The other side of the hacker

Hackers are not the kind of dark, underworld creatures as depicted in the movies. But the ones who make the news are hackers, who have gone astray. Actually, there are three kinds of hackers, the White Hats, the Black Hats, and the Gray Hats.

CONTINUED FROM PAGE 17

4. Be careful who you share information with. Generally, if you don't know their voice phone number, name, and occupation or haven't spoken with them voice on non-info trading conversations, be wary.
5. Never leave your real phone number to anyone you don't know. This includes logging on boards, no matter how k-rad they seem. If you don't know the sysop, leave a note telling some trustworthy people that will validate you.
6. Never hack government computers. Yes, there are government systems that are safe to hack, but they are few and far between. And the government has infinitely more time and resources to track you down than a company who has to make a profit and justify expenses.
7. Never codes unless there is *NO* way around it. You use codes long enough, you will get caught.
8. Never afraid to be paranoid. Remember, you *are* breaking the law. It doesn't hurt to store everything encrypted on your hard disk, or keep your notes buried in the backyard or in the trunk of your car.
9. Watch what you post on boards. Most of the really great hackers in the country post *nothing* about the system they're currently working, except in the broadest sense (I'm working on a UNIX, or a COSMOS, or something generic. Not "I'm hacking into General Electric's Voice Mail System" or something inane and revealing like that.)
10. Don't be afraid to ask questions. That's what more experienced hackers are for. Don't expect *everything* you ask to be answered, though. There are some things (LMOS, for instance) that a beginning hacker shouldn't mess with. You'll either get caught, or screw it up for others, or both.

Well, as you can see, hackers are not the kind of dark, underworld creatures as depicted in the movies. But the ones who make the news are hackers, who have gone astray. Actually, there are three kinds of hackers, the White Hats, the Black Hats, and the Gray Hats. The white guys are actually system ops who are in charge of maintaining the security of large systems, and their job is quite challenging, not to mention high-paying. The Black Hats are what people commonly know as "hackers", and the gray ones are somewhere in between these two. They are freelancers who DO hack into a system, but then inform the system admin about the chinks in the armor of the network. Mostly these guys are people with a mission; to make the information superhighway more secure. They also often help track, catch or shut down people or firms who put indecent items on the net, or other black hats.

I might as well stop here. But I hope this has helped to clear out any misconceptions you might have had about hackers. And in my own opinion, hackers are not a menace, but a boon to the digital world; they do make it a safer place.

Viruses: A general autopsy!

MANNAN MASHHUR ZARIF

Viruses are programs just like any other on your PC. They consist of instructions for or codes that your computer executes. What makes viruses special is that they do their "job" by placing self-replicating code in other programs, so that when those other programs are executed, even more programs are "infected" with the self-replicating code. "Self-replicating code" is simply a program that copies itself to other programs. This self-replicating code, when triggered by some event, may do a potentially harmful act to your computer--but this is strictly optional. Only a minority of viruses contain deliberately destructive code.

VIRUSES: A feared word by most computer users and netizens! The spread of viruses through the Internet is the most rampant version of cyber crime; however, viruses can spread in other modes as well. The term 'virus' creates confusion amongst numerous computer laymen out there. So here is a quick look at what viruses actually are and how they behave!

What Do Viruses Do?

I'm going to present a detailed explanation of viruses and other types of malicious software. For now, it's enough to understand that viruses are potentially destructive software that spreads from program to program or from disk to disk. Computer viruses, like biological viruses, need a host to infect; in the case of computer viruses this host is an innocent program. If such a program is transferred to your PC, other programs on your PC will become infected. Even though some viruses do not intentionally damage your data, I consider all viruses to be malicious software since they modify your programs without your permission with occasional disastrous results.

The bottom line is that if you have a virus, you are no longer in control of your PC. Every time you boot your PC or execute a program the virus may also be executing and spreading its infection. While most viruses haven't been written to be destructive, almost all viruses can cause damage to your files--mostly because the viruses themselves are very poorly written programs. **If viruses destroy nothing else, they destroy your trust in your PC--something that is quite valuable.**

Are Viruses Mostly Hype?

