Computer Virus Myths

by Rob Rosenberger
with Ross Greenberg

A number of myths have popped up recently about the threat of computer "viruses". There are myths about how widespread they are, how dangerous they are, and even myths about what a computer virus really is. We'd like the facts to be known.

The first thing you have to understand is that a virus is a programming technique that falls in the realm of "Trojan horses." All viruses are Trojan horses, but very few Trojan horses can be called a virus.

That having been said, it's time to go over the terminology we use when we lecture:

BBS	Bulletin Board System. If you have a modem, you can call a BBS and leave messages, transfer computer files back & forth, and learn a lot about computers. (What you're reading right now most likely came to you from a BBS, for example.)
Bug	an *accidental* flaw in the logic of a computer program that makes it do things it shouldn't really be doing. Programmers don't mean to put bugs in their program, but they always creep in. The first bug was discovered by pioneer Grace Hopper when she found a dead moth shorting out a circuit in the early days of computers. Programmers tend to spend more time debugging their programs than they do writing them in the first place.
Hacker	someone who really loves computers and who wants to push them to the limit. Hackers don't release Trojan horses onto the world, it's the *wormers* who do that. (See the definition for a "wormer".) Hackers have a healthy sense of curiosity: they try doorknobs just to see if they're locked, and they tinker with a piece of equipment until it's "just right."
Shareware	a distribution method for quality software available on a "try before you buy" basis. You pay for the program only if you find it useful. Shareware programs can be downloaded from BBSs and you are encouraged to give an evaluation copy to friends. There are few advertising & distribution costs, so many shareware applications can rival the power of off-the-shelf counterparts, at just a fraction of the price.
Trojan horse	a generic term describing a set of computer instructions purposely hidden inside a program. Trojan horses tell a program to do things you don't expect it to do. The term comes from a historic battle in which the ancient city of Troy was offered the "gift" of a large wooden horse that secretly held soldiers in its belly. The Trojans rolled it into their fortified city....
Virus	a term for a *very* specialized Trojan horse that can spread to other computers by secretly "infecting" programs with a copy of itself. A virus is the only type of Trojan horse which is *contagious*, like the common cold. If it doesn't meet this definition, then it isn't a virus.
Worm	a term similar to a Trojan horse, but there is no "gift" involved. If the Trojans had left that wooden horse outside the city, they wouldn't have been attacked -- but worms can bypass your defenses. An example is an unauthorized program designed to spread itself by exploiting a bug in a network software package. (Such programs could possibly also contain a virus that activates when it reaches the computer.) Worms are usually released by someone who has normal access to the computer or network.
Wormers	the name given to the people who unleash destructive Trojan horses. Let's face it, these people aren't angels. What they do hurts us. They deserve our disrespect.

Viruses, like all Trojan horses, are purposely designed to make a program do things you don't expect it to do. Some viruses are just an annoyance, perhaps only displaying a "Peace on earth" message. The viruses we're worried about are the ones designed to destroy your files and waste the valuable time you'll spend to repair the damage.

Now you know the difference between a virus and a Trojan horse and a bug. Let's get into some of the myths:

All purposely destructive code comes as a virus.

Wrong. Remember, "Trojan horse" is the general term for purposely destructive code. Very few Trojan horses are actually viruses.

All Trojan horses are bad.

Believe it or not, there are a few useful Trojan horse techniques in the world. A "side door" is any command not documented in the user manual, and it's a Trojan horse by definition. Some programmers install side doors to help them locate bugs in their programs. Sometimes a command may have such an obscure function that it makes sense not to document it.

Viruses and Trojan horses are a recent phenomenon.

Trojan horses have been around since the first days of the computer. Hackers toyed with viruses in the early 1960s as a form of amusement. Many different Trojan horse techniques were developed over the years to embezzle money, destroy data, etc. The general public wasn't aware of this problem until the

IBM PC revolution brought it into the spotlight. Just five years ago, banks were *still* covering up computerized embezzlements because they believed they'd lose too many customers.

Computer viruses are reaching epidemic proportions.

Wrong again. Viruses may be spread all over the planet but they aren't taking over the world. There are only about fifty or so known virus "strains" at this time and a few of them have been completely eliminated. Your chances of being infected are slim if you take proper precautions. (Yes, it's still safe to turn on your computer!)

Viruses could destroy all the files on my disks.

