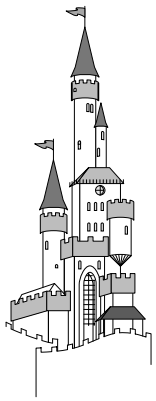
CHAPTER 9

Viruses, Trojan Horses, Hoaxes

(Spies and Saboteurs in the Village)



Now that John's village is defended and a nice thriving economy is booming in his town, what is left to do but sit back and enjoy? That would be nice, but it's not quite that easy. Enemies of the village can't attack by force now because John is prepared for that, but they can use subtlety and subterfuge. Spies and saboteurs can still attack the village and cause problems. Because these spies move through the village unseen, they represent a more difficult security problem than a direct attack. At least a direct attack announces itself. John would be able to see the armies massing, could watch their movements, and could respond to those pieces of information accordingly. But the spy or saboteur is a different threat entirely.

These enemies look and act like anyone who would normally be traveling through the village, even buying goods and visiting local spots of interest. They might come as peddlers, offering a service, or as entertainers. Once inside the walls and the security restraints, however, the spies can begin to do damage. Sometimes this damage is so slight that the town might not notice right away, or they might not suspect that incidents are related. But if left unchecked, these spies and saboteurs can destroy the village without firing a shot, or they can create enough disturbances that John will be unable to defend the town against the attack.

What can John do about these threats Ñ the ones he can't see or hear until they're causing problems? The answer for sure isn't easy, but let's look at the options. We have already discussed John's layered security. He has extra deputies in the more sensitive areas and requires credentials before anyone can get in. Those sensitive areas are isolated from less secure areas wherever possible. Additionally, the lookouts watch for suspicious activity in an attempt to prevent harm to the town's resources or defenses. Combining all these security measures

with active monitoring might seem to be the best John can do. But he has an additional point in his favor: He has some spies and saboteurs working for him too. The old saying "It takes a thief to catch a thief" holds true for catching such deceptive attacks. John hires spies to constantly update the sheriff about what is at risk, how the threat might be carried out, and signs to look for to identify an attack early. John's spies might even have information about specific people and the techniques they plan to use so the sheriff can check out those people.

The bad news is that if a totally new spy with a totally new technique appears, that new spy will probably not be caught. Then all John can do is try to contain the damage. With layered security, John can prevent serious losses, but he can't catch everyone. Luckily, he has one final, very effective tool in his arsenal: cooperation. John can talk to trusted neighboring villages and allies to gather and share information. He can talk to professionals who spend their days tracking and catching spies. He can keep lists of information about similar activities in different locations. By doing all this, John can put together a quick picture of new activities and threats and shut them down by early detection, limiting the overall damage.

Computer Viruses and Trojan Horses

What are the computer equivalents to spies and saboteurs? Viruses and Trojan-horse programs. Before we go farther, here are some definitions you'll need:

- **Computer virus:** Stealthy software code designed to self-replicate and carry a payload. Might also be polymorphic.
- **Stealth, stealthy:** Conscious effort to hide oneself from detection.
- **Self-replication:** Capability to make copies of itself and infect other files or systems.
- **Payload:** Code that makes the virus do something. Can be as simple as displaying a message or as bad as formatting your hard drive (if you aren't protected).
- **Polymorphic:** Capability of a virus to change itself as it infects different files or systems. Helps the virus remain stealthy.
- **Infection:** When a virus becomes active on a system or attached to a file.

- **Trojan horse:** Software that carries with it code that is not acknowledged or not for the stated purpose. Often used to break into systems for the first time or to install software a user would not typically install knowingly.
- **Worm:** Software code designed to spread autonomously from system to system, usually without any user interaction.
- **Clean system:** Has no virus infection in its files or memory.
- **"In the wild":** Describes a virus that has been reported as being on real systems in use at home or at a business.

As you can see, the model used for computer viruses is the same as that used for live viruses that infect people (such as a cold or the flu). The two viruses have many similarities. Both are able to self-replicate and might carry a damaging payload. Both might also change over time to avoid "dying off." If you think about your computer as you would think about moving around in a crowded area during flu season, you can begin to get the idea of the threat you might face. Not everyone gets sick during flu season; however, as more people get sick, more people are exposed, and the cycle gets bigger. After enough people get sick, they begin to get treatment, and the flu begins to go away. That's true of computer viruses too. A few folks hit by a virus might not even know or care. If they don't expose anyone else, no one will probably know. However, if those infected computers share data or connect to other systems, they can pass the infection to other systems. If this occurs, the antivirus experts hear about it. They work up a "cure" for the virus, and it can be contained.

