**Labs 9. OllyDbg**

**Lab9-1>**

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

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

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

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

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

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

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

**Lab9-2>**

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

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

**2. What happens when you run this binary?**

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

**4. What is happening at 0x00401133?**

**5. What arguments are being passed to subroutine 0x00401089?**

**6. What domain name does this malware use?**

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

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

**Lab9-3>**

**Analyze the malware found in the file Lab09-03.exe using OllyDbg and IDA Pro. This malware loads three included DLLs (DLL1.dll, DLL2.dll, and DLL3.dll) that are all built to request the same memory load location. Threrefore, when viewing these DLLs in OllyDbg versus IDA Pro, code may appear at different memory locations. The purpose of this lab is to make you comfortable with finding the correct location of code within IDA Pro when you are looking at code in OllyDbg.**

**1. What DLLs are imported by Lab09-03.exe?**

**2. What is the base address requested by DLL1.dll, DLL2.dll, and DLL3.dll?**

**3. When you use OllyDbg to debug Lab09-03.exe, what is the assigned based address for: DLL1.dll, DLL2.dll, and DLL3.dll?**

**4. When Lab09-03.exe calls an import function from DLL**