OS Security - Windows: Antiviruses, Antispyware, Vulnerability Scanners

Adware

Adware or advertising-supported software is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.

Computer virus

A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term "virus" is also commonly used, albeit erroneously, to refer to many different types of malware programs. The original virus may modify the copies, or the copies may modify themselves, as occurs in a metamorphic virus. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a floppy disk, CD, or USB drive. Meanwhile viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer. Viruses are sometimes confused with computer worms and Trojan horses. A worm can spread itself to other computers without needing to be transferred as part of a host, and a Trojan horse is a file that appears harmless. Both worms and Trojans will cause harm to computers when executed.

- Timeline of notable computer viruses and worms (http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms)
- List of computer viruses (http://en.wikipedia.org/wiki/List_of_computer_viruses)

Computer worm

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Malware

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau of the words malicious and software. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.

Malware should not be confused with defective software, that is, software which has a legitimate purpose but contains harmful bugs.

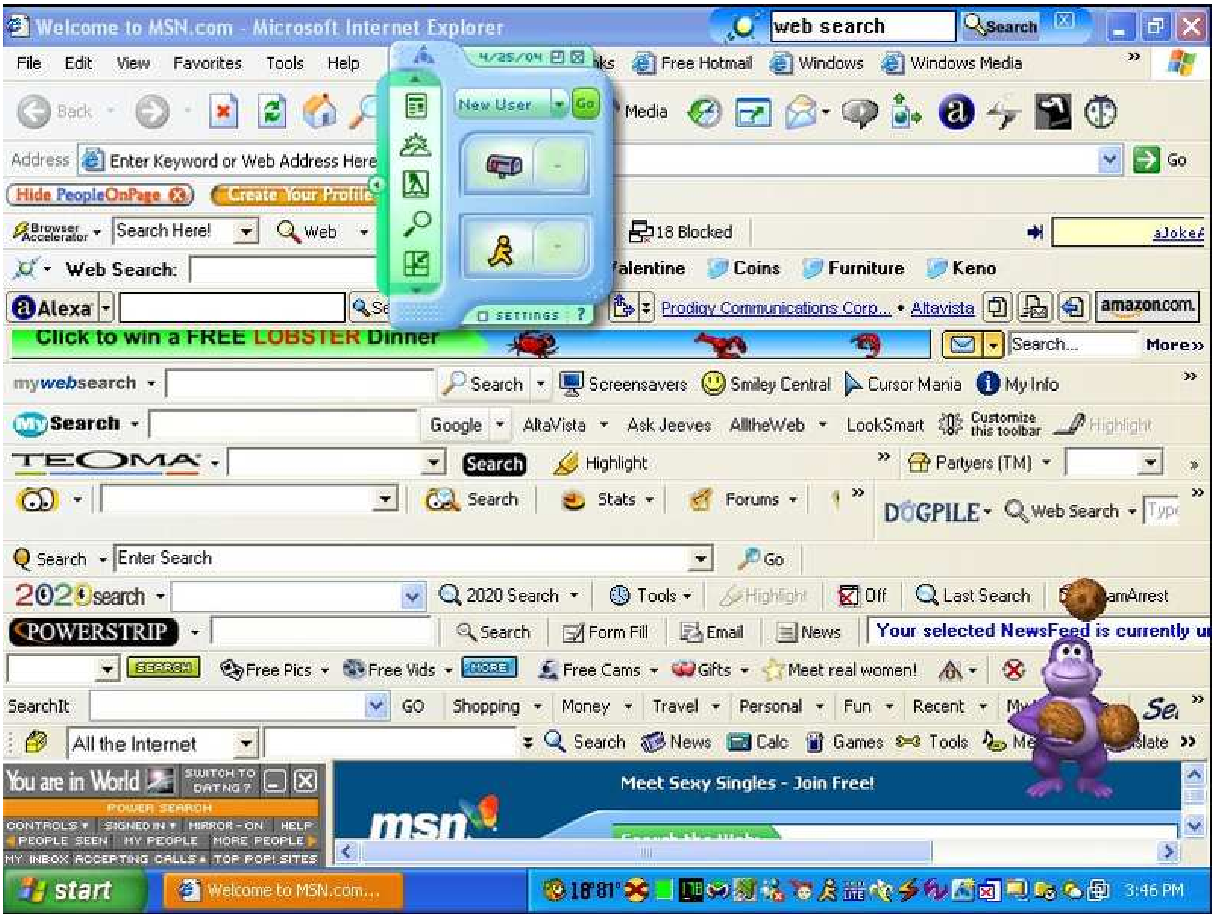
Rootkit

A rootkit is a program (or combination of several programs) designed to take fundamental control (in Unix terms "root" access, in Windows terms "Administrator" access) of a computer system, without authorization by the system's owners and legitimate managers. Access to the hardware (ie, the reset switch) is rarely required as a rootkit is intended to seize control of the operating system running on the hardware. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms. Often, they are also Trojans as well, thus fooling users into believing they are safe to run on their systems. Techniques used to accomplish this can include concealing running processes from monitoring programs, or hiding files or system data from the operating system.

Spyware

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habit, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term privacy-invasive software.



Trojan horse

In the context of computing and software, a Trojan horse, or simply trojan, is a piece of software which appears to perform a certain action but in fact performs another such as a computer virus. Contrary to popular belief, this action, usually encoded in a hidden payload, may or may not be actually malicious, but Trojan horses are notorious today for their use in the installation of backdoor programs. Simply put, a Trojan horse is not a computer virus. Unlike such malware, it does not propagate by self-replication but relies heavily on the exploitation of an end-user (social engineering). It is instead a categorical attribute which can encompass many different forms of codes. Therefore, a computer worm or virus may be a Trojan horse. The term is derived from the classical story of the Trojan Horse.

