3

Bad Things Come in Small Packages

How Viruses Are Transmitted Through Email Attachments

IN THIS CHAPTER

- **The Trusted, the Innocent, and the Seductive**
- **All Dressed Up, with Nowhere to Go**
- **Not What I Say, But What I Do**
- **Beware of Email Bearing Gifts**

After spam, viruses are probably the most discussed email problem. Most people are aware of their existence and hear about the major new strains on the mainstream news. Viruses strike fear into many computer users' hearts, who cringe when they imagine files being deleted or corrupted or their computers being damaged.

Viruses and Trojan horses are also misunderstood. Many computer problems get blamed on viruses, often unjustifiably, and sometimes this misdirected blame does more damage than a virus would have. Because most people don't understand viruses and how they work, even hoaxes about viruses have become attacks and caused problems for many people who were never infected.

This chapter discusses viruses and Trojan horses and explains how they are passed through email messages. You learn the real risks and how to protect against them. Also, you look at hoaxes and misdiagnoses and see how to avoid hurting yourself by falling for them.

The Trusted, the Innocent, and the Seductive

Viruses are malicious code that attaches itself to files sent through email as attachments. Although viruses are shrouded in mystery and often attributed almost supernatural powers, they are simply a special type of program. My six-year-old was acting goofy yesterday, and my wife asked him why he wasn't listening. He told her he thought he had a computer virus from opening an attachment. I've been probably talking about the book too much, but many people, like Michael, believe that viruses can do things that are beyond their grasp. Like all programs, they must be run to do any work or, in the case of viruses, any damage. This section shows how email attackers convince you to open virus-infected files and allow the malicious code to run on your computer. By falling for their trap, your term paper, presentation for a big meeting, or the photos from your last vacation can be damaged or even lost forever.

Case Study 3-1

Tina opened her email program to find an email from her sister in Georgia. She clicked on the email and read a short note from her sister:

> Subject: Brighten up your day
>
> You've got to take a look at this program. It's hilarious. Let me know what you think.

Tina opened the attachment, a file called `funstuff.exe`. When she ran it, nothing seemed to happen. She tried again with the same result. Finally, Tina sent an email to her sister, saying that she couldn't open the attachment. Over the next few days, Tina noticed her computer getting slower and slower. She wondered if she needed to get a new computer. She never realized that the attachment she had opened had infected her computer with a virus that was responsible for the speed issues she was having. Buying a new computer would "fix" the problem, but simply dealing with the virus would have the same effect with a lot less cost and hassle.

Case Study 3-2

Ben came to work on Monday morning and logged in to his computer. As he started working through his email from the weekend, he noticed one from Acme Software, a major software company that Ben's company used.

From: support@acmesoftware.com

Subject: Important Security Patch

Dear Valued Customer,

We have just released an important security patch, which is critical for you to install to prevent hackers from attacking and taking over your computer. To get this information into your hands as quickly as possible, we have attached the security patch to this email.

Simply open the attachment, and the security patch will be installed on your computer immediately. We've tried to make this process as quick and painless as possible.

If you know anyone who uses the fine products from Acme Software but might not have registered the products, please forward this email to them. It is important to us that as many people as possible install this security patch before malicious hackers take advantage of them.

Thanks for your assistance in this matter,

Technical Support

Acme Software

Ben installed the security patch and forwarded the email to some friends who used Acme Software products at their companies.

Two days later, Ben was looking for an important file, but there was something wrong. None of his documents were in the directory where he had saved them. As he looked through all his directories, it appeared that all his documents were missing. He called the company's technical support line to find out what was going on.

They informed him that a virus had deleted most of the documents from their servers. The tech support staff was busy upgrading the virus protection software and restoring files from backup tapes. Ben was upset over the damage the virus had done, but he never considered that the security patch he installed had actually been the cuplrit.

Case Study 3-3

The subject of the email message caught Tom's attention immediately: "View Naked Pictures of Britney Spears!!!" Tom looked over his shoulder to make sure no one was around and clicked on the email.

The email didn't contain any pictures of Britney but described a special viewer that would allow downloading the pictures in a manner that couldn't be detected or tracked. Tom had heard rumors of some people being caught with porn on their computers and figured a secure viewer might just be the key.

