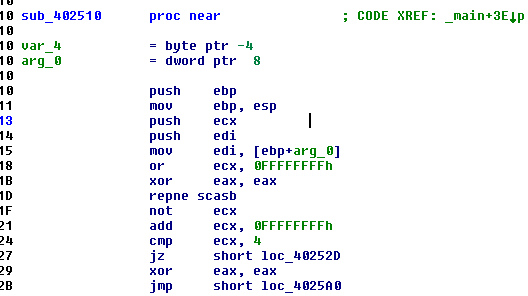
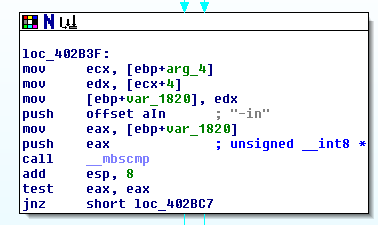
**Lab 9-1**

Analyze the malware found in the file *Lab09-01.exe* using OllyDbg and IDA Pro to answer the following questions. This malware was initially analyzed in the Chapter 3 labs using basic static and dynamic analysis techniques.

***Questions***

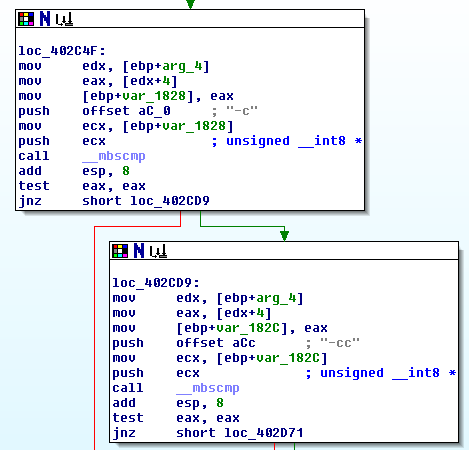
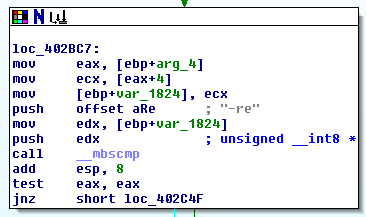
1. How can you get this malware to install itself?

This malware installs itself with a password which was abcd and the option -in which tells the malware to install itself. Therefore “Lab09-01.exe -in abcd”.



1. What are the command-line options for this program? What is the password requirement?

The command line options for the program is one of the four values given in strings. -in tells the malware to install itself, -re does the uninstalling, -c causes the program to self-update, and -cc tells the program to print the configuration. The password is abcd and it is essential by the program to do all the actions except the normal actions.



1. How can you use OllyDbg to permanently patch this malware, so that it doesn’t require the special command-line password?

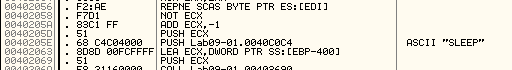
To permanently path the program, you need to patch the binary by changing the first bytes of the function located in 402510 to true. B801000000C3.

1. What are the host-based indicators of this malware?

The program creates a registry key HKLM\Software\Microsoft\XPS\Configuration, a service called XYZ Manager Service, and copies itself to the system.

1. What are the different actions this malware can be instructed to take via the network?

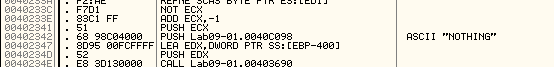
The program can execute five commands. Sleep which makes the program sleep, upload which reads a network file and writes it to the system, download which sends the file over to the remote host, cmd which is what executes the shell command, and nothing which does nothing.











1. Are there any useful network-based signatures for this malware?

The program goes to <http://www.practicalmalwareanalysis.com> and has HTTP Get requests.

