ABI SOFTWARE DEVELOPMENT

Written by: Adam Berent

Defending Against a Trojan Horse

One of the deadliest and easiest ways to attack a PC is to use a Trojan Horse. Unlike a virus a Trojan Horse does not attach itself to another file but contains all of the executable code in itself. Simply put it is malicious software.

There are many categories of Trojan Horses. Some are destructive in nature and do damage to your systems. Other will monitor your computer activities and report back to their creator. Others still just place advertisements and/or shortcuts that try to sell you stuff. Some people will call certain types of Trojan Horses different names such as spamware and spyware. For the duration of this paper I will place them all in the same category and call them Trojan Horses.

Most of the time a Trojan Horse relies on you, the system's user to double click on it and initiate its malicious code. In most cases this is not so hard to accomplish. Many of the Trojan Horses rely on what is called Social Engineering, which basically means using human nature against unsuspecting users. Actually it is much easier then to use Social Engineering then to remotely force yourself through the users computer defenses such as firewalls and routers. For example consider emailing a Trojan Horse called sex.exe to potential victims. This file name guarantees that a certain percentage of people will be tempted to open it and become infected. There are of course better ways to do it. Smarter file names will give you a better percentage of infected users. Often however Trojan Horses can be actually attached to software you download off the Internet. For example some freeware programs will often install software that will monitor your computer activity or display certain advertisements. These are often called spamware or spyware.

Once a Trojan Horse gets through your defenses and runs on your PC it will probably move to a new and safer destination. For example if you run the sex.exe Trojan Horse on your desktop it would probably install itself somewhere deep in your system before actually executing its payload. This way when you delete the sex.exe program from your PC, the Trojan Horse will survive. A popular place for hiding Trojan Horses is your Windows or Systems directory however anywhere out of sight is good. Once copied onto your system the Trojan Horse will have to find a way to get executed over and over again without your permission. Most Trojan Horses add themselves to the Windows Startup sequence so that they get executed every time your computer starts. There are many ways a Trojan Horse can accomplish this. It is important that we take a close look at these different tactics and study them. Checking these places is the best way to check if your system is infected and to remove the malicious files.

C:\WINDOWS\Start Menu\Programs\StartUp

This is the first place you should look. It is hardly ever used by Trojan Horses because it is easy to find and most users know about it. Any file found in the C:\WINDOWS\Start Menu\Programs\StartUp directory will automatically run when Windows starts. However not every file in that folder is necessarily a Trojan Horse. It is up to you to know your PC and to recognize the files you have installed from the files you have not. Any files that do not belong in that directory can be removed safely however make sure that it is not something you need and use.

Registry Keys

Any key in the following paths will get executed at startup. Again make sure the keys you remove are not windows components or keys for software that you use. Some of the software that validly uses these keys are Virus Scanners, Fire Walls and even your Windows operating system. Be careful not to remove any of the valid keys. Registry is most often used by the Trojan Horses since they are harder to access and find as well the fact that many users are unaware of its existence.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
```

You can safely access these registry keys by clicking on the Start button in the lower left part of your screen, then choosing Run and typing in: regedit. This will bring up a registry editor where you can search for the above key entries and look at what values they contain. If you do find any keys that you think should not belong there you should first carefully write them down on a piece of paper and then delete them from the registry. In case they turn out to be valid keys you can always place them back by using the piece of paper created in the previous step. You should never try to delete more then one key at a time. You will also have to restart your computer after changing or deleting a key in order for the changes to take effect.

System.ini

System.ini is very unusual. It is used by a few Trojan Horses and is very hard to find for any inexperienced user. The System.ini file is located in the C:\WINDOWS directory in Windows 9*/Me and in the C:\WINNT directory in Windows NT/2000/XP

You can open the file by double clicking it. In the first paragraph of the file you should find lines that look similar to this:

```
[boot]
shell=Explorer.exe
```

Any file name you place after the shell=Explorer.exe will be executed at startup. An infected file can look like this:

```
[boot]
shell=Explorer.exe TrojanHorse.exe
```

There are other ways of storing a Trojan Horse on your PC. Other new ingenious attacks are being thought of almost all the time. To further protect yourself I suggest own an updated Antivirus software such as one available from www.symantec.com. I also suggest you download a personal fire wall such as Zone Alarm available at www.zonelabs.com as well as a great spamware and spyware scanning software called Ad-aware from www.lavasoftUSA.com.

There is nothing you can do to guarantee that you will never fall victim to a Trojan Horse, however the information you have just read will go a long way to help you protect yourself and in case of an infection remove the damaging components from your PC.

This paper was written by Adam Berent and can be distributed without copyright as long as proper credit is given. If you would like to contact me feel free to do so at aberent@abisoft.net or visit www.abisoft.net.