Lab 5 Solutions

Lab 5 - The Case of Brontok Worm

While investigating a suspect system for possible compromise, you find a suspect file (***tux.exe***). You also notice that when you try launching registry editor (***regedit.exe***) on the infected system, instead of registry editor notepad is invoked. Analyze the sample (tux.exe) and answer these questions:

1. Which executable files are created by the malware?
2. Apart from the entry added in the Run registry key, Which other registry entries are added by malware for persistence?
3. Why do you think notepad is launched, instead of registry editor? and which another legitimate application is targeted using the similar technique?

Answers

01. Which executable files are created by the malware?

Malware creates various files, the following are some the executable files created by the malware.

```
[CreateFile] tux.exe:2848 > %WinDir%\M68162\EmangEloh.exe
[CreateFile] tux.exe:2848 > %WinDir%\M68162\smss.exe
[CreateFile] tux.exe:2848 > %WinDir%\SysWOW64\X84667go\Z451621cie.cmd
[CreateFile] tux.exe:2848 > %WinDir%\sa-188511.exe
[CreateFile] tux.exe:2848 > %WinDir%\Ti078306ta.exe
[CreateFile] tux.exe:2848 > %WinDir%\M68162\Ja280254bLay.com
[CreateFile] tux.exe:2848 > %WinDir%\SysWOW64\4516210783061.exe
```

02. Apart from the entries added in the Run registry key, which other registry entries are added by malware for persistence?

In addition to the entries in the ***Run*** registry key, the Brontok worm achieves persistence by modifying the following Winlogon registry values with its malicious executables:

```
[RegSetValue] smss.exe:2492 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion
\Winlogon\Shell  =  explorer.exe, ""C:\Users\training\AppData\Roaming\Microsoft
\Windows\Templates\O06060Z\TuxO06060Z.exe

[RegSetValue] smss.exe:2492 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion
\Winlogon\Userinit  =  C:\Windows\system32\userinit.exe , ""C:\Windows\M68162\Ja280254bLay.com
```

03. Why do you think notepad is launched, instead of registry editor? and which another legitimate application is targeted using the similar technique?

Malware prevents you from opening the registry editor (***regedit.exe***), this is done adding the below entry which sets the debugger for ***regedit.exe*** to ***notepad.exe***. As a result of adding this registry entry notepad is launched instead of ***regedit.exe***. The other application that is targeted with a similar technique is ***msconfig.exe***

```
[RegSetValue] smss.exe:2492 > HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Image File Execution Options\regedit.exe\debugger  =  C:\Windows\notepad.exe
```

```
[RegSetValue] smss.exe:2492 > HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
\Image File Execution Options\msconfig.exe\debugger  =  C:\Windows\notepad.exe
```