

Use the table below to compare and contrast a computer virus to a biological virus.

	Computer Virus	Biological Virus
Host	1.	
Alive?	2.	
Mode of survival	3.	

2. How did the early computer viruses work? Use this word bank to answer the question.

game trigger executed virus memory infect date program  
computer replicated downloads destructive data code spreads

Early viruses were pieces of **4.** \_\_\_\_\_ attached to a common program, like a **5.** \_\_\_\_\_. When a person **6.** \_\_\_\_\_ and then plays the game, the **7.** \_\_\_\_\_ loads itself into **8.** \_\_\_\_\_. It looks for another **9.** \_\_\_\_\_ to **10.** \_\_\_\_\_. When the newly infected program is **11.** \_\_\_\_\_, the same process occurs and the virus **12.** \_\_\_\_\_. Most viruses have some sort of **13.** \_\_\_\_\_ attack phase that is activated by a **14.** \_\_\_\_\_ that causes some kind of damage to the host **15.** \_\_\_\_\_. It can even erase all of your **16.** \_\_\_\_\_. The trigger may be a certain **17.** \_\_\_\_\_, the number of times the virus has been **18.** \_\_\_\_\_ or something similar.

# Spreading a Digital Disease

adapted from an article from *How Stuff Works*

## Introduction to Computer Viruses

In the movie "Independence Day," it takes everyone a while to figure out how to fight back against the aliens. Not only do the aliens outnumber the earthlings, they're also equipped with far superior technology. So, it's pretty amazing when the "good guys" finally figure out how to take out the "bad guys." And, the plan seems remarkably simple: Give the aliens a virus -- a computer virus -- that will cripple their technology! That exact scenario is actually pretty far-fetched. However, the concept itself is not.



Computer viruses are actually a very real and very serious threat to our own technology. A properly engineered virus can have a staggering effect. For example, experts estimate that the **Mydoom** worm infected approximately a quarter-million computers in a single day in January 2004.

Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer. A biological virus passes from person to person. A biological virus is not a living thing. It is a fragment of DNA inside a protective jacket. Unlike a cell, a virus has no way to do anything or to reproduce by itself -- it is not alive. Instead, a biological virus must inject its DNA into a cell. The viral DNA then uses the cell's existing machinery to reproduce itself. A computer virus must piggyback on top of some other program or document in order to be executed. Once it is running, it is then able to infect other programs or documents. Obviously, the analogy between computer and biological viruses stretches things a bit, but

there are enough similarities that the name sticks. Early viruses were pieces of code attached to a common program like a popular game. A person might download an infected game and run it. A virus like this is a small piece of code embedded in a larger, legitimate program. This type of virus is designed to run when the legitimate program is executed. So in this case, that would be the first time the game is played. The virus loads itself into memory and looks around to see if it can find any other programs to infect. If the virus can find one, the virus infects the program by adding its own code to the unsuspecting program. Then the virus launches the "real program." The user really has no way to know that the virus ever ran. Unfortunately, the virus has now reproduced itself, so two programs are infected. The next time either of those programs executes, they infect other programs, and the cycle continues. Now, let's say one of the infected programs is shared with another person's computer. This is how other programs get infected. This is how the virus spreads.

Besides spreading, most viruses also have some sort of destructive attack phase where they do some form of damage. Some sort of trigger will activate the attack phase, and the virus will then "do something" -- anything from printing a silly message on the screen to erasing all of your data. The trigger might be a specific date, or the number of times the virus has been replicated, or something similar.

### Worms

A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.



