

Practical Malware Analysis Lab 3-3

Questions

1. What do you notice when monitoring this malware with Process Monitor?
2. Can you identify any live memory modifications?
3. What are the malware's host based indicators?
4. What is the purpose of this program?

Static Analysis

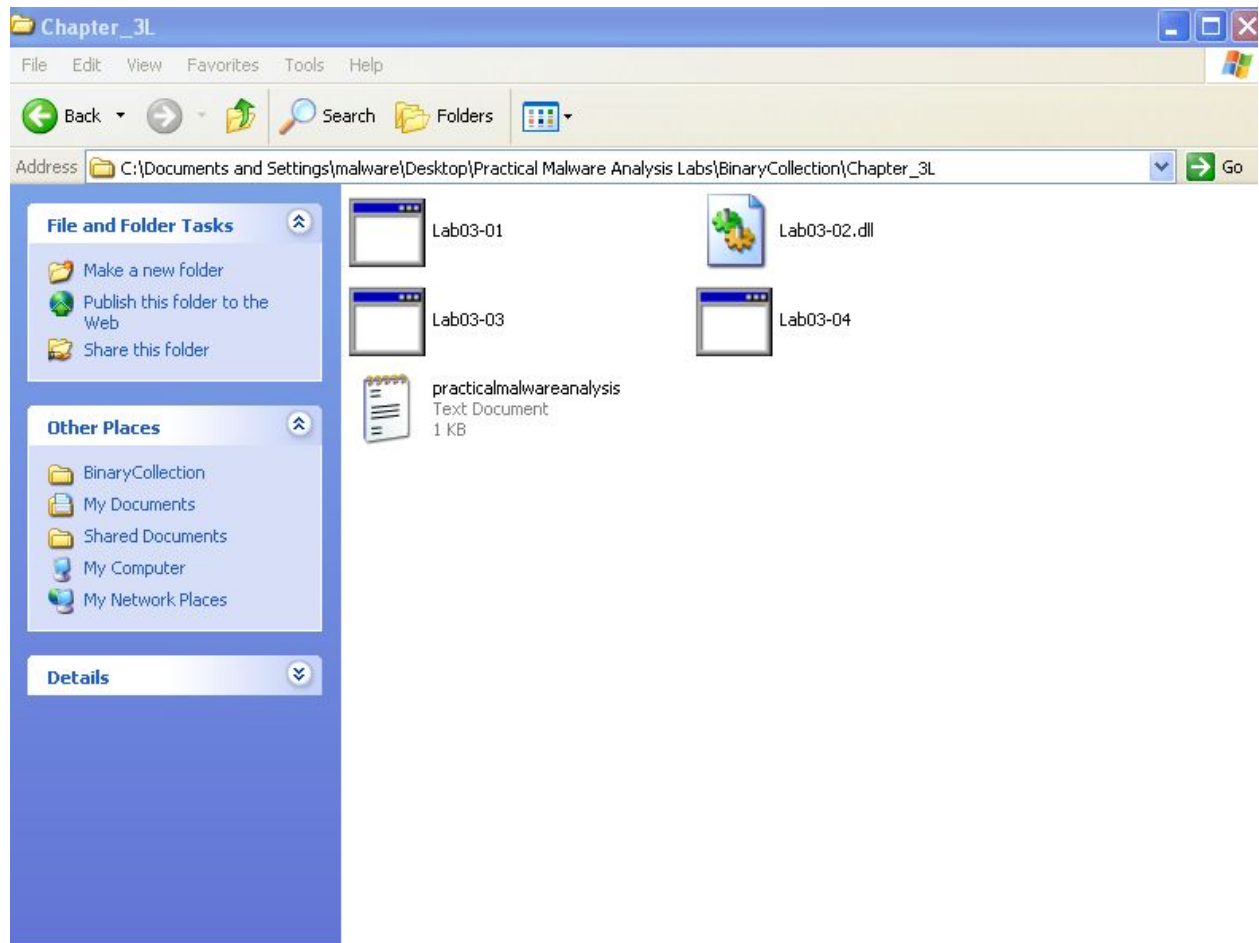
File: Lab03-03.exe

Imports: Kernel32.dll

Kernel32.dll → Closehandle, [CreateFile](#), [CreateProcessA](#), ExitProcess, FindResourceA, [FreeEnvironmentStringA](#) / [W](#), [GetCPInfo](#), [GetCommandLineA](#), [GetCurrentProcess](#), GetFileSize, LoadResource, LockResource, ReadProcessMemory, Sleep, [WriteFile](#), VirtualFree, WriteProcessMemory

000000005058 000000405058 0 ntdll.dll

Dynamic Analysis



Whenever the malware is run it immediately kills itself and disappears, but the log file keeps updating. By filtering procmon by the operation WriteFile this allows us to see what is still writing to the file.

4:00:3...	svchost.exe	988	WriteFile	C:\Documents and Settings\malware\D...	SUCCESS	Offset: 0, Length: 12
4:00:3...	svchost.exe	988	WriteFile	C:\Documents and Settings\malware\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log		
4:00:3...	svchost.exe	988	WriteFile	C:\Documents and Settings\malware\D...	SUCCESS	Offset: 22, Length: 4
4:00:3...	svchost.exe	988	WriteFile	C:\Documents and Settings\malware\D...	SUCCESS	Offset: 26, Length: 1
4:00:3...	svchost.exe	988	WriteFile	C:\Documents and Settings\malware\D...	SUCCESS	Offset: 27, Length: 1
4:00:3...	svchost.exe	988	WriteFile	C:\Documents and Settings\malware\D...	SUCCESS	Offset: 28, Length: 1

The program svchost.exe is writing to the log file! The malware must infect this file.

Question 1

The program immediately kills itself when run.

Question 2

Svchost is writing to the keyloggers log file.

Question 3

The hundreds of registry entries such as

HKU\S-1-5-21-2000478354-1202660629-839522115-500\Software\Microsoft\MediaPlayer\Battery\Presets\Nerds Are Cool

HKU\S-1-5-21-2000478354-1202660629-839522115-500\Software\Microsoft\MediaPlayer\Battery\Presets\Nerds Are Cool\CurrentShiftInfo

HKU\S-1-5-21-2000478354-1202660629-839522115-500\Software\Microsoft\MediaPlayer\Battery\Presets\Nerds Are Cool\CurrentShiftInfo\0

HKU\S-1-5-21-2000478354-1202660629-839522115-500\Software\Microsoft\MediaPlayer\Battery\Presets\Nerds Are Cool\PostShiftInfo

HKU\S-1-5-21-2000478354-1202660629-839522115-500\Software\Microsoft\MediaPlayer\Battery\Presets\Nerds Are Cool\PostShiftInfo\0

Question 4

This malware is a keylogger.