

Computer Viruses

Viruses - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs too, and it has the chance to reproduce by attaching to other programs.

Email Viruses - An email virus travels as an attachment to email messages, and it multiplies by emailing himself to people in the victim's address book. Some email viruses don't even need you to click on them, they run when you open the message that is infected.

Trojan Horses - A Trojan Horse is a computer program that claims to do one thing but instead does damage when you run it (it may erase your hard drive or install other viruses). Trojan horses have no way to multiply automatically.

Worms - A worm is a small piece of software that uses computer networks and security holes to multiply. A copy of the worm scans the network for another machine with a security hole. It copies itself to the new machine using the security hole and keeps multiplying from there, as well.

Virus Origins

Computer viruses are called viruses because they have similarities to biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person.

Unlike a cell, a virus has no way to multiply itself. Instead, a biological virus must inject its DNA into a cell. The virus's DNA then uses the cell's existing machinery to reproduce itself.

A computer virus shares some of these characteristics. A computer virus needs to attach itself to another program to be able to run and reproduce.

People write computer viruses. A person has to write the code, test it to make sure it spreads properly and then release it.

Why do they do it? - There are at least three reasons. The first is the same psychology that drives vandals and arsonists. For some people, that seems to be a thrill. If that kind of person knows computer programming, then he or she could create destructive viruses. The second has to do with the thrill of watching things blow up. Some people have a fascination with things like explosions and car wrecks. Creating a virus is a little like that -- it creates a bomb inside a computer. The third reason involves bragging rights. Some people just like to know that they were able to get a way with it. Or that they were able to do something that was supposed to be really hard to do.

A lot of virus creators, don't realize that they cause real damage with their actions. Computer viruses can cost millions of dollars to clean even if they didn't destroy anything. For this reason, the legal system is getting much tougher in punishing people who create viruses.

Virus History

Traditional computer viruses started showing up in the late 80s, and they started because of several factors. The first factor was the spread of personal computers. Before the 1980s, home computers were nearly non-existent or they were toys. Real computers were rare, and they were locked away for use by experts. During the 1980s, real computers started to spread to businesses and homes.

The second factor was the use of computer bulletin boards. People could dial up a bulletin board with a modem and download programs. Games and simple programs were extremely popular. Bulletin boards led to the precursor of the Trojan Horse. You would think you were getting a game, but when you ran it, it would wipe out your system.

The third factor that led to viruses was the floppy disk. People started moving information and programs from one computer to another. Virus authors took advantage of this and created the first self-replicating program.

The spreading part is the infectious phase of the virus, but most viruses also have a destructive attack phase. After a computer has been infected, some sort of trigger

activates the attack phase and virus does something; anything from showing a silly message on the screen to erasing all your information. The trigger could be a specific date, the number of times the virus has multiplied, etc.

Virus Evolution

At first, viruses were really small programs attached to real programs. When the victim ran the program, the virus would run instead, reproduce and then start the real program. The victim would not know he had just run the virus until the attack phase.

As virus creators became more sophisticated, they learned how to load a virus into memory so that it could continue running in the background as long as the computer was on. This gave viruses a much more effective way to replicate. They also learned how to infect the boot sector of floppy disks and hard drives. The boot sector is a small program that tells the computer how to translate all the information on the disc. By putting a virus in the boot sector, the virus is guaranteed to be executed.

In general, neither kind of virus is very threatening any longer. Nearly every program you buy today comes on a compact disc. CDs can not be modified and that makes infection of a CD unlikely. Also, modern operating systems protect the boot sector, making this kind of virus almost extinct.

Virus authors adapted to the changing environment by creating the email virus. For example the Melissa Virus in 1999 spread in a Microsoft Word document sent in an email, and it worked like this:

Someone created a virus as a Word document and uploaded it to an Internet newsgroup. Anyone who downloaded the document and opened it would trigger the virus. The virus would then send the document (and therefore itself) in an email message to the first 50 people in the person's address book. The email message contained a friendly note with the person's name, so the recipient would open the document thinking it was harmless. The virus would create 50 new messages from the recipient's machine.

Worms

A worm is a computer program that has the ability to copy himself from machine to machine. Worms use up computer time and network bandwidth when they replicate, and they often carry payloads that do considerable damage. A worm usually exploits some sort of security hole in a program or the operating system. Worms move around and infect other machines through computer networks. Using a network, a worm can multiply incredibly fast.

A worm called Code Red made headlines in 2001. It replicated itself 250,000 times in nine hours. Experts predicted that this worm could clog the internet so effectively that things would completely grind to a halt.

How to Protect Your Computer

- Have a good anti-virus.
- Avoid programs from unknown sources.
- Do not disable Macro Virus Protection on Microsoft applications and never run macros in documents if you don't know what they do. In most cases, macros are unnecessary, so avoiding all macros is a good policy.
- Never double-click an attachment that contains an executable. Files with extensions like .exe, .com or .vbs are executables, and once you run them, you have given it permission to do all sorts of things to your computer.
- If you are truly worried about traditional viruses, you should be running a more secure operating system like UNIX.

Other Threats

Viruses are not the only threats to your computer. Malware is another name for software that has an evil intent. Other common types of malware are:

- **Adware** puts ads up on your screen. While it is not destructive by design, it can slow down a computer by using large amounts of memory.

- **Spyware** collects personal information like browsing habits, passwords, etc. Spyware isn't designed to damage your computer.
- **Hijackers** turn your machine into a zombie computer. A hacker infiltrates the victim's machine and uses it to conduct illegal activities. The victim remains unaware since he can still use his computer.
- **Dialers** force your computer to make phone calls. For example, one might dial 900-numbers and run up your phone bill while making money for the owner of the 900-number.
- **Phishing** is a method of online identity theft. A phisher sends a phony message that appears to be from a reputable source, like your bank. This message links to a fake website that asks for your user name and password. When you enter your information, the phisher records it and is then able to use it to take money from your accounts, or make purchases with your credit cards.