Computer viruses are different from live ones in one way: computer viruses usually need the person who is being infected to do something before the virus can succeed. This might simply be reading or opening a file that has been infected, or it might be visiting a particular Web site. If you have a clean system and you never open infected files or visit untrustworthy sites, your chances of infection are reduced. However, I'll show you later why your safety is still not guaranteed. First, take a look at the types of infections that can occur:

- **Master boot record (MBR):** Virus designed to infect the Master Boot Record or Boot Sector of a disk so that when the disk is used, the virus is loaded into memory.

- **File infector:** Virus designed to infect a file. The virus is loaded when the file is opened or run.
- **Macro virus:** Virus written in macro coding languages and dependent on a particular program or operating system to operate. Most common example is Microsoft Word macro viruses.
- **E-mail virus/worm:** Usually a special variety of macro virus that scripts activities in e-mail programs. One of the most publicized was the "I Love You" virus in 2001 or the more recent Code Red and Nimda viruses.

Nimda, Code Red, and I Love You

In the time that I was working on this book, three e-mail worms caused large disruptions in the e-mail system of the Internet. The three used slightly different approaches but were very effective at spreading quickly and essentially taking down e-mail systems and severely impacting the Internet. I'll describe them here to illustrate how viruses work. First to surface was the "I Love You" or LoveLetter worm, which has been modified and recirculated several times since its original launch. It goes by many names now, but the gist was that it mailed you a message that said "I Love You" or contained a file called resume.txt.vbs. If you ran the file, it downloaded a second file that was a Trojan horse and then mailed itself to people in your address book. It might show you a bogus resume, too. You can find more details at vil.nai.com/vil/content/v_98617.htm.

Next came Code Red, a worm that exploited a hole in the Internet Information Server (IIS) to spread and move about the network. What's worse, the hole that allowed the virus was patched months before the worm, and published best practices also would have prevented the worm from succeeding. But the worm found unprotected systems and managed to slow or stop e-mail communications in many companies. Details can be found at www.symantec.com/avcenter/venc/data/codered.worm.html.

The third one was Nimda. This worm contains some attempts to exploit systems that were victims of a previous worm (Code Red II) as well as a few different infection vectors. This one shut down e-mail systems and networks for a few days while the impacts were being understood and repaired, but it appears to be under control at the time of this writing. Details on this virus are at www.sophos.com/virusinfo/analyses/w32nimdaa.html.

In-depth discussions of how viruses work and how they can hide but still function are outside the scope of this book, but I do want to make some points about these programs. Because writing computer code is a logical operation, computer viruses act predictably. Clever use of stealth or polymorphism can delay or obscure the activities of the virus, but ultimately the virus has to act in certain ways because of how computers work. Having antivirus software and setting proper security in your e-mail software and Web browser can go a long way toward reducing your risk of virus infection. Additionally, you can avoid headaches by making sure you know who sent files to you before you open them. To be most safe, you should know the senders well enough to know that they are using virus protection.

Why Should I Care?

The first virus ever written was an accident, sort of. The story goes that the software writer was trying to make a piece of software (later dubbed the Morris Internet worm) that was a "message in a bottle." It would replicate until it got to the target system and then would pop up a message. Unfortunately, because of bugs in the code and changing disk-format standards, this "message" could end up scrambling data on floppy disks. That wasn't the intention at all; it just worked out that way. The Morris Internet worm of those early Internet days was designed to be a self-replicating piece of software, but was supposed to replicate very slowly. Instead, a coding error or bug caused it to replicate very quickly, and it consumed system resources and literally brought the Internet to its knees.

How does all this affect you? First, the world of computer viruses is complex. People make and distribute viruses for a wide variety of reasons, from simple experimentation to clandestine international espionage. At the time of this writing, well over 48,000 viruses are known. Many of these viruses are harmless and easily controllable; some are not. The biggest problem is that these viruses are not very discerning—they attack anyone they can. If you do not protect yourself, you are eventually going to fall victim to one or more of them. Quite a few "virus creation kits" exist now for viruses and macro

viruses. Even novice programmers can easily create viruses these days, unlike in the past when programmers needed reasonably advanced programming knowledge to write a "decent" virus. One thing should be painfully clear: what you don't know about viruses can hurt you.

