Lab 4 Solutions

Lab 4 - The case of Trojan Small

During your investigation of an infected system, you come across a file (***bas.exe***). Analyze this file and answer the following questions:

1. What is the name of the file dropped by the malware? In which directory the file is dropped?
2. How is malware persisting on the system?
3. Can you open the registry editor (regedit.exe) and identify the entry added by the malware?
4. Can you spot the malicious process in the task manager (taskmgr.exe)?

01. What is the name of the file dropped by the malware? In which directory the file is dropped?

Upon execution, ***bas.exe*** drops a file ***LSPRN.EXE*** in ***C:\Windows*** directory.

```
[CreateFile] bas.exe:2192 > %WinDir%\LSPRN.EXE
```

02. How is malware persisting on the system?

Malware adds the entry in the run registry key so that the malicious program can start every time the system starts.

```
[RegSetValue] bas.exe:2192 > HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Printe
rSecurityLayer = C:\Windows\LSPRN.EXE
```

03. Can you open the registry editor (regedit.exe) and identify the entry added by the malware?

Malware prevents you from opening the registry editor, this is achieved by setting the below registry value.

```
[RegSetValue] LSPRN.EXE:2488 > HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Image File Execution Options\regedit.exe\Debugger  =  0
```

Even though the malware prevents launching registry editor, you can still query the registry or delete the entry added by the malware using ***reg*** utility as shown here:

```
C:\> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\regedit.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\regedit.exe
    Debugger    REG_SZ    0
```

```
reg delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\regedit.exe" /v debugger
Delete the registry value debugger (Yes/No)? yes
The operation completed successfully.
```

04. Can you spot the malicious process in the task manager (taskmgr.exe)?

Malware also prevents you from opening task manager, this is achieved by setting the below registry value. You can delete this entry using ***reg*** utility as shown earlier.

```
[RegSetValue] LSPRN.EXE:2488 > HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Image File Execution Options\taskmgr.exe\Debugger  =  0
```