Malware – Computer Viruses – Spyware - Hoaxes

Malware, short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent. 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. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses.

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, crimeware and other malicious and unwanted software.

A **computer virus** is a computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance, because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading 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, which are technically different. A worm can exploit security vulnerabilities to spread itself to other computers without needing to be transferred as part of a host, and a Trojan horse is a program that appears harmless but has a hidden agenda. Worms and Trojans, like viruses, may cause harm to either a computer system's hosted data, functional performance, or networking throughput, when they are executed. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious or go unnoticed.

File Infectors. Some file infector viruses attach themselves to program files, usually selected .COM or .EXE files. Some can infect any program for which execution is requested, including .SYS, .OVL, .PRG, and .MNU files. When the program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly-contained programs or scripts sent as an attachment to an e-mail note.

System Or Boot-Record Infectors. These viruses infect executable code found in certain system areas on a disk. They attach to the DOS boot sector on diskettes or the Master Boot Record on hard disks. A typical scenario (familiar to the author) is to receive a diskette from an innocent source that contains a boot disk virus. When your operating system is running, files on the diskette can be read without triggering the boot disk virus. However, if you leave the diskette in the drive, and then turn the computer off or reload the operating system, the computer will look first in your A drive, find the diskette with its boot disk virus, load it, and make it temporarily impossible to use your hard disk. (Allow several days for recovery.) This is why you should make sure you have a bootable floppy.

Macro Viruses. These are among the most common viruses, and they tend to do the least damage. Macro viruses infect your Microsoft Office applications and typically insert unwanted words or phrases.

Special virus types:
A **computer worm** is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to the poor security the computers infected have. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Trojan horses are designed to allow a hacker remote access to a target computer system. Once a Trojan horse has been installed on a target computer system, it is possible for a hacker to access it remotely and perform various operations. The operations that a hacker can perform are limited by user privileges on the target computer system and the design of the Trojan horse.

A successfully-installed **rootkit** allows unauthorized users to maintain access as system administrators, and thus to take and keep full control of the "rootkitted" or "rooted" system. Most rootkits typically hide files, processes, network connections, blocks of memory, or Windows Registry entries from other programs used by system administrators to detect specially privileged accesses to computer system resources. However, a rootkit may masquerade as or be intertwined with other files, programs, or libraries with other purposes. While the utilities bundled with a rootkit may be maliciously intended, not every rootkit is malicious. Rootkits may be used for both productive and destructive purposes.

Virus Hoax. A virus hoax is a false warning about a computer virus. Typically, the warning arrives in an e-mail note or is distributed through a note in a company's internal network. These notes are usually forwarded using distribution lists and they will typically suggest that the recipient forward the note to other distribution lists.

If you get a message about a new virus, you can check it out by going to one of the leading Web sites that keep up with viruses and virus hoaxes. If someone sends you a note about a virus that you learn is a virus hoax, reply to the sender that the virus warning is a hoax.

Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

Data collecting programs that are installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared. However, spyware is often installed without the user's consent, as a drive-by download, or as the result of clicking some option in a deceptive pop-up window. adware, software designed to serve advertising, can usually be thought of as spyware as well because it almost invariably includes components for tracking and reporting user information.

The **cookie** is a well-known mechanism for storing information about an Internet user on their own computer. However, the existence of cookies and their use is generally not concealed from users, who can also disallow access to cookie information. Nevertheless, to the extent that a Web site stores information about you in a cookie that you don't know about, the cookie mechanism could be considered a form of spyware.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Grayware (or greyware) is a general term sometimes used as a classification for applications that behave in a manner that is annoying or undesirable, and yet less serious or troublesome than malware. Grayware encompasses spyware, adware, dialers, joke programs, remote access tools, PUP and any other unwelcome files and programs apart from viruses that are designed to harm the performance of computers on your network.

A **PUP** (potentially unwanted program) is a program that may be unwanted, despite the possibility that users consented to download it.