HW-4

(CPRE 538-Spring 2023)

Please submit as many screenshots as you can to show that you found the answer in Ghidra and OllyDbg.

Preparation: Please install OllyDbg (https://www.ollydbg.de/download.htm, OllyDbg 1.10)

Q-1) Analyze the malware found in the file Lab09-01.exe using OllyDbg and Ghidra to answer the following questions. (50pt)

a) How can you get this malware to install itself? (10pt)

b) What are the command-line options for this program? What is the password requirement? (10pt)

c) How can you use OllyDbg to permanently patch this malware, so that it doesn't require the special command-line password? (10pt)

d) What are the host-based indicators of this malware? (5pt)

e) What are the different actions this malware can be instructed to take via the network? (10pt)

f) Are there any useful network-based signatures for this malware? (5pt)

Q-2) Analyze the malware found in the file lab09-02.exe using OllyDbg to answer the following questions. (50pt)

a) What strings do you see statically in the binary? (5pt)

b) What happens when you run this binary? (5pt)

c) How can you get this sample to run its malicious payload? (10pt)

d) What is happening at 0x00401133? (10 pt)

e) What arguments are being passed to subroutine 0x00401089? (5pt)

f) What domain name does this malware use? (5pt)

g) What encoding routine is being used to obfuscate the domain name? (10pt)