The good news is that you can get a large amount of protection by taking two steps and performing one ongoing task. Regularly back up your data. Install a virus-protection package. Then, regularly manually update the software or set it to get updates automatically. With these steps, you can cover your bases extremely well for relatively little cost and effort.

Appendix A "Additional Resources" includes links to antivirus (AV) programs and resources, or you can get AV software from your local computer software dealer. Most reputable AV software is easy to use, takes up little memory, and has options for updating automatically if you are connected full-time or have a dial-on-demand connection. I'll say it again: Regular backups should always be part of your safe computing routine. Viruses are just one more reason to do it.

> ***NOTE:*** *If you find you have a virus and you restore from a backup tape or CD, always rescan your system with a virus scanner after restoring it. The virus might have been on the system when you made that backup, and you could put the virus back on your system by restoring. If that happens, simply use the AV software to clean your system after restoring and then make a full backup immediately. This should ensure that you have at least one full clean backup. Another good idea is to run a full virus scan before creating a full backup, just to be sure you're clean.*

Defending Against Threats

Although the threat of viruses and Trojans is constantly changing, protecting against them is relatively easy. The first and best defense is antivirus software, which I'll talk about momentarily. If you're already armed with AV software, here are a few tricks that will help reduce your risk of exposure.

- Do not open files or run software from unknown sources. Even e-mail from known sources can contain Trojans or viruses, so encourage your friends and family to get antivirus protection too.
- Read e-mail in plain text only. HTML allows scripting that can be used to gather data about your system or put Trojan code on your system. To set this in Outlook, choose Options from the Tools menu. Then select the Mail Format tab shown in Figure 9-1. You can select plain text or Rich Text format safely; just don't use HTML format.
- Download software only from reputable sources. Software from unknown sources can easily be altered with Trojan-horse code.
- Upgrade to the newest versions of your browser and Office Suite software, and turn on macro protection if your software supports this option (see Figure 9-2).
- Turn off Windows Scripting Host if you do not need it. You can learn how by going to www.sophos.com/support/faqs/wsh.html. Windows Scripting Host is a program that lets you run scripts

