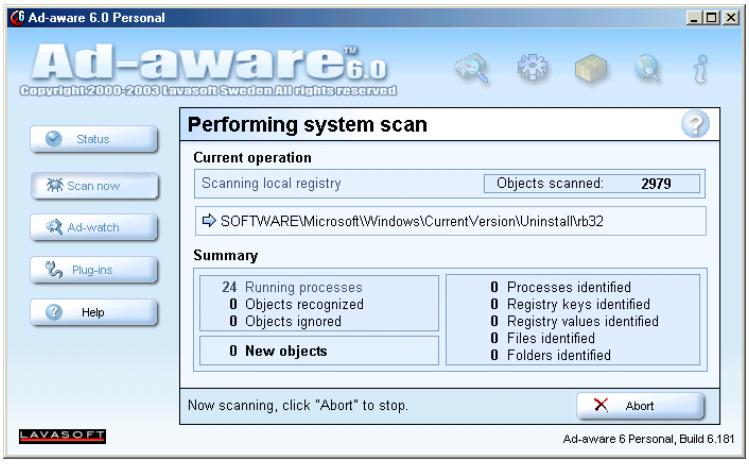
Spyware and Adware Defence

by Edmond Ng

John is about to click on a hyperlink while surfing the Internet, when a pop-up advertisement appears and is clicked instead. He then closes all the pop-up advertisements and continues his surfing without realising that his last action has triggered an installation of a program running in the background on his PC. When John works on his PC the next time, he faces occasional advertisements pop-ups on his computer screen even when the Internet is disconnected.

Jane downloads a program from a website offering freebies like screen savers, games, or pictures. After scanning the files to ensure there is no virus, she installs the program, unaware that another program is also being installed in the background on her PC. The next time she uses the PC, she finds occasional pop-up advertisements appearing on her computer screen.

These are two common scenarios of how adware and spyware can unknowingly be installed into a PC. The dangers faced by PC users today are bountiful. Not only are viruses, worms, and malicious programs lurking in almost every PCs connected to the Internet, there are also the spyware and adware that can seriously affect computer performance, infringe PC security, and intrude privacy.



The quickest way to find out whether a PC has malicious programs is to do a CTRL+ALT+DELETE and observe whether any program processes that are unfamiliar or are known spyware or adware. If you are a frequent user of the Internet, it is likely that your PC may have been invaded by more than one of these programs.

Getting rid of these programs is not at all easy, as it usually writes into

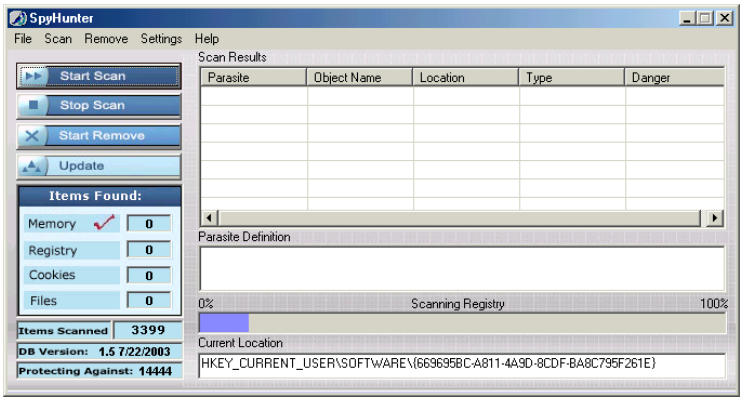
the Windows registry, creates directories in your Program Files folder, and cannot completely uninstall itself even if you perform a program removal through the Control Panel. Certain spyware programs also write parameters in the registry that ensures it gets reinstalled if deleted or uninstalled.

Fortunately, there are many software out there that helps you detect and remove spyware and adware programs conveniently, but these solutions can be costly. For the price conscious and those who cannot afford the cost, the alternative is to use freeware.

Freeware can help solve many problems, but being free, it is understandable why most comes with certain limitations or conditions. A good place to begin searching for free software is at http://download.com.

Three of the more popular and frequently used anti-spyware and anti-adware freeware are *Ad-aware*, *Spybot*, and *SpyHunter*.

Ad-aware scans and detect memory, program processes, registry, files, and folders before it removes all suspicious and malicious known parameters. The program provides a preview that allows users to select what to be and not to be removed before execution. *Ad-aware* comes with regular updates for detection that should be performed before scanning. The difference between the free version and the paid version is in the function, *Ad-watch*, which is a resident program that provides preventive action against installation of malicious program. This means that if you are using the freeware version, you must regularly run the program to provide anti-spyware and anti-adware support.



Spybot is functionally similar to *Ad-aware*. It has a quarantine option that registers objects removed for each session, which can be recovered if required. This quarantine objects, however, must be removed manually if no longer needed. *Spybot* also provides the option to set search exclusions and immunisation on the Internet Explorer. The *immunize* function blocks known bad products from installing into your PC. The

program is a fully functional and is not tagged with a price. Information for optional donation is included in the Help menu.

SpyHunter is an anti-spyware scanning program, which provides extensive information on the exact location of registry parameters, folders, and files. The free version does not provide automated removal of spyware or adware. Its primary purpose is to inform, and if you are technically competent, you can manually remove the registry parameters, folders, and files one-by-one. Detection scanning for this program is somewhat slow, but may be more extensive than other anti-spyware programs. *SpyHunter* automatically starts on boot-up – even if you do not want it to do so. The only way to get rid of the program from starting up during Windows login (even after it has been uninstalled), is to remove the program statement in the registry manually:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Run\...SpyHunter

For frequent users of the Internet, the anti-spyware program is best run at least once a week. Each time before executing scan, ensure that program is updated. Consider running more than one of these programs where necessary, as not all spyware or adware is detectable by a single program. As part of preventive measures, do not sign-up or install programs that are not necessary for your PC and do not click on links provided by spam e-mail or advertisement banners.

Glossary

Spyware. Any technology that aids in gathering information about a person or organisation without their knowledge. On the Internet, spyware can be a program that is installed in someone's computer secretly which is used to relay information to advertisers or other interested parties. Spyware can also be in the form of a software virus.

Adware. Any software application that displays advertising banners while program is running. Adware applications deliver advertisements which may be viewed through pop-up windows or through a bar that appears on a computer screen.

The author of this article is a freelance writer @ http://www.writers.net/writers.
Email: journalist@edvencomm.net; Web: http://www.edvencomm.net