An Online metaphor - Understanding Biological Viruses

Malignant computer applications are commonly known as "malware", since they frequently piggyback off of other programs, files, or even E-mails to enter the infected computer. A typical malware application has a single goal: to wreak havoc and make the user's system work slower or with security vulnerabilities. Since a malware program may have several goals, it is important that an infected program work in a specific way to do its job. This article discusses the most common malware applications and how they work.

The most common types of malware infecting computers today are known as "self-replicating programs." Self-replicating computer programs are used for several reasons: to steal personal information, to send spam, and to distribute fake security alerts. Some self-replicating viruses are also used to hack into networks and steal data. The best way to protect against these harmful programs is to install anti-virus and anti-spyware programs that have been specifically designed to detect and remove these types of malware. These programs work by detecting the virus, which will then be sent to the user's control panel where the infected files can be manually removed.

Computer viruses are made up of multiple components that combine to perform their tasks. Two of the most essential components of a biological virus include a protein molecule (or DNA) and a promoter (or promoter region). The DNA is the actual coding part of the biological virus, while the promoter is the method by which the genetic information of the virus is read by the immune system. Common biological virus components are generally composed of DNA, small amounts of lipids and amino acids, viral RNAs, and possibly a protein shell. The HIV virus, for example, contains nothing other than DNA and a short protein called a capsid.

While it may seem like an obvious analogy, biological viruses are really more similar to different kinds of malware than they are to typical viruses. For example, there are several kinds of viruses that are important to antivirus programmers, such as computer viruses, worm viruses, and Trojan horses. However, the analogy stops at that point. Viruses can copy themselves, mutate into other forms, and inject codes into a computer or network without the creator's knowledge or permission. Other forms of malware, on the other hand, function more like Trojans, spyware, and viruses in that they are designed to do specific things. A hacker could attack a web server and disperse adware through the server; this is analogous to how a real virus spreads from one computer to another.

While it's possible to find many different forms of a biological virus, the best analogy to explain the spreadability of viruses is how software viruses spread between computers. For example, a program that installs itself onto a computer without the permission of the host will likely spread into all computers on the network. Similarly, a worm that embeds itself into an executable file can spread from computer to computer. There are many different kinds of ways to distribute these types of programs, but the most common ways are through email, file sharing networks, and the Internet. It's also possible for a virus to propagate from host to host, but this has yet to be observed in any real world application.

The most interesting and widely spread kind of virus is the boot sector infector. These viruses make their way into a computer's core memory and begin to execute without the user's permission. Most people are familiar with the so-called "virus" that causes computers to crash (the "IAB" virus, for instance). This kind of virus spreads by embedding itself into an application, boot sector, or the operating system and then spreading through the entire host without the user's permission.

Because of this broad definition, it's sometimes difficult to tell if a particular file is really an infected file. If you're unfamiliar with a particular file, you should attempt a standard anti-virus software removal before using other options. One example is if you suspect that your computer had become infected with an email virus, you could remove its attachments and compare the results with a known list of emails. Viruses use several techniques to avoid detection. Some simply hide themselves in commonly used file formats; others change their names, are encrypted, or use different codes when displayed.

This analogy might also explain the success of viruses. While there's no worm, bacteria, or virus that can replicate itself, they can spread rapidly between machines. Like human cells, they divide uncontrollably and tend to attack other cells. Just as you wouldn't want one virus to attack another without your knowledge, you don't want any viruses to reproduce themselves without your knowledge. If you suspect a biological virus is causing problems in your life (such as chronic headaches, stomach aches, or general malaise), see your doctor immediately.