SPYWARES ANALYSIS

Danilo Vizzarro

info@danilovizzarro.it

2 May 2007

Trojan Horses and Spywares

A trojan horse is a malware composed by a client and a server. All the attacker needs to do, is to find a way to install the server on the target machine. After that, using the client, he will be able to have the full control of the victim.
A spyware, instead, is a malware that collects informations about the user. Generally the Trojan Horses implement spyware features.
In this paper we will examine 4 different spywares: Spy Sheriff, Spy Locked, Spy Axe and Spy Tropper.

Spy Sheriff

This is a program that simulates to be an anti-spyware. It's not so easy to remove because it reinstalls itself in some hidden part of the hard disk. Trying to remove it using the Windows Add/Remove program feature, may cause the crash of the system. The aim of Spy Sheriff is to trick the user to buy the full rogue version of the software. Following the features of the program.

- It can stop the internet connection and show a blue screen containing the message:

  ```
  The system has been stopped to protect you from Spyware.
  ```

- It can replace the desktop wallpaper with a blue screen containing the message:

  ```
  SPYWARE INFECTION! Your system is infected with spyware.
  Windows recommends that you use a spyware removal tool
  to prevent loss of data. Using this PC before having it
  cleaned of spyware threats is highly discouraged.
  ```

- It create another account with administrator's privileges, to be able to deny the access to some utilities.
- It bocks the Windows System Restore utility. In any case this utility will remain available if Windows is executed in Safe Mode.
- It deny the access to some websites from where is possible to download anti-spyware software.

Spy Locked

This is another program that generates fake security massages alleging that the computer is infected by some spywares. It's quite difficult to remove because it could reinstall himself also when it's partially removed. It blocks the Windows Add/Remove program feature and removing it manually could generate a system crash. His aim, like Spy Sheriff, is to trick the user to buy the full rogue version of the program. Following the features of Spy Locked.

- It generates an huge amount of advertising popups.
- It may show an icon on the system tray. Clicking on it it will display a message of this kind

  ```
  The system has detected a number of active spyware
  applications that may impact on the performance of
  ```

```
your computer. Click the icon to get rid of unwanted
spyware by downloading an up-to-date anti-spyware
solution.
```

- It generates many other processes that can't be stopped.
- As Spy Sheriff, it deny the access to some website from where is possible to download anti-spyware software.

Spy Axe

Also this program pretend to be an anti-spyware software. Spy Axe will be downloaded, by another trojan like Zlob that has already infected the target machine. This trojan will display on the system tray an icon with a popup that allege that the computer is infected. When the popup is clicked, it will start the download and the installation of Spy Axe that will detect some spywares and will ask the user to go on the Spy Axe website to buy the software before to allow the removal. Following the features of Spy Axe.

- It may change the desktop wallpaper.
- It may change the Internet Explorer homepage.
- It will install the processes mscornet.exe, mssearchnet.exe, nvctrl.exe, spyaxe.exe.
- It will install the DDLs ioctrl.dll svchosts.dll, webconm.dll, wbeconm.dll.
- It will create the directories C:\Program Files\SpyAxe, C:\Windows\System\1024, C:\Windows\System32\1024, C:\Winnt\System32\1024.

Spy Trooper

This is another example of fake anti-spyware software that warns the user about non existing threats. Only when the full version of the program is purchased, the computer is supposed to be clean and the threats are not detected anymore. Spy Trooper uses some exploits to be downloaded automatically if you are surfing on adult or warez websites. Once downloaded, it will display an icon on the system tray, that will let you believe that the computer has no protection. Following the features of Spy Trooper.

- It may generate a popup windows alerting about the presence of some spyware.
- It creates a Spy Tropper shortcut link on the desktop.
- It will create a directory called SPYTROOPER in the Program Files folder containing several files inside.
- It will create a directory called SPYTROOPER in the Start menu containing several files inside.
- It will create new entries in the Windows Registry.