Software

The Cyberpunk Project

Computer Virii

By definition, a computer virus is any program that is created to cause damage to the targeted system. Just like the name implies, a computer virus resembles a biological virus in many ways. Different virii cause different symptoms to arise, but most do the following : infect the host, cause damage to all files it touches, replicates itself, and infects all other systems that come into contact with it.

A computer virus, like all other programs, is created by a programmer. Unfortunately, there are literally millions of places where a given system might "contract" a virus. Simply by visiting a website one could be downloaded. The common method is through file attachments in email. By opening or executing the attachment, the virus loads into memory and starts doing it's damage. Some email programs are even easier to take advantage of, a topic we will discuss a little later.

These virii come in various shapes and sizes, with varying levels of damage. There are three main classifications of viruses, determined by it's method of infection :

- Program : infects/attaches to executable files (files that have extension like COM, EXE, OVL, DRV, SYS and BIN).
- Boot : infects the Boot Record, Master Boot, FAT, and/or Partition Table.
- Multipartite : a combination of a program and a boot infector virus.

Characteristics

Each type of virus has one or more of these characteristics :

Memory Resident
: Stays in memory and can easily replicate itself. This is the most common type of virus.

Non-Resident
: Does it's damage ONLY while host program (the one it has infected & attached itself to) is open. This one isn't as common.

Stealth
: Avoids detection by doing the following :
Full - redirects disk reads to avoid detection (keeps the drive from reading it's particular location on the hard disk).
Size - Disk directory data is altered hide the additional space taken up by the virus (rewrites the file's size so that it appears to be the same size as it was prior to infection).

Encrypting

The virus converts itself into cryptic symbols. In order to launch (execute), however, it must decrypt (which is when it is normally detected by antivirus software).

Polymorphic
: This type of virus has the ability to alter it's code from one infection to another. This is one of the largest challenges for antivirus detection programs.

Triggered Event
: Like the name implies, this virus is triggered by an event, such as a date, keyboard stroke, a DOS function, deleting files... etc.

In the Wild
: A virus that is "in the wild" is one that has caused infections outside a laboratory situation. In other words, it has not been found or properly categorized by antivirus developers, and its effects are unknown.

Bots

A bot is a software robot. On the Net, robots have taken on a new form of life. Bots are normally used for digging through large amounts of data You give a bot directions and it bring back answers, examples : search engines. Bots can also be used to perform some repetative tasks in the Net, examples : IRC bots.

Since all Web servers are connected, robot-like software is the perfect way to perform the methodical searches needed to find information. For example, Web search engines send out robots that **crawl** from one server to another, compiling the enormous lists of URLs that are the heart of every search engine. Shopping bots compile enormous databases of products sold at online stores.

The term bot has become interchangeable with **agent**, to indicate that the software can be sent out on a mission, usually to find information and report back. Strictly speaking, an agent is a bot that goes out on a mission. Some bots operate in place; for example, a bot in Microsoft Front Page automates work on a Web page.

Bots have great potential in **data mining**, the process of finding patterns in enormous amounts of data. Because data mining often requires a series of searches, bots can save labor as they persist in a search, refining it as they go along. Intelligent bots can make decisions based on past experiences, which will become an important tool for data miners trying to perfect complex searches that delve into billions of data points.

Bots were not invented on the Internet, however. Robotic software is generally believed to have been created in the form of *Eliza*, one of the first public displays of **artificial intelligence**. Eliza is a computer programmer that can engage a human in conversation : Eliza asks the user a question, and uses the answer to formulate yet another question. Artificial intelligence is an advanced form of computer science that aims to develop software capable of processing information on its own, without the need for human direction.

At times, Webmasters look on some forms of robots as a nuisance. A spider robot may uncover information the Webmaster would prefer would remain secret; occasionally, a bot will mis-behave as it crawls through a Web site, looking for URLs over and over, and slowing down the server's performance. As a result, search engine developers have formed standards on how robots should behave and how they can be excluded from Web sites.

References

Software Piracy