Title:
Computer Virus

Word Count:
603

Summary:
Who can forget the way the world was frozen with the threat of the "Millennium Bug"? While people around the globe should have been counting down to a phenomenal celebration, we were too busy preparing for certain doom and gloom beset by a computer virus. Of course, the clock struck twelve on January 1, 2000 and a new millennium quietly began, bug-free.

Those unfortunate enough to have had to deal with a computer virus knows all too well the damage that can be done. F...

Keywords:

Article Body:
Who can forget the way the world was frozen with the threat of the "Millennium Bug"? While people around the globe should have been counting down to a phenomenal celebration, we were too busy preparing for certain doom and gloom beset by a computer virus. Of course, the clock struck twelve on January 1, 2000 and a new millennium quietly began, bug-free.

Those unfortunate enough to have had to deal with a computer virus knows all too well the damage that can be done. From taking on annoying quirks, to erasing files, to completely obliterating computers or entire systems, the powerful effect of a computer virus is nothing to sneeze at. Computer viruses pose real threats that can be minimal, or can cause worldwide destruction.

In computer security technology circles, the definition of a computer virus is a "self-replicating program that spreads by inserting copies of itself into other executable code or documents". A computer virus behaves in a manner similar to a biological virus, which spreads by inserting itself into living cells.

Extending the analogy, the insertion of a computer virus into a program is termed as an "infection" and the infected file (or executable code that is not part of a file) is called a "host". Viruses are one of several types of malicious software, also known as "malware". The term "virus" is often extended

to refer to worms, Trojan horses and other sorts of malware. These are less common than they used to be, however, so the inclusion of these types of malware can be confusing to computer users. This confusion can have serious implications, as it can lead to a focus on preventing one genre of malware over another, potentially leaving computers vulnerable to future damage. The basic rule holds that computer viruses can only damage software, not hardware.

Viruses have targeted in the following types of hosts:

* Boot sectors of floppy disks; hard disk partitions.

* Master boot record of a hard disk.

* Binary executable files (.COM-files and .EXE-files in MS-DOS; portable executable files in Microsoft Windows; ELF files in Linux).

* General-purpose script files (batch files in MS-DOS and Microsoft Windows; shell script files on Unix-like platforms).

* Application-specific script files (Telix scripts).

* Documents containing macros (Microsoft Word documents).

A computer virus by nature is destructive, but others are created solely for the annoyance factor. Some viruses pester computer users with a delayed payload, also known as a "bomb". For example, a bomb virus might display a message on a specific day, or wait until it has infected a certain number of hosts. A time bomb occurs on a particular date or time, and a logic bomb occurs when the computer user takes an action that triggers the bomb. However, the predominant negative effect of viruses continues to be their uncontrolled self-reproduction, which wastes or overwhelms computer resources.

To hinder the continuous spread of computer viruses, programmers have created anti-virus software. However, a fast infector can infect every potential host file that it's able to access. This presents a special problem to anti-virus software. A virus scanner will perform a system-wide scan, accessing every potential host file on the computer. If the virus scanner fails to notice that a virus exists in the computer's memory, the virus can "piggy-back" on the virus scanner, and infect every file that is scanned. Fast infectors rely on their incredible spreading rate. To combat the problem, certain anti-virus software programs, like the well-known Spyware, are expanding to cover worms and other threats.

Like the potential devastation of the Millennium Bug in 2000, computer viruses

continue to present a real threat to single users and corporate networks alike.