Unfortunately not! There is some confusion about this issue because some extreme claims have been made regarding numbers of viruses and how likely you are to become infected. During the Michelangelo media extravaganza in early 1991, some exaggerated figures were presented in the media which led some people to suspect that all viruses were nothing but hype. One company was quoted in *Information Week* that based on their reports, one out of four PCs was infected every month! You may also hear reports of there being from ten to thirty thousand different PC viruses with the number expected to double in six to nine months. So, are we faced with impending doom? No, not quite. The truth is viruses are very wide-spread but a relatively small number (about one-hundred) account for ninety percent of all infections. Many of these viruses are created by kids that can't even program. They use automated viruses creation programs that produce very poor quality viruses. These viruses are so obvious that they rarely spread in the wild. Still, viruses are a real threat that we can't afford to ignore. Viruses have been found on brand-new PCs, direct from the manufacturer, and on shrink-wrapped software, direct from the publisher. Viruses are not merely hype and no one is safe from potentially being infected. If you value your data and programs, you have to take some precautions.

How Serious Are viruses?

Viruses are a problem but they are not the main thing you should be concerned about. There are many other threats to your programs and data that are much more likely to harm you than viruses. **Problems such as hardware glitches, software conflicts, software bugs, and even typos are much more likely to cause undetected damage to your data than viruses.** A well known anti-virus researcher once said that you have more to fear from a spilled cup of coffee than from viruses. While the growth in number of viruses now puts this statement into question, it's still clear that there are many more occurrences of data corruption from other causes than from viruses. So, does this mean that viruses are nothing to worry about? Emphatically, no! It just means that we need to address the other threats to our data as well as viruses. Because viruses have been deliberately written to invade and possibly damage your PC, they are the most difficult threat to guard against. It's pretty easy to understand the threat that disk failure represents and what to do about it, but the threat of viruses is much more difficult to deal with.

Software attacks against your computer:

Viruses are one specific type of program written deliberately to cause harm to someone's computer or to use that computer in an unauthorized way. There are many forms of malicious software; sometimes the media calls all malicious software viruses, but it's important to understand the distinction between the various types. Let's examine the different types of malicious software:

Logic Bombs

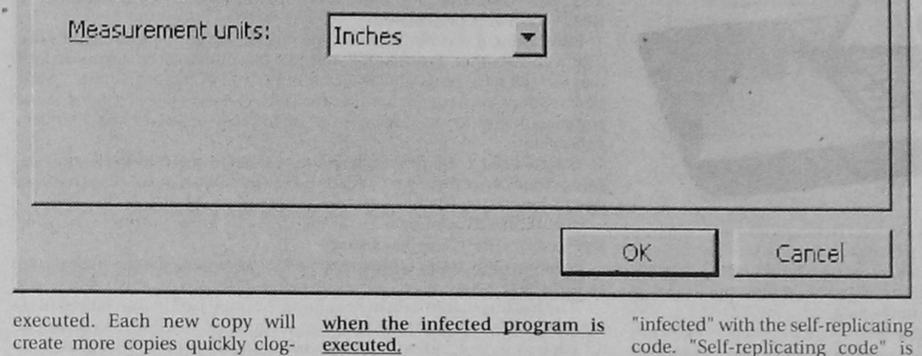
Just like a real bomb, a logic bomb will lie dormant until triggered by some event. CIH virus being the classic example! The trigger can be a specific date, the number of times executed, a random number. When the logic bomb is triggered it will usually do something unpleasant. This can range from changing a random byte of data somewhere on your disk to making the entire disk unreadable. The changing of random data on disk may be the most insidious attack since it would do a lot of damage before it would be detected.

Trojans

These are named after the Trojan horse which delivered soldiers into the city of Troy. Likewise, a Trojan program is a delivery vehicle for some destructive code (such as a logic bomb or a virus) onto a computer. The Trojan program appears to be a useful program, but when a certain event occurs, it will attack your PC in some way.

Worms

A worm is a self-reproducing program which does not infect other programs as a virus will, but instead creates copies of itself, which create even more copies. These are usually seen on networks and on multi-processing operating systems, where the worm will create copies of itself which are also executed. Each new copy will create more copies quickly clogging the system. The so called Morris ARPANET/INTERNET "virus" was actually a worm. It created copies of itself through the ARPA network, eventually bringing the network to its knees. It did not infect other programs as a virus would, but simply kept creating copies of itself which would then execute and try to spread to other machines.



Viruses:

Here's our definition:

A virus is a program which reproduces its own code by attaching itself to other programs in such a way that the virus code is executed when the infected program is executed.