Yes, and a spilled cup of coffee will do the same thing. If you have adequate backup copies of your data, you will be able to recover from a virus/coffee attack. Backups mean the difference between a nuisance and a disaster.

Viruses have been documented on over 300,000 computers.

This statistic comes from John McAfee, a self-styled virus fighter who seems to come up with all the quotes the media love to hear. We assume it includes every floppy disk ever infected by a virus, as well as all of the computers participating in the Christmas worm attack. (That worm was designed for a particular IBM network software package; it never infected the computers. Therefore, it wasn't a virus. The Christmas worm attack can't be included in virus infection statistics.) Most of the media don't understand computer crimes, so they tend to call almost anything a virus.

Viruses can be hidden inside a data file.

Data files can't wreak havoc on your computer -- only an executable program can do that. If a virus were to infect a data file, it would be a wasted effort.

Most BBSs are infected with viruses.

Here's another scary myth drummed up in the big virus panic. Very few BBSs are really infected. (If they are infected, they won't be around for long!) It's possible a dangerous *file* could be available on a BBS, but that doesn't mean the BBS itself is infected.

BBSs and shareware programs spread viruses.

"The truth," says *PC Magazine* publisher Bill Machrone, "is that all major viruses to date were transmitted by commercial packages and private mail systems, often in universities." The Peace virus, for example, made its way into a commercial software product sold to thousands of customers. Machrone goes on to say that "bulletin boards and shareware authors work extraordinarily hard at policing themselves to keep viruses out." Many reputable sysops check all new files for Trojan horses; nationwide sysop networks help spread the word about dangerous files. You should be careful about software that comes from friends & BBSs, that's definitely true -- but you must also be careful with the software you buy at computer stores. The Peace virus proves it.

My computer could be infected if I call an infected BBS.

BBSs can't write information on your disks -- that's handled by the communications software you use. You can only transfer a dangerous file if you *let* your software do it. (In rare cases, a computer hooked into a network could be sent a dangerous file or directly infected, but it takes specialized software to connect a computer into a network. BBSs are NOT networks.)

My files are damaged, so it must have been a virus attack.

It could also have been caused by a power flux, or static electricity, or a fingerprint on a floppy disk, or a bug in your software, or perhaps a simple error on your part. Power failures and spilled cups of coffee have destroyed more data than all the viruses combined.

Donald Burleson was convicted of releasing a virus.

A recent Texas computer crime trial was hailed all over the country as a "virus" trial. Donald Burleson was in a position to release a complex, destructive worm on his employer's mainframe computer. This particular worm wasn't able to spread itself to other computers, so it wasn't a virus. The prosecuting attorney, Davis McCown, claims he "never brought up the word virus" during the trial. So why did the media call it a virus?

1. David Kinney, an expert witness testifying for the *defense* (oddly enough), claimed he believed Burleson unleashed a virus. This is despite the fact that the programs in question had no capability to infect other systems. The prosecuting attorney didn't argue the point and we don't blame him -- Kinney's bizarre claim on the witness stand probably helped sway the jury to convict Burleson, and it was the defense's fault for letting him testify.

2. McCown doesn't offer reporters a definition for the word virus. He gives the facts behind the case and lets the reporters deal with the definitions. The Associated Press and USA Today, among others, used such vague terms that *any program* could be called a virus. If we applied their definitions in the medical world, we could safely claim penicillin is a biological virus (which is absurd).
3. McCown claims many of the quotes attributed to him "are misleading or fabricated" and identified one in particular which "is total fiction." Reporters occasionally print a quote out of context, and McCown apparently fell victim to it. (It's possible a few bizarre quotes from David Kinney or John McAfee were accidentally attributed to McCown.)

Robert Morris Jr. released a benign virus on a defense network.

It may have been benign, but it wasn't a virus in the strict technical sense. Morris, the son of a chief scientist for the National Security Agency, allegedly became bored and decided to take advantage of a tiny bug in the Defense Department's network software. (We say "alleged" because Morris hadn't been charged with a crime when we went to press.) That tiny bug let him send a worm through the network and have it execute when it reached certain computers. Among other things, Morris's "Internet" worm was able to tell some computers to send copies of itself to other computers in the network. The network became clogged in a matter of hours. The media called the Internet worm a "virus" (like it called the Christmas worm a virus) because it was able to spread itself to other computers. But it didn't *infect* those computers, so it can't be called a virus. (We can't really fault the press for calling it one, though. It escapes the definition of a virus because of a technicality.) A few notes:

1. This worm worked only on Sun-3 & Vax computers with a UNIX operating system that was linked to the Internet network;
2. The 6,200 affected computers should not be counted in any virus infection statistics (they weren't infected);
3. Yes, Morris could easily have added some infection code to make it a worm/virus if he'd had the urge; and,
4. The network bug Morris exploited has since been fixed.