Another glance over his shoulder, and Tom began installing the viewer. After all, it was Britney. The viewer didn't seem to work correctly, however, and Tom never saw the promised pictures of Britney. Almost immediately, his computer started acting strangely. Some programs that Tom used started crashing or wouldn't load. Tom realized that he had probably gotten a virus from the viewer, but he was afraid if he asked for help, someone would trace the problem back to the viewer. So Tom just kept silent and hoped it would go away.

How the Attack Works

To understand how these attacks work, first you need to understand what a virus is. A virus is simply a computer program with all the same characteristics of any computer program. A virus is written by a programmer, not some mysterious entity with magical properties.

Sometimes users attribute qualities to viruses that are beyond their capabilities. For example, viruses can't live through a reformatting of your hard disk because, like any other program, they'll be deleted. If a virus was inadvertently copied over to a disk and you insert that disk into your computer, you can reinfect the machine, but the original copy of the virus on your computer would have been destroyed.

Also, viruses have bugs, just like all other programs. Sometimes the damage a virus does is unintentional and is actually the result of a bug in the software. Although the result is the same, these programs aren't necessarily the most sophisticated software out there. Often virus developers are copying someone else's code and making minor modifications to it.

Although a virus is a computer program, a distinct characteristic separates a virus from other programs: its capability to replicate. This trait is what makes a virus a virus. Viruses can spread by copying files onto floppy disks, burning CDs, or passing computer files over the Internet or network. Any

medium that allows computer code to be passed from one computer to another is fair game for a virus to attempt replication.

The issue most people have with viruses is the damage they cause. However, a virus isn't necessarily built to cause damage. Sometimes the damage is deliberate, sometimes it's accidental, as when a bug causes the damage, and sometimes a virus simply replicates without any other behavior. When a virus does cause damage, whether intentionally or not, it has access to all the files and resources that other computer programs have. Usually this access results in a significant loss of data and time.

In email messages, files passed as attachments can be infected with a virus. When a virus infects a file, it modifies the file in a way that's similar to how you might edit a document. The virus changes the original file so that the virus code becomes part of the file. When a user sends the file, the virus is transmitted as well. When the file is opened, the virus code runs and spreads to the new computer.

As you saw in the case studies, the reasons people have for opening attachments can vary. You might trust the people who send you email, but do you trust their ability to keep their computer free and clear of viruses? Tina trusts her sister, of course, but the file her sister sent might be infected without her knowledge.

Several Christmases ago, a frantic relative across the country phoned me. This relative had sent an email to the entire family and then found out later that the attachment contained a virus. By the time I was called, several family members had already opened the email attachment and infected their machines. The day after Christmas included a run to the mall to pick up a popular virus protection package to install on my father-in-law's computer. Trusting a person and trusting the security of his or her computer are often quite different things.

In Ben's case, getting a patch mailed from a company sounds helpful, but no major company would do this. The risk is too high that someone pretending to be the company is sending a malicious patch. Never trust these types of emails. Whether or not they're a virus or other malicious program, rely on established ways of updating your software. Go to the software company's Web site and download your patches there.

Finally, Tom is a difficult situation, in that he's the most likely to run into a virus and the least likely to report it. Reporting a virus might raise some questions that Tom doesn't want to answer, so he's more likely to keep silent about any potential problems, which actually compounds the problem. As time goes on, the chance of Tom infecting other computers increases substantially.

An Ounce of Prevention

The first and most important rule to help in the battle against viruses and Trojan horses is to avoid opening attachments and clicking on links to install software. If you never open attachments or install software from the Internet, you substantially reduce the risk of virus infection. Of course, there will be times you want to see a picture of your new nephew or install a new game, but if you start out with a cautious approach, you'll be burned far less often. If you need to open an attachment, be sure to protect yourself by following the second rule.

The second rule, which goes hand in hand with the first, is to install and run virus protection software. There are a number of options, with Norton and McAffee being two of the more popular packages. No computer should be without virus protection software. The cost of the software and the time to keep it up to date are minor matters compared to the time and money spent on a single virus attack.

Another important step is to make sure you're running the latest patches on your operating system and applications. The security patches that Microsoft, Apple, and Linux vendors make available for their operating systems often fix the problems that viruses exploit in attacks. If you keep up to date on these security patches, the damage a virus causes to your files, if your computer does become infected, might be limited.