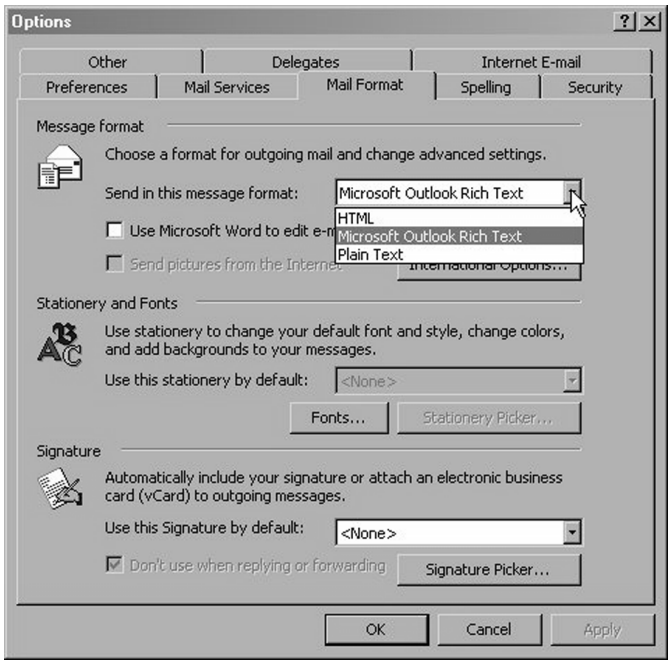


Figure 9-1 Changing the mail format

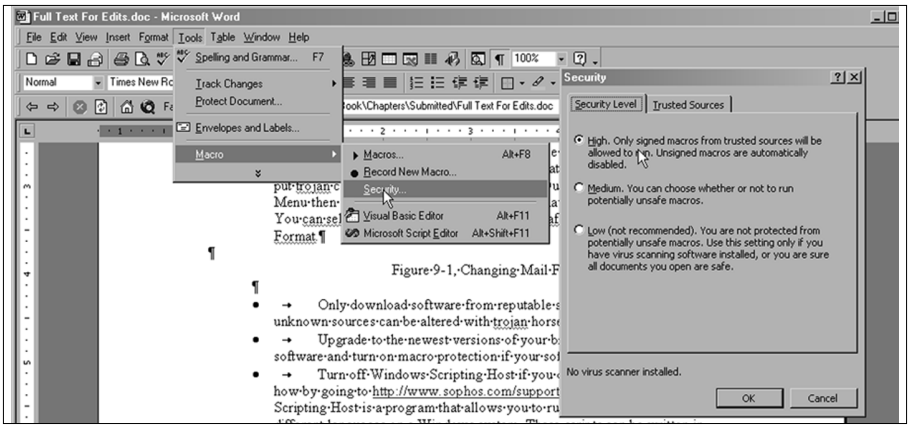


Figure 9-2 Turning on Macro Security in Microsoft Word 2000

written in several different languages on a Windows system. These scripts can be written in VBScript, JavaScript, or PERL, among others.

- Always write-protect floppy disks (if you still use them) before taking them to other machines for use.
- Make regular backups of data. If possible, use CDs for your backups or write-protect your tapes or disks after creating the backup to prevent infection later.
- Make a clean system boot disk with a copy of your AV software on it (if you can), so you have a way to get a clean startup for cleaning, if needed. Put this disk in a safe place and update it when you upgrade your operating system.

Using these techniques can reduce your exposure and help protect you, but there is no real substitute for a good antivirus software package. Because AV software is one of the most critical elements of a home security plan, I'll spend some time now discussing what to expect and how to use it. I'll also list some resources (which are repeated in Appendix A) for getting information, software, and updates.

Antivirus Software

What exactly is an AV software package? There are many forms of AV protection, and many software vendors are trying to cover all the bases

by providing packages of tools for preventing, detecting, and cleaning viruses and Trojans, as well as ways to keep their tools updated with the latest information. Each tool in the package often has one or more purposes, but we can look at the tasks individually. Some software vendors package their tools as one program; others provide many smaller programs. Whether everything is in the same program is usually not important. Let's look at the tasks that one of these packages typically accomplishes:

- **Virus detection:** The heart of all AV packages. After all, what good is antivirus software if it can't detect viruses? This software gets loaded into memory at the time the system boots. To do this, you use Terminate and Stay Resident (TSR) techniques, System Services, System Extensions, or other means available to the operating system you are using. The software inspects your hard drive for files that might be infected, giving warnings and reports or cleaning up the files as it goes. The drives, directories, and types of files inspected are usually configurable but should always include (for Windows-based systems) EXE, COM, BAT, and (if you're using Windows NT) CMD. Several other factors might also be configurable, depending on the software. You should scan your system at least once a week or have the software do this automatically if it can.
- **Virus cleaning:** This program tries to clean up the virus from your system. Though normally safe, this process might render a file unusable if the virus was particularly destructive. It is best to rely on prevention rather than cleaning as much as possible.
- **Trojan-horse detection:** Similar to virus detectors, but this one detects Trojan-horse software. These functions are usually added after a particular type of Trojan-horse software is detected.
- **Virus definition updates:** Obtains the latest information files (definition files) about viruses and Trojan horses from the AV software vendor. The software uses these files to determine if viruses or Trojans are present in memory, in files, or in e-mail and attachments.

How you use your AV software depends somewhat on your particular vendor, but here are some rules that will help it run smoothly. First,

buy your software from a company that will be able to supply you with long-term support and protection. You might save a dollar or two by buying from a small company, but if they go out of business, you'll lose support. Second, set the software to automatically scan your system and get the virus definitions, if possible. This saves you the trouble of doing it and keeps your system up-to-date. If you set this to occur at night or during off hours, the system will take care of this for you and your performance won't suffer a hit at all. If you try to work during a scan, you will sometimes see a slowdown. Do not alter the settings for what the AV software does or how it does them unless you know what the results will be. Accidentally disabling the software but thinking it is running is worse than having none.

Here are some links to antivirus-related information. All of these links are repeated in Appendix A.

Resources for Virus utility software:

VirusScan: www.mcafee-at-home.com/products/anti-virus.asp?m=1

Symantec Security Response, home of Norton AntiVirus: www.symantec.com/avcenter

PC-cillin 2000: www.antivirus.com/pc-cillin/products/

Sophos Anti-Virus: www.sophos.com

Norman Virus Control: www.norman.com

F-Prot Professional Anti-Virus Toolkit: www.datafellows.com

Integrity Master: www.stiller.com/stiller.htm

Simtel.Net MSDOS Anti-Virus Archives: http://www.simtel.net/pub/msdos/virus/

Simtel.Net Windows 3.x Anti-Virus Archives: oak.oakland.edu/simtel.net/win3/virus.html

Grisoft's antivirus offering: www.grisoft.com/html/us_index.cfm

Links to more information about viruses:

"Viruses in Chicago: The Threat to Windows 95"[1] (Ian Whalley, editor of "Virus Bulletin"): www.virusbtn.com/VBPapers/Ivpc96/

Computer Virus Help Desk: iw1.indyweb.net/~cvhd/

[1] Windows 95 code was named Chicago during its development.