## E-mail Viruses

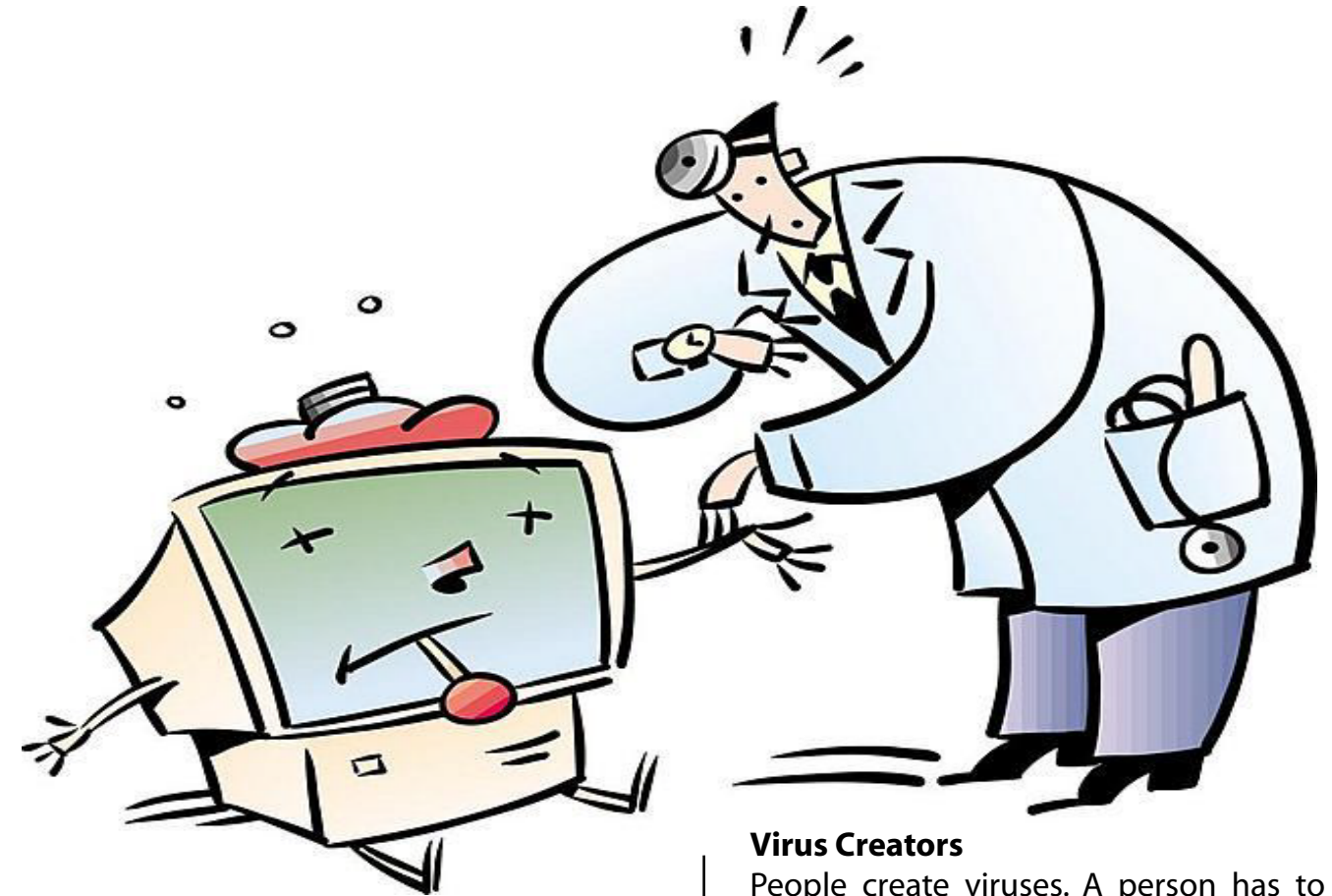
Probably the most recognized type of computer virus is the e-mail virus. An e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. The **Melissa virus** in March 1999 was particularly effective. Melissa spread in Microsoft Word documents sent via e-mail, and it worked like this:

Someone created the virus as a Word document uploaded 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 e-mail message to the first 50 people in the person's address book. The e-mail message contained a friendly note that included the person's name, so the recipient would open the document thinking it was harmless. The virus would then create 50 new messages from the recipient's machine. As a result, the Melissa virus was the fastest-spreading virus ever seen! It was amazing that such a simple virus could be so powerful that it forced Microsoft and a number of other very large companies to turn off their e-mail systems entirely until the virus could be contained.

The **ILOVEYOU virus**, which appeared on May 4, 2000, was even simpler. It contained a piece of code as an attachment. People who double-clicked on the attachment allowed the code to execute. The code sent copies of itself to everyone in the victim's address book and then started corrupting files on the victim's machine. This is as simple as a virus can get.

The Melissa virus took advantage of the programming language built into Microsoft Word called VBA, or **Visual Basic** for Applications. It is a complete programming language and it can be programmed to do things like modify files and send e-mail messages. It also has a useful but dangerous auto-execute feature. A programmer can insert a program into a document that runs instantly whenever the document is opened. This is how the Melissa virus was programmed. Anyone who opened a document infected with Melissa would immediately activate the virus. It would send the 50 e-mails, and then infect a central file so that any file saved later would also contain the virus! It created a huge mess.

In the case of the ILOVEYOU virus, the whole thing was human-powered. If a person double-clicked on the program that came as an attachment, then the program ran and did its thing. What fueled this virus was the human willingness to double-click on the executable.



### Virus Creators

People create viruses. A person has to write the code, test it to make sure it spreads properly and then release the virus. A person also designs the virus's attack phase, whether it's a silly message or destruction of a hard disk. Of course, most virus creators seem to miss the point that they cause real damage to real people with their creations. Destroying everything on a person's hard disk is real damage. Forcing the people inside a large company to waste thousands of hours cleaning up after a virus is real damage. Even a silly message is real damage because a person then has to waste time getting rid of it. For this reason, the legal system is getting much harsher in punishing the people who create viruses.

### A Trojan Horses

A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

### Protect Yourself

Protection against viruses is possible with a few simple steps. To protect a computer from traditional (as opposed to e-mail) viruses, running a secure operating system like UNIX will help. You never hear about viruses on these operating systems because the security features keep viruses (and unwanted human visitors) away from the computer's hard disk. Run virus protection software. Avoid programs from unknown sources (like the Internet). Instead, stick with commercial software purchased on CDs -- it eliminates almost all of the risk from traditional viruses. And, never double-click on an attachment that contains an executable that arrives as an e-mail attachment. A file with an extension like EXE, COM or VBS is an executable. An executable can do any sort of damage it wants. Once you run it, you have given it permission to do anything on your machine. The only defense is never to run executables that arrive via e-mail.