Tech Info Library

Computer Viruses (part 1 of 4)

Revised: 9/26/94
Security: Everyone

Computer "Viruses" (part 1 of 4)

==========

This article last reviewed: 15 April 1988

GENERAL ISSUES

What is a virus?

A virus is a program with two distinct functions:

- It spreads itself from machine to machine (self-reproducing code). This includes the actual infection of other systems as well as the stashing away of code into as many "carriers" as possible.

- It implements the "symptoms" planned by the perpetrator of the virus. This could be any number of things, up to and including erasing a disk on a specific date.

A Bit of History

Computer viruses have been around for almost as long as computers. John Van Neumann, the father of the modern computer, toyed with the idea of self-reproducing computer code as early as 1948. In the late 1970s, there was even a training ground for the writing of viruses. It was a program called Core Wars that implemented an artificial environment pitting two virus programs against each other.

Viruses Are Not Unique to the Macintosh

The Macintosh is not the only system to be plagued by viruses. Mainframe and minicomputers are also targets for virus programmers. One of the more recent mainframe incidents was the virus that invaded IBM's mail system and brought it to its knees for a couple of days. IBM PC users have been experiencing viruses for several years now. The most common method of attack is through the COMMAND.COM file. The Macintosh community has been lucky to have gone so long without virus programming becoming the thing to do.

Not All Viruses Are Meant To Be Damaging, But...

Viruses are not all meant to be damaging. The programmer may just want to prove he can do it and have the satisfaction of reading about it in magazines and on the BBS network. Sometimes, these viruses can cause problems anyway. For example, the virus that has prompted this series of articles was meant to be benign except in specific cases. However, it takes up memory and processing time and has caused random side effects such as printing problems and system crashes.

Don't Panic; Don't Overreact

If you think that you have a virus, it's important to not overreact. It is important to take a step back and evaluate the situation calmly. Once you know that you have a virus and what it has infected, it is a relatively easy thing to combat. This document contains enough information for you to deal with most viruses.

Unix Viruses

In all of this, there has not been much discussion of Unix viruses, but they do exist, and the spread of public domain software is almost as great in the Unix world as it is in the microcomputer world.

THE GREAT VIRUS HUNT

When Do You Suspect You Might Have a Virus?

When your computer begins to do things out of the ordinary, or when it stops being able to do things it has always done in the past. The problem with this is that corrupted system files can lead to similar symptoms even though a virus isn't involved. When problems occur, they are much more likely to be the result of non-virus difficulties. When you have ruled out the standard problem areas, you should look into the possibility that your system has been infected by a virus.

What to Look For If You Think You Have a Virus

Look for invisible files in your System folder that don't belong there. Unless you specifically have an application that creates invisible files in the System folder, every invisible file in the System folder should be suspect. Also, a general check of all the files in your System folder for resources that don't belong in those files is well worth the effort.

Files and Resources a Virus Might Infect

- Any and all applications

- HyperCard Stacks (the MacMag virus was spread via a HyperCard stack)

- Files in the System folder, including:

System
Finder
Note Pad file
Scrapbook file
Clipboard file
Easy Access
Sound
Mouse
Startup Device
Monitors
Color
General
Keyboard
LaserWriter
ImageWriter
AppleTalk ImageWriter
ImageWriter LQ

In other words, all system files.

Files a Virus Might Damage Inadvertently

- Any file on an infected volume or system, including system files, documents, applications, etc.

Public Domain Issues

Most viruses spread via public bulletin board systems and are hidden in public domain programs. "Sexy Ladies," a program distributed at a MacWorld Expo in San Francisco, erased whatever hard disk or floppy disk it was on when it was launched.

Network Issues

The use of networks can easily enhance the spread of a virus. Different scenarios are possible, with the simplest being a public domain folder on a server that everyone gets the latest neat stuff from. Also, shared applications residing on a server could become infected, which would then infect every machine that those applications were run on.

Tech Info Library Article Number:2821