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?

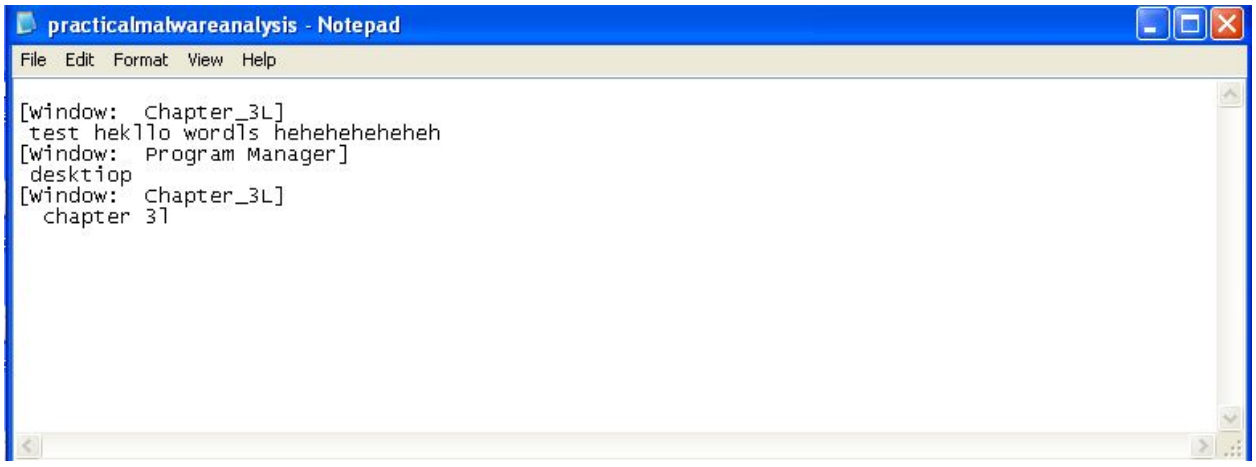
Static Analysis

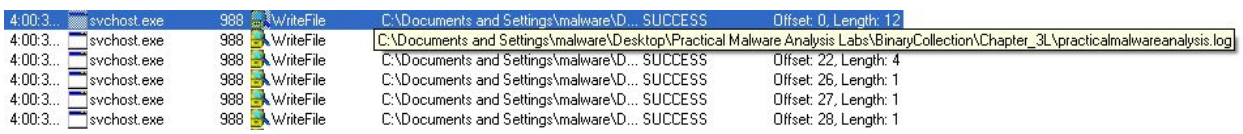
File: Lab03-03.exe
Imports: Kernel32.dll

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

Dynamic Analysis

Whenever the malware is run it immediately kills itself and disappears. The malware creates the text document practicalmalwareanalysis.log and inside it is recorded keystrokes and the programs the user is using.Even though the malware closes itself immediately the log file keeps updating. By filtering procmon by the operation WriteFile this allows us to see what is still writing to the file.





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

Regshot Results

```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2021/3/13 22:56:58  ,  2021/3/13 22:59:30
Computer: DREW , DREW
Username: malware , malware

----------------------------------
Keys added: 9
----------------------------------
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\ShellNew
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.log
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.log\OpenWithList
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.log\OpenWithProgids
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.log
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012021031320210314
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Notepad

----------------------------------
Values added: 140
----------------------------------
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\ShellNew\Briefcase:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 00 72 00 69 00 65 00 66 00 63 00 61 00 73 00 65
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 00 72 00 69 00 65 00 66 00 63 00 61 00 73 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\ShellNew\Bitmap Image:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 00 69 00 74 00 6D 00 61 00 70 00 20 00 49 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 69 00 6E 00 74 00 2E 00 50 00 69 00 63 00 74 00 75 00 72 00 65 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\ShellNew\Wordpad Document:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 6F 00 72 00 64 00 70 00 61 00 64 00 2
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 6F 00 72 00 64 00 50 00 61 00 64 00 2E 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2E 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\ShellNew\Rich Text Document:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 00 69 00 63 00 68 00 20 00 54 00 65 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 72 00 74 00 66 00 66 00 69 00 6C 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\ShellNew\Text Document:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 00 65 00 78 00 74 00 20 00 44 00 6F 00 63 0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 00 78 00 74 00 66 00 69 00 6C 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\ShellNew\Wave Sound:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 61 00 76 00 65 00 20 00 53 00 6F 00 75 00 6E
```

```
----------------------------------
Values modified: 3
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  21 18 81 40 C8 AA 0D 78 9D 17 45 48 AB 5C 56 6D 7E 25 F2 42 3C 4D C3 46 D7 93 6B 4E 72 09 D7 30 58 2B 76 29 C9 CF
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  E2 CA 88 1B D8 D8 DD 5F D5 0F F6 EE 35 0F 7B F8 C2 7F 36 F6 21 C0 16 C4 CE 35 E9 2A 50 29 45 04 1E 12 43 47 11 69
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\SessionInformation\ProgramCount: 0x00000003
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\SessionInformation\ProgramCount: 0x00000004

----------------------------------
Files added: 6
----------------------------------
C:\Documents and Settings\malware\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\practicalmalwareanalysis.log
C:\Documents and Settings\malware\Local Settings\History\History.IE5\MSHist012021031320210314\index.dat
C:\Documents and Settings\malware\Recent\Chapter_3L.lnk
C:\Documents and Settings\malware\Recent\practicalmalwareanalysis.lnk
C:\WINDOWS\Prefetch\LAB03-03.EXE-235C8BE6.pf
C:\WINDOWS\Prefetch\NOTEPAD.EXE-336351A9.pf

----------------------------------
Files [attributes?] modified: 6
----------------------------------
C:\Documents and Settings\malware\NTUSER.DAT
C:\Documents and Settings\malware\NTUSER.DAT.LOG
C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf
C:\WINDOWS\system32\config\software.LOG
C:\WINDOWS\system32\wbem\Logs\wmiprov.log

----------------------------------
Folders added: 1
----------------------------------
C:\Documents and Settings\malware\Local Settings\History\History.IE5\MSHist012021031320210314
```

Question 1

The program immediately kills itself when run.

Question 2

Svchost is writing to the keyloggers log file.

Question 3

The log file practicalmalwareanalysis.log

Question 4

This malware is a keylogger.