Viruses can spread to all sorts of computers.

All Trojan horses are limited to a *family* of computers, and this is especially true for viruses. A virus designed to spread on IBM PCs cannot infect an IBM 4300-series mainframe, nor can it infect a Commodore C64, nor can it infect an Apple MacIntosh.

My backup disks will be destroyed if I back up a virus.

No, they won't. Let's suppose a virus does get backed up with your other files. Backups are just a form of data, and data can't harm your system. You can recover the important files from your backups without triggering the virus.

Anti-virus software will protect me from viruses.

Anti-virus packages offer some good front-line protection, but they can be tricky to use at times. You could make a crucial mistake in deciding whether to let a "flagged" event take place. Also, Trojan horses can be designed to take advantage of holes in your defense.

Copy-protected software is safe from an attack.

This is totally wrong. Copy-protected software is the *most* vulnerable software in a Trojan horse attack. You may have big problems trying to use or re-install such software, especially if the master disk was attacked. It should also be noted that copy-protection schemes rely on extremely tricky techniques which have occasionally "blown up" on users. Some people mistakenly believe they were attacked by a clever virus.

Viruses are written by hackers.

Yes, hackers have written viruses -- just to see how they operate. But they DON'T unleash them to an unsuspecting public. Wormers are the ones who do that. (You can think of a wormer as a hacker who was seduced by the Dark Side of The Force.) Hackers got a bum rap when the press corrupted the name.

We hope this dispels the myths surrounding the virus scare. Viruses DO exist, many of them will cause damage, and all of them can spread to other computers. But you can defend yourself from an attack if you keep a cool head and a set of backups.

The following guidelines can shield you from Trojan horses and viruses. They will lower your chances of being attacked and raise your chances of recovering from one.

1. Download files only from reputable BBSs where sysops check every program for Trojan horses. If you're still afraid, consider getting your programs from a BBS or "disk vendor" company which gets its programs directly from the author;
2. Let a newly uploaded file "mature" on a BBS for one or two weeks before you download it (others will put it through its paces).
3. Set up a procedure to regularly back up your files, and follow it religiously. Consider purchasing a user-friendly backup program that takes the drudgery out of backing up your files.
4. Rotate between two sets of backups for better security (use set #1, then set #2, then set #1...).
5. Consider using a program which will create a unique "signature" of all the *programs* on your computer. Once in a while, you can run this program to determine if any of your applications have been modified -- either by a virus or by a stray gamma ray.
6. If your computer starts acting weird, DON'T PANIC. It may be a virus, but then again it may not. Immediately reboot from a legitimate *copy* of your master DOS disk. Put a write-protect tab on that disk just to be safe. Do NOT run any programs on your regular disks (you might activate a Trojan horse). If you don't have adequate backups, try to bring them up to date. Yes, you might be backing up a virus as well, but it can't hurt you as long as you don't run any of your normal programs. Set your backups off to the side. Only then can you safely hunt for the problem.
7. If you can't figure out what's wrong with your computer, and you aren't sure of yourself, just turn it off and call for help. Consider calling a local computer group before you hire an expert to fix your problem. If you need a professional, consider hiring a regular computer consultant before you call on a "virus expert."
8. If you can't figure out what's wrong with your computer, and you *are* sure of yourself, execute a low-level format on all of your regular disks (you can learn how to do it from almost any BBS), then do a high-level format on each one of them. Next, carefully re-install your software from legitimate copies of the master disks, not from the backups. Then, carefully restore only the data files (not the executable program files!) from your backup disks.

If you DO find a Trojan horse or a virus, we'd appreciate it if you'd mail a copy to us. (But please, don't handle one unless you *know* what you're doing.) Include as much information as you can, and put a label on the disk that says it contains a Trojan horse or virus. Send it to Ross Greenberg, 594 Third Avenue, New York, NY 10016. Thank you.

Ross Greenberg is the author of a popular Trojan/virus detection program. Rob Rosenberger is the author of a modem analysis program. These men have never met in person; they worked on this story completely by modem.