Tools improving security

Antivirus

Antivirus software are computer programs that attempt to identify, neutralize or eliminate malicious software. Antivirus is so named because the earliest examples were designed exclusively to combat computer viruses; however most modern antivirus software is now designed to combat a wide range of threats, including worms, phishing attacks, rootkits, trojan horses and other malware. Antivirus software typically uses two different techniques to accomplish this:

- Examining (scanning) files to look for known viruses matching definitions in a virus dictionary
- Identifying suspicious behavior from any computer program which might indicate infection. This technique is called heuristic analysis. Such analysis may include data captures, port monitoring and other methods.

Most commercial antivirus software uses both of these approaches, with an emphasis on the virus dictionary approach.
Examples: avast!, AVG, F-Secure, Kaspersky Anti-Virus, McAfee VirusScan, NOD32, Norton AntiVirus, Sophos Anti-Virus, Windows Defender, ZoneAlarm (http://en.wikipedia.org/wiki/List_of_antivirus_software)

Antispyware

Antispyware programs effectively detect and remove spyware, adware threats and other kinds of computer parasites from the system.
Examples: Ad-Aware, HijackThis, RootkitRevealer, Spybot - Search & Destroy, Windows Defender (http://www.2-spyware.com/anti-spyware, http://en.wikipedia.org/wiki/Category:Spyware_removal)
Corrupt antispyware programs are corrupt, rogue, fake, illegal, even harmful anti-spyware tools that cannot correctly detect and remove spyware or other parasites and therefore are totally ineffective and should NOT be used (http://www.2-spyware.com/corrupt-anti-spyware).

Wininternals

(http://technet.microsoft.com/cs-cz/sysinternals/default(en-us).aspx)

Autoruns

See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

Process Explorer
Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process Monitor
Monitor file system, Registry, process, thread and DLL activity in real-time.

Sigcheck
Dump file version information and verify that images on your system are digitally signed.

DiskMon, FileMon, RegMon

Testing

European Institute for Computer Antivirus Research
European expert group for IT-Security.
http://www.eicar.org/

The Spycar Project
Spycar is a suite of tools designed to mimic spyware-like behavior, but in a benign form. Intelguardians created Spycar so anyone could test the behavior-based defenses of an anti-spyware tool. Spycar runs only on Windows, the same platform most targeted by spyware developers.
http://www.spycar.org/

Materials:

- http://en.wikipedia.org/wiki/Adware
- http://en.wikipedia.org/wiki/Anti-virus_software
- http://en.wikipedia.org/wiki/Computer_virus
- http://en.wikipedia.org/wiki/Computer_worm
- http://en.wikipedia.org/wiki/Malware
- http://en.wikipedia.org/wiki/Rootkits
- http://en.wikipedia.org/wiki/Spyware
- http://en.wikipedia.org/wiki/Trojan_horse_(computing)
- http://www.2-spyware.com/software.php
- http://technet.microsoft.com/cs-cz/sysinternals/default(en-us).aspx
- http://www.viry.cz