Viruses
What They Are And One Reason Why People Make Them

Over recent years, computers have become synonymous with viruses and viruses don't show any signs of disappearing any time soon. In recent news, LiveScience.com reported that "Before the month is even done, April has set a record for virus e-mails."1 In the past, we would be comfortable in telling new computer users not to worry about viruses and that catching a computer virus is rare. Today, that would be some of the worst advice we could give anyone. As reported in countless news reports, computer viruses are rampant and they're extremely worrisome. This article will describe what viruses are and then point you in the direction of some rather unique protection and prevention.

In short, a computer virus is a software program designed to destroy or steal data. It attacks computers via distribution - often unknowingly - through email attachments, software downloads, and even some types of advanced web scripting. Viruses that destroy data are known as Trojan horses, viruses that explode their attacks are called bombs, and viruses that duplicate themselves are called worms. Some viruses are a combination of each, however they can be further identified according to where they're located on a computer.

A virus originating from the boot sector of a computer is a boot-sector virus and this nasty devil does its dirty work the moment a computer is turned on. A virus that attaches itself to (infects) other programs is a file virus and activates the moment that an infected program starts. File viruses may also be referred to as parasitic viruses, however should a virus work from both the boot-sector and from an infected program, the virus is then known as a multipartite virus.

Why viruses exist remains a mystery, however we had privy access to the mind behind a virus programmer who explained his motivation behind his destructive inclinations. Apparently, this person had a deep grudge against a popular online service which shall remain unnamed. In this hacker's mind, the online service failed to do a quality job in protecting children from online smut and as retaliation, he created and distributed a virus to as many file libraries of this service as he could. His intentions were to disable the computers of the online service's users so much that they wouldn't be able to connect for days. In his mind, the loss of connection meant loss of revenue for the online service.

Although the malicious code that this person generated may have worked for a small percentage of users, sufficed to say, the online service continued on and still exists today. Despite his motivation or intention, his efforts were null.

We wouldn't be surprised to learn if other motivations behind spreading viruses were similar to this person's, but that doesn't justify the damage that viruses do. Innocent people become pawns for the evil plans of others who've convinced themselves they're doing the "right" thing.

To protect a computer from getting a virus, or clean a virus from a computer system once infected requires the use of an antivirus utility. But may be something else we can do. Perhaps we could make an effort to educate the people who want put viruses into the public about ways to display dissatisfaction with a service or product that don't involve harming innocent parties. In doing so, we just might reduce the number of virus news stories and protect our own investments at the same time.

PPPPP

Word count 578
1 Source: http:// news.yahoo.com/s/livescience/20070426/sc_livescience/recordset tingspameffortturnscomputersintozombies