Practical Malware Analysis Lab 3-4

Questions

1. What happens when you run this file?
2. What is causing the roadblock for dynamic analysis?
3. Are there other ways to run this program?

Static Analysis

Strings gathered using binText

00000000B170 00000040B170 0 command.com
00000000B554 00000040B554 0 JanFebMarAprMayJunJulAugSepOctNovDec
00000000B53C 00000040B53C 0 SunMonTueWedThuFriSat
00000000C0D4 00000040C0D4 0 >> NUL
00000000C0CC 00000040C0CC 0 cmd.exe
00000000C0C4 00000040C0C4 0 SLEEP
00000000C0B8 00000040C0B8 0 UPLOAD
00000000C0AC 00000040C0AC 0 DOWNLOAD
00000000C098 00000040C098 0 NOTHING
00000000C070 00000040C070 0 HTTP/1.0
00000000C134 00000040C134 0 %SYSTEMROOT%\system32\
00000000C0E8 00000040C0E8 0 http://www.practicalmalwareanalysis.com
00000000C14C 00000040C14C 0 k:%s h:%s p:%s per:%s

Imports

Kernel32.dll → CopyFileA, CreateFileA, CreateProcessA, DeleteFileA, GetCommandLineA, GetCurrentProcess, Sleep, WriteFile, GetSystemTime, GetTimeZoneInformation, GetSystemDirectoryA, GetProcAddress, GetModuleHandleA,GetLocalTime, ReadFile, SetEnvironmentVariableA, SetFileTime …. etc

ADVAPI32.dll → ChangeServiceConfigA, CloseServiceHandle, CreateServiceA, DeleteService, OpenSCManagerA, OpenServiceA, RegCreateKeyExA, RegDeleteValueA, RegOpenKeyExA, RegQueryValueExA, RegSetValueExA

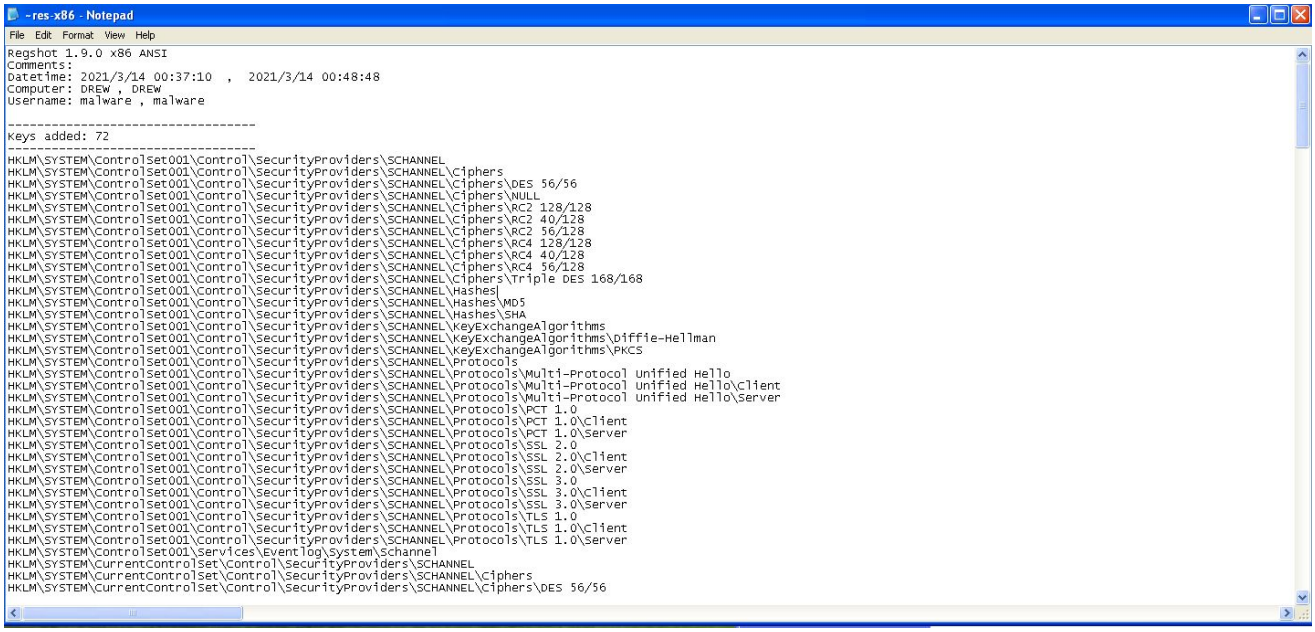
SHELL32.dll → ShellExecuteA

WS2_32.dll → closesocket, connect, htons, recv, send, shutdown, socket, gethostbyname, WSAStartup, WSACleanup

Dynamic Analysis

When I ran the executable from cmd it deleted itself.

RegShot Results



Question 1

The file deletes itself

Question 2

The file is very sneaky this malware requires a more in depth analysis. I think it may be a logic bomb because of the various functions including getting the system and local time. Maybe also this program needs some type of argument.

Question 3

You can run it either from double clicking it or running it from CMD.