"eicar" (European Institute for Computer Antivirus Research): www.eicar.org

"Future Trends in Virus Writing" (Vesselin Bontchev, Research Associate, University of Hamburg): www.virusbtn.com/OtherPapers/Trends/

McAfee Virus Information Library: vil.mcafee.com/default.asp?/

Symantec Virus Search Page: www.symantec.com/avcenter/vinfodb.html

Hoaxes and Why They're a Problem

Strange as it might sound, this final threat that you should be aware of is not even a real threat—it's a hoax. A common example is an e-mail message describing the threat of a virus and instructing you to "inform everyone you know about this threat." Unless this warning comes from an AV vendor or reputable security resource, it is likely a hoax. Before spreading any e-mail about a "virus," always check your AV vendor site for news about it. If you don't see the virus described on their site, do not mail warnings to your friends and family. Why people start these hoaxes is not clear, but usually they can be traced to one of two things. Perhaps the perpetrator wants to focus so much attention on the hoax that it makes the news, and they'll get some satisfaction out of knowing they caused it. Or the perpetrator might genuinely want to cause a

Crying Wolf or Real Threat?

Remember the story of the boy who cried wolf? If enough hoaxes are perpetrated in a short enough period of time, some people will assume that the next one is a hoax. If, instead, it's a real virus, some people will not be prepared, and the virus will be launched into the wild. This complex bit of social engineering can be highly successful. If you hear about a "new virus threat" from a coworker, family member, or friend, please do not immediately forward the message to your entire mailing list. Check your AV vendor or security mailing list for confirmation first.

Denial of Service (DoS) attack on the e-mail systems of one or more areas. By causing a flood of warning e-mails, such a person can enlist the general public as tools in crashing or seriously delaying e-mail systems. Note, too, that sometimes a virus warning claiming to have the "fix" for some security issue is actually a Trojan horse itself. When you run the file, it infects your system.

Active Content on the Web

Active content on the Web simply means using scripting and programming languages to provide dynamic and interactive Web pages. (That sounds like a marketing brochure.) I guess the easiest way to describe this is to say that most content on the Web is static, but it can be specifically built to perform tasks, collect data, or display dynamically. Some of this can be done by using animated graphics or HTML tags (the language for programming Web pages). Sometimes a more advanced programming language is used to "instruct" the computer or browser what to do. Most Web programmers are designing active content to provide their users with a better experience on the Web—easier and more enjoyable—but hackers can use the scripting for other reasons. By taking advantage of poorly coded ActiveX controls or using scripting to access files on your local system, hackers can do many things from a Web page. The catch is that if you protect yourself by turning off Active Scripting in your browser, you'll lose out on some of the features programmed into pages to make them easier to use. So what can you do?

Microsoft Internet Explorer includes a feature called security zones that lets you determine the level of access programs can have, based on their "zone." You can set the zone levels or leave them at their defaults. (I talked about the details in Chapter 7). Using these settings can increase your security. Additionally, don't browse the Web while you're logged on as Administrator. If a Web page tries to do something on your system, it does so with the same permissions you have (because your user ID opened the browser) and, therefore, with the same access to files, directories, and user rights. Always use the account with the lowest privileges when you browse the Web.

Active Content is getting safer, but it has a long way to go before it can be considered truly safe. If you browse sites that are not "mainstream" or run by reputable companies, I recommend upping your browser security so you can be as safe as possible.

Virus and Trojan Horse Security Checklist

This chapter's checklist isn't too complex, but here it is:

1. Are you backing up your system regularly?
2. What virus protection package are you running?
3. When did you last update your protection software?
4. Do you get your downloaded software from reputable sources?
5. Do you browse the Internet while logged on as Administrator?
6. Do you use your AV scanner frequently?
7. Do you use floppy disks to share information? If so, are they write-protected as much as possible?
8. Do you have your AV software vendor's Web site bookmarked so you can get updates and news regularly?