Know Your Enemy: a Look Inside Viruses, Trojans, and Worms

Believe it or not, destructive software applications aren't always viruses, and not all viruses are destructive. So how can you tell the difference?

The computing industry uses the term malware to describe the gamut of malevolent software that makes its way around the world from computer system to computer system. Malware includes viruses, Trojans, computer bombs, worms, and many other forms of software created specifically to wreak havoc on computers and networks, but also describes software applications that are annoying but usually not destructive. When you can accurately identify the different types of malicious software in circulation, you have taken a key step in developing strategies to contain that software and keep your valuable networks safe from it.

Viruses

By definition, a virus is a self-replicating computer program that can infect other computer programs. This doesn't automatically mean that a virus will cause damage, and in fact many don't. In effect, for a virus to replicate itself and spread to other computers, it must stay undetected. The more widespread its destruction, the more attention it draws to itself, and the faster patches and other fixes become available to stop it. A typical virus has three key components:

- A method of infection that allows the virus to replicate. The virus may infect the boot sector, insert itself into Microsoft Office documents, modify an existing program or just a few lines of code, or even attach itself to network resources.
- A trigger that launches the virus payload (if it has one). The trigger may be one of many things: a specific date or time, a sequence of events or keystrokes, a user action (closing a file), or even some repetition or combination of events. With each day the trigger is delayed, the more opportunity the virus has to propagate if it has an efficient infection mechanism. However, if the trigger delay is too long, the virus may be detected by an antivirus scan.
- A payload or warhead that causes the actual damage. A virus' payload can be as harmless as a simple screen message or as destructive as a package that scrambles data, deletes files, creates backdoors into systems, or causes system crashes.

Warning: Not every virus has a trigger and payload. The first time you become aware you have a virus may be when your antivirus software detects it.

Trojans

Just like the original wooden horse in ancient Greece that they are named after, computer Trojans claim to be one thing (often harmless), but in reality carry an unfriendly and possibly destructive payload. By definition, a Trojan is a program that acts as a delivery vehicle for other forms of malware and may rely on social engineering to convince a user to actually launch the program. Even though mainstream news media coverage is rife with warnings to computer users not to click on e-mail attachments (especially executables), Trojans remain an effective tool for spreading malware.

Trojans have two components: a client and a server. When a user unknowingly runs the server on his computer, the attacker then uses the client to connect to the server and start using the Trojan. The server works hard to stay hidden on the user's computer while it listens on ports for incoming connections from the attacker, modifies the Registry, or uses some other auto-starting method.

Worms

Worms are computer programs that replicate themselves across network connections without modifying or attaching themselves to a host program. In recent news, we've seen worms such as the MS Blaster worm, Slammer, and SoBig and its variants.

SoBig is a worm/virus spreading via the Internet as an attachment to infected e-mails. It also downloads and sets up a backdoor program. The SoBig.f worm activates only when a user double-clicks on the attached file. Once the worm is launched, it installs itself in the system and runs its spreading routine and payload. The latest variant, W32.Sobig.F@mm, is a mass-mailing, network-aware worm that sends itself to all the e-mail addresses it finds in the files that have the following extensions: *.dbx *.eml *.hlp .htm *.html *.mht *.wab *.txt.

The worm uses its own SMTP engine to propagate. It also attempts to create a copy of itself on accessible network shares, but fails due to bugs in the code. As the worm searches through each file to send an e-mail, it may use a part of the e-mail, such as the From field, to create a spoofed address (which means that the sender in the From field is most likely not the real sender). That's what makes many worms look harmless but yet so effective: their From address is familiar and trusted.

Oh My!
Within the study of virus protection, there's always the temptation to relate some kind of artificial intelligence to this malicious code, but be warned: There are people behind the development of exploit code for Microsoft, Unix, and Linux systems. The more you know, the better able you will be to protect your network from them.

For more information

- Learn more about the HP/McAfee Security Management Solution designed to help your business combat a variety of security threats.
- The CERT Coordination Center, operated by Carnegie Mellon University, offers Internet security expertise. For regular updates on security patches, subscribe to the CERT mailing list.
- Browse the virus resources from Computerworld.
- Take free online classes on virus protection, firewall basics, networking, and other topics at the HP Learning Center.