Malware Glossary

Sheila M.Blackford, PLF Practice Management Advisor

Back door: A means to gain access to a computer program that bypasses security mechanisms. Cyber criminals often use back doors that they have detected or that they have installed in order to exploit the computer. If a security system is in place, a back door allows entry without detection.

Hacking: Gaining unlawful access to a computer and then viewing, copying, creating, or changing data on the computer.

Key Logger: A type of malware that identifies the input from the computer keyboard and then sends this information to the cyber criminals, who decipher passwords and other types of information. Some secure websites are now providing options to use a mouse click to make entries via a virtual keyboard.

Link Manipulation: The technique in which a phisher (fraudulent impersonator) routes a link to a website. By clicking on the deceptive link, it opens up at the phisher website instead of the website mentioned in the link. Catch this by moving your mouse over a link to view the actual URL address.

Malware: Software that is intended to damage or disable computers or computer systems is called malware because of its malevolent purpose.

Phishing: Impersonations of legitimate emails or instant messaging (IM) by fraudsters to gain financial or account information or login credentials that can be further exploited.

Ransomware: A type of malware designed to block access to your computer files or computer by the use of encryption and charging a ransom to release the encryption key so you can unlock your data.

Spyware: A category of malware installed onto a computer that gathers information about the computer user's Internet browsing habits and personal data and then transmits this information covertly to the remote location of the spyware user.

Trojan or Trojan horse: A type of malware that looks innocuous but is designed to breach the security of a computer system. Upon activation, it performs a malicious action such as destroying data files. Ransomware is usually delivered via a Trojan. Unlike a virus or worm, Trojans cannot reproduce by infecting other files or by self-replicating.

Virus: A type of computer code capable of copying itself to detrimental effect, usually the corruption of your hard drive and destruction of your data. The computer virus usually is attached to an executable file (.exe file extension) and will only infect your computer if you run or open the malicious program.

Worm: A self-replicating virus that does not alter your computer files but resides in your active memory duplicating itself. Worms spread by computer to computer, taking advantage of file or information transport features on your computer so that it travels without human aid. Because it can self-replicate, the danger is that your computer could send out hundreds or thousands of copies of itself to everyone listed in your address book.

Zero Day Exploit: A piece of software or sequence of commands that takes advantage of a vulnerability in software or hardware before notice of the vulnerability can be released to the public or before a corrective patch be issued.