Trojan Horse or Virus?

by Joseph Lo aka Jolo
Part of the Trojan horse attacks help page
updated May 6, 2000

In May 2000, the "Love Bug" spread like wild fire and affected countless computers around the world. The media described it with many technical buzzwords. A CNN story called it a "hybrid virus and worm", others have tossed around buzzwords like Trojan horse, hacking, and cracking. Which is it?

If you're just a regular computer user, you don't really need to know these differences, but we wanted to try to make this confusing subject as clear as possible.

Definitions

Virus

A virus is a program that propagates itself by infecting other programs on the same computer. Viruses can do serious damage, such as erasing your files or your whole disk, or they may just do silly/annoying things like pop up a window that says "Ha ha you are infected!" True viruses cannot spread to a new computer without human assistance, such as if you trade files with a friend and give him an infected file (such as on a floppy or by an email attachment).

Worm

Like a virus, a worm is also a program that propagates itself. Unlike a virus, however, a worm can spread itself automatically over the network from one computer to the next. Worms are not clever or evil, they just take advantage of automatic file sending and receiving features found on many computers.

Trojan horse

This is a very general term, referring to programs that appear desirable, but actually contain something harmful. The harmful contents could be something simple, for example you may download what looks like a free game, but when you run it, it erases every file in that directory. The trojan's contents could also be a virus or worm, which then spread the damage. See our Trojan horse help page for more information.

Cracker

Crackers are often mistakenly called "hackers". Crackers are the "bad guys" who seek to "crack" or gain unauthorized access to computers, typically to do malicious things e.g. to steal credit card information or crash the computer. Crackers might do this by writing a virus, worm, or Trojan horse. Alternatively, they may just exploit weaknesses in the computer's operating system in order

to gain entry. Many crackers will install a "backdoor" which allows the cracker to "remote control" your computer over the internet, such as to distribute child porn or perform a [denial of service attack](#) against somebody else. Most crackers are just bored, anti-social kids who aren't particularly smart and just take advantage of well-known, existing exploits or the gullibility of the typical internet user.

Hacker

When used properly, this term refers to an elite breed of "good guys" who are talented computer programmers. They enjoy solving challenging problems or exploring the capabilities of computers. Like a carpenter wielding an axe to make furniture, the hacker does good things with his skills. True hackers subscribe to a code of ethics and look down upon the illegal and immoral activity of crackers (defined above). When the press uses "hackers" to describe virus authors or computer criminals who commit theft or vandalism, it is not only incorrect but also insulting to true hackers.

Land of Confusion

OK so you think you've got those terms all straight in your head? Prepare to be confused. :-)

Remember the "Love Bug"? Is it a **virus**, **worm**, or **trojan**? Answer: all three! It's a trojan because it pretends to be a love letter when it is really a harmful program. It's a virus because it infects all the image files on your disk, turning them into new trojans. Finally, it's also a worm because it propagates itself over the internet by hiding in trojans that it sends out using your email address book, IRC client, etc.

Here's another one. Traditionally you use **anti-virus programs** to check your computer for viruses and prevent their spread. The problem is, traditional viruses don't really exist any more. Nowadays, lame **crackers** are busy making trojans and worms, so that's what anti-virus programs try to tackle now. The problem is, with everybody online these days, trojans and worms are fast to spread and easy to modify, so anti-virus programs are useless in trying to prevent them. If you're lucky, then can remove the infection after the fact, assuming your disk isn't so messed up there is nothing left to disinfect.

Oh that's not all. **Firewalls** are network barriers designed to keep out crackers. With the recent proliferation of **trojans** which install a backdoor program, however, a whole new market has sprung up in "personal firewalls" which are programs that run on your PC and can block communications from some backdoor programs. Since file downloads are a normal part of your internet experience, however, personal firewalls can't stop you from downloading the **trojan** that installs that backdoor in the first place.

| Go Back | Search | Help! | Send Email |

[go back | search | help | send email]

all pages © IRCHELP.ORG or original authors