Title:
Computer Viruses, Worms And Trojans Explained

Word Count:
638

Summary:
Fighting viruses and getting rid of them is big business right now. The first
step is knowing just what the enemy is.

THE ENEMY - Hackers and Crackers

Computer geeks say that there is a difference between hackers and crackers.
Crackers do damage to systems they break into while hackers just want to see how
everything works. We'll use the more common term of hacker. Originally the term
hacker was someone who made furniture with the use of an axe.

A virus is "malware" ...

Keywords:
virus, trojan horse, worm, internet security, pc security, antivirus

Article Body:
Fighting viruses and getting rid of them is big business right now. The first
step is knowing just what the enemy is.

THE ENEMY - Hackers and Crackers

Computer geeks say that there is a difference between hackers and crackers.
Crackers do damage to systems they break into while hackers just want to see how
everything works. We'll use the more common term of hacker. Originally the term
hacker was someone who made furniture with the use of an axe.

A virus is "malware" for your computer. This is a term that covers all kinds of
software that is malicious. The most common types of malware are Trojans, worms,
and viruses.

VIRUSES

Viruses are often hidden inside of other programs, for example installation
programs that arrive to you through email attachments. When you run this host

program the virus is executed. When the virus is in your computer memory it will be able to do a lot of damage such as infecting other computer programs.

Once the infection phase of the virus is complete the next stage begins: the destructive phase. Viruses will wait for a certain trigger, such as a date or the number of times that the virus has been copied, before the payload is delivered. The payload can be as simple as messages all the way to the deletion of files to the destruction of your operating system.

When viruses were first created they were often distributed on a floppy disk. As the Internet has grown, email and file downloads are the best way for viruses to be passed. Email can have attachments that can contain any type of computer file. Executable files can be loaded with viruses and therefore you shouldn't run them unless you're sure that they are virus free.

WORMS

Worms are much like viruses because they are self-copying. They can reproduce across multiple networks without human aid, such as through the sending of emails. Worms, however, don't need an executable program in order to be passed along.

A worm can affect a computer network more than it can infect computers that are on that network. Because they self-copy they can overload the resources on a network. This can cause slow downs in the speed of data transfers by using a large amount of bandwidth...more bandwidth than is needed for normal network traffic. Any network that routes traffic on the Internet is simply known as software and hardware that is specialized. Both software and hardware can be bothered by malware.

A worm can be created to carry payloads by using an installation program through the backdoor. A backdoor is an access point into the computer that is hidden. The worm uses the backdoor and ignores the usual procedure for login. Backdoors are often used by spammers so that they can send junk email.

TROJAN HORSES

A Trojan horse is another kind of malware. A Trojan horse is a computer program that acts as though it will do one thing when it will actually do something different. This term comes from the story of Troy, a city which was deceived by the Greeks to get into the inner city undetected. A Trojan horse can't replicate itself the way viruses and worms can.

A Trojan horse can be hidden in software that is otherwise useful. When a Trojan

horse starts it can do such things as corrupt files, install backdoors, erase data, and keep track of keystrokes. This information will enable hackers to steal your personal information such as passwords and credit card numbers.

COMBATING MALWARE

In this series we will talk about what you can do to fight malware. Until then it's important to just be passive and not expect that your computer problems will be taken care of by someone else. Combating viruses needs the involvement of users, webmasters, and software vendors.