National Cyber Security Awareness Month
(October 2008) Newsletter Series (1 of 4)

Understanding Malware

Viruses: A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels.

Worms: In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them.

Trojans: A Trojan is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems.

Wabbits: Malware that is content simply to focus on utterly devastating the infected machine instead of spreading.

Backdoors: Backdoors open a "backdoor" onto a computer, providing a network connection for hackers or other malware to enter or for viruses or spam to be sent out through.

Rootkit: A rootkit is designed to camouflage itself in a system's core processes so as to go undetected. It is the hardest of all malware to detect and therefore to remove. Many experts recommend completely wiping your hard drive and reinstalling everything fresh.

Keylogger: Keyloggers log your keystrokes, i.e., what you type. Typically keyloggers are out to log sensitive information such as passwords and financial details. Many also take screen shots or capture video from web cams.

Dialers: Dialers dial telephone numbers via your computer's modem. Dialers either dial expensive premium-rate telephone numbers or they dial a hacker's machine to transmit stolen data.

"Zero Day": The name "zero day" designates malware that security vendors have not had time to create protection against and is therefore even more effective for a period of time till vendors can catch up.

Spyware: Spyware is software that spies on you and tracks your internet activities.

Adware: Adware is a type of spyware that secretly imbeds itself on your computer and analyzes your web browsing habits presenting related banner advertising as popup

windows. While most of the advertisements you see are for legitimate companies, the actual producers of the spyware are not. Because a user's personal details are often passed on to third parties, adware has been criticized by privacy advocates.

Drive-By Downloads (DBD): In general, the term "drive-by download" (DBD) refers to any malware installed without user consent or knowledge. The reason "drive-by downloads" are so dangerous is that it requires no action by a web surfer to get infected. A hyperlink does not even have to be clicked for the install to occur, as some DBDs exploit browser flaws. Proper patching is the best defense against DBDs.

Piggyback: Piggyback malware refers to embedded malicious code within an otherwise harmless executable file. Typically piggyback sites are those having downloads for games, music, and wallpapers, as well as adult and celebrity web sites. One of the aspects of piggybacking that makes it so dangerous is that the person sending the malware often does not know it themselves.

Hoax: Hoaxes are "joke emails" warning of alleged viruses. Contact the University Technology (uTech) helpdesk (309-298-2704 or supportcenter@wiu.edu) or your college technology representative to report suspicious email.

Ransomware: Users of ransomware hold computers hostage unless an infected machine's owner makes a payoff.

Crimeware: Malware evolves to focus on obtaining financial returns.

Now that we have a better understanding of the types of malware that are out to do us harm, my hope is that we will think twice before we click! Next week's newsletter will focus on the issue of social engineering.

Regards,

Michael Rodriguez CTSO @ Western Illinois University
MA-Rodriguez@wiu.edu