No. 80, July 2000

THE COMPUTER CORNER

A Virus Primer

- by Stan Kaplan, WB9RQR
105 Martin Drive
Port Washington, WI 53074-9654
(262) 284-9346
skaplan@mcw.edu

Nearly everyone has heard of the recent spread of the virus contained in an email message called “ILOVEYOU”, with the ability to overwrite (destroy) many files, and the ability to then mail itself to everyone in your Microsoft Outlook Address Book. However, did you know you cannot become infected unless you open an attachment to that message? Just opening and reading text-based email messages does NOT subject you to the danger of being infected with ANY current virus. Did you know that there is no known instance of a virus damaging computer hardware? Not yet. Did you know that there are well over 5,000 different viruses and variations that have been documented over the years?

Well, we all have to deal with viruses – they are here to stay. Weird folks with what could probably be classed as an abnormal psychological makeup continue to write and release them. Contrary to what some say, it is not the antiviral software writers who write viruses. It is the weird folks who hide behind their anonymity. So what are viruses and how do they work? This month’s issue will present a virus primer to help you understand the answer.

A virus is nothing more or less than a single tiny program, written to hide itself, to propagate itself and to do damage to the recipient’s computer files. Usually the term is used loosely to describe any sort of infection that a computer can catch, but all these infections are most correctly classed into three groups:

1. A WORM is a self-reproducing program that copies and spreads itself on networked computers. Unlike viruses, worms don’t hide themselves inside of other programs. They just make copy after copy of themselves, which clogs up circuits and uses up hard disk space. They use up so many resources that they can slow down an entire network.

2. A TROJAN HORSE is another infection that is usually not able to reproduce itself. Usually these executable programs (with a .COM or .EXE file extension) masquerade as a useful program. Example: if a damaging program was introduced into your computer named MSWORD.EXE and it overwrote the original MSWORD.EXE, it would be run the first time you ran your word processor. It would do damage immediately. The Horse of Troy was thought to be a gift, but it really contained a payload of soldiers hidden in the hollow statue.

3. A VIRUS, which usually has the following three characteristics:
   a. It has an incubation period. That is, it does not usually do damage immediately upon infecting a system. Rather, it drops a payload (the damaging effects) at some predetermined time after infection, such as the 6th of March, or Friday the 13th, or Tuesday at 3:00 p.m.
   b. It can replicate itself (they are contagious). Once having infected a computer, it tries to hitch a ride on a floppy to the next machine victim. Alternatively, they ride a wire. Or a CD-ROM. Or a tape. Yes, virus-infected files can be transferred from computer to computer using any of these means.
   c. It is destructive! It does some kind of damage, overwriting files or scrambling the File Allocation Table (FAT) so you can no longer access anything on your hard drive. Or it can do other bad stuff without consent of the owner. What about the virus that does no direct damage to your files, but which sends confidential information from your machine

to a remote Internet address next time you log on? Is that destructive? You bet! The payload is theft of your confidential information. Let me take that a step further – the payload is theft of ANY information, without your consent, confidential or not! Did you know that, right now, there are companies on the Internet that do that for profit? But that issue is the subject for another article.

So where do they hide? A virus is a tiny piece of computer code. Real programs often have some blank space inside the file – space that has no code in it. The virus can hide there, in the blank space. Sometimes the virus pushes the program over to one end of the file, so that it has enough room to get in. Clever beasties! Sometimes there just is not enough room, so it overwrites part of the original program, thus destroying it. However, the virus doesn't care, so long as IT can run.

How can viruses outfox antiviral software? AV software looks inside each file it scans for a virus signature, a little piece of the virus code that distinguishes it from all normal programs and other viruses. Sometimes this signature is human understandable ("STONED", "CONCEPT"), but most often it is not. Virus writers have devised several ways to hide their signatures.

If you are a virus, one way to confuse AV software is to change your signature each time you infect a new computer. Viruses that can do this are the so-called polymorphic viruses (poly = many, morphos = form). There is even one writer out there, self named the "Dark Avenger," who wrote a polymorphic engine. This engine isn't a virus by itself. It is a piece of code he gave to the virus-writing world which, when included with a virus written by anyone else, would turn the virus into a polymorphic type. Talk about specialization!

Another way to give grief to AV software is to encrypt yourself, much like PKZIP encrypts (and compresses) a file. These encrypting viruses effectively hide their signatures from view, but they can't replicate or run while encrypted. They have to unencrypt themselves to do that. Thank goodness! When unencrypted, their signatures are hanging out there for all AV scanners to see.

Another way that AV software can detect new virus infections is to keep a database of all file sizes on the hard drive. When a virus infects, it often increases the file size, and the AV software detects the change. One ploy taken by stealth viruses is to mask this change in file size when infecting a new file, thus confounding the AV software. An even sneakier ploy by stealth viruses is as follows. Some of them are able to detect when a virus scanning AV program is about to open the file in which they are hiding in order to "sniff them out." Some stealth viruses, upon detecting the bloodhounds on their trail, will then "bail out" of the file temporarily, only to return when the AV software is finished looking at their host file! Other stealth viruses will stay in their host file, but will quickly put a good copy of their host file under the nose of the AV scanner. They keep a stash of a good copy of their host file hidden somewhere on the drive for just this purpose! Amazing!

Wouldn't it be wonderful if all that talent used by virus writers could be channeled into writing decent software, instead of the bloatware coming out of Microsoft and other software houses. What a waste! Not only is their talent lost to constructive enterprise, but so is the time and talent of all those who must be employed to write the AV software to thwart them. What a waste!

Perhaps down the line we'll have an article on steps you can take to protect your machine. Most steps are common sense, but it is good to see them organized in one place, so you can make a mental note of them. Hope you had a great Field Day!! Happy computing.