You could also say that the virus must do this without the permission or knowledge of the user.

What Viruses Do:

Our virus definition is very general and covers all viruses. Let's consider specifically how this works. Viruses are programs just like any other on your PC. They consist of instructions for or codes that your computer executes. What makes viruses special is that they do their "job" by placing self-replicating code in other programs, so that when those other programs are executed, even more programs are "infected" with the self-replicating code. "Self-replicating code" is simply a program that copies itself to other programs. This self-replicating code, when triggered by some event, may do a potentially harmful act to your computer--but this is strictly optional. Only a minority of viruses contain deliberately destructive code. You could say that viruses are distributed in the form of a trojan. In other words, the virus code has been planted in some useful program. Since the virus infects other useful programs, absolutely any piece of executable code can suddenly become a trojan delivery vehicle for the virus.

Another way of looking at viruses is simply to consider them to be a program which can create copies of itself. These copies are inserted in other programs (infecting these programs). When one of these other programs is executed, the virus code (which was inserted in that program) executes, and places copies of itself in even more programs.

You'll notice that I used the word "attach" in our definition of a virus. This is because viruses can "attach" themselves to a program without directly modifying that program. This might seem hard to believe at this point, but I'll soon explain exactly how they accomplish this trick.

General Virus Behaviur

Viruses come in a great many different forms, but they all potentially have two phases to their execution; the infection phase and the attack phase:

1. When the virus executes it will infect other programs. What is often not clearly understood is precisely when it will infect the other programs. Some viruses infect other programs each time they are executed, other viruses infect only upon a certain trigger. This trigger could by anything; it could be a day or time, an external event on your PC, a counter within the virus etc. Some viruses are very selective about when they infect programs; this is vital to the virus's survival. If the virus infects too often, it is more likely to be discovered before it can spread far. Virus writers want their programs to spread as far as possible before anyone detects them. This brings up an important point which bears repeating:

It is a serious mistake to execute a program a few times -- find nothing infected and presume there are no viruses in the program. You can never be sure that the virus simply hasn't triggered its infection phase!

Many viruses go resident in the memory of your PC just as a *terminate and stay resident* (TSR) program. This means the virus can wait for some external event such as inserting a diskette, copying a file, or executing a program to actually infect another program. This makes these viruses very dangerous since it's hard to guess what trigger condition they use for their infection. Resident viruses frequently corrupt the system software on the PC to hide their existence.

2. The second phase is the attack phase. Many viruses do unpleasant things such as deleting files or changing random data on your disk, simulating typos or merely slowing your PC down; some viruses do less harmful things such as playing music or creating messages or animation on your screen. Just as the virus's infection phase can be triggered by some event, the attack phase also has its own trigger. Viruses usually delay revealing their presence by launching their attack only after they have had ample opportunity to spread. This means that the attack may be delayed for years after the initial infection. The attack phase is optional; many viruses simply reproduce and have no trigger for an attack phase. Does this mean that these are "good" viruses? No, unfortunately not! Anything that writes itself to your disk without your permission is stealing storage and CPU cycles. This is made worse since viruses which "just infect", with no attack phase, damage the programs or disks they infect. This is not intentional on the part of the virus, but simply a result of the fact that many viruses contain extremely poor quality code. One of the most common viruses, the STONED virus is not intentionally harmful. Unfortunately the author did not anticipate other than 360K floppy disks, with the result that the virus will try to hide its own code in an area on 1.2mb diskettes which causes corruption of the entire diskette.

Quick Guidelines:

It's important to keep viruses in perspective. They are but one threat to your data and programs. They need not be regarded as mysterious and they are quite easy to understand. Here are a few tips to keep in mind when considering viruses:

- You can only get a virus by executing an infected program or booting from an infected diskette. Any diskette can be infected by a boot sector virus, even non-bootable diskettes.
- You cannot get a virus simply by being on the internet, or an online service. You will only become infected if you download an infected file and execute that file.
- Most viruses are transferred by booting from an infected diskette (e.g. Stoned, Form, Stealth-B, AntiExe, Monkey). Remove diskettes from your A drive as soon as you are through with the diskette.
- Make sure you have at least two backups for all of your files. Backups are essential not only to safely recover from virus infections, but also to recover from the other threats to your data.

Be sure to check all new software for viruses. Even shrink-wrapped software from a major publisher may contain a virus.