Finally, make frequent backups of your system. If a virus does infect your system and succeeds in causing some damage, a backup could be your only resort. A good backup is important for a number of reasons, but protecting against virus damage should be enough by itself.

By taking steps to protect yourself from these attacks, you help not only yourself, but also those around you. Viruses can spread only by infecting one computer and then being transferred to the next. If enough people take steps to protect against viruses, it becomes more difficult for them to spread. Also, by taking the proper measures, your system can inform you of a virus in an email message, which allows you to inform the sender and minimize the damage that's caused.

A Pound of Cure

If you have already been infected with a virus, the first step is to run a virus protection software package. These software packages typically come with a disk or CD that you can boot from to clean up the virus without allowing it to run. You might also need to download the latest signatures to catch the most recent viruses and variants.

Until your virus problem is cleaned up, limit your use of the computer. Especially avoid sending emails with attachments or other risky behavior that could actually enable the spreading of the virus. It's bad enough to have your system infected. When your friends, family, and co-workers become infected, the problem becomes much bigger.

Finally, if you suspect your system has been infected, backing up the system is still a good idea. The backups might contain the virus and should be destroyed after the virus is cleaned up and a new backup has been made. However, if the virus causes some form of data loss, knowing that the data is safe and protected so that you can try again to remove the virus can be reassuring.

Checklist

- ✔ Avoid downloading software, especially from sources you're not familiar with.
- ✔ Avoid opening attachments you aren't expecting, especially from sources you aren't familiar with.
- ✔ Install and run virus protection software.
- ✔ Back up your computer.

All Dressed Up, with Nowhere to Go

Many people access their computers every day, oblivious to the threat of virus infection. As troublesome as that is, it's worse when people are aware of the risk and take action to protect themselves, but leave themselves vulnerable due to simple configuration problems. This section is about using virus protection software and emphasizes that the software is only as effective as you let it be. You can actually do more harm than good by installing virus protection and not configuring it properly. Installing virus protection software can leave you with a sense of security that lowers your guard in dealing with suspicious files. If this is a false sense of security because of a misconfiguration, you might be at more risk than if you hadn't installed virus protection at all.

Case Study 3-4

Greg was stewing again. As usual, Andrew was the source of his frustration. Even though Greg had been working at the company about 6 months longer than Andrew, it seemed as though Andrew got all the breaks. Today the frustration was Andrew's computer.

Andrew had just received a brand-new, blazing fast computer. Greg's computer was fine yesterday, but now it paled in comparison to Andrew's finely tuned machine. Everyone who passed by Greg's cube could tell he was upset. Even if you didn't hear the low murmur of Greg's grumbling, it was hard to miss the force with which Greg was hitting his keyboard.

To add insult to injury, the boss wanted their latest changes to the software compiled by 11:00. Greg was sure that Andrew's computer had already finished, and he was probably off for an early lunch. Greg's eyes fell on the icon for the virus protection software. He quickly clicked on the icon and turned off the virus checks it was conducting. His computer cranked on with the compile, and Greg hoped that shutting off the virus protection would give him enough of a speed boost to catch Andrew. After all, he'd just turn it back on later when the compile was done.

Case Study 3-5

Pam bought her computer about a year ago. Even though she had been nervous about computers, things had gone pretty smoothly for her—that is, until the past month. All of a sudden, she had been having all sorts of strange problems. Programs that used to work perfectly fine would complain about missing or corrupt files.

Finally, Pam decided to take her computer into a local repair shop. Later that afternoon, the repair shop called and informed her that her computer was infected with a virus. She explained to the technician that when she bought the computer, the salesman had specifically sold her a virus protection package to keep this from happening.

The technician explained that although the virus protection software was installed and running, it had never been updated. Now Pam would have to pay the repair shop to fix the problem and determine the extent of the damage.

Case Study 3-6

Joanne was having problems with her mail-order computer system. She couldn't point to any particular cause; it just seemed a lot slower than when she first got it. She called the support line to see whether someone could help her.

After hearing her complaint about the computer's slowness, the technician asked Joanne if she ran any virus protection software. Kathleen said she did not.

The technician told her that it sounded like her computer was infected with a virus. She would need to get her setup CD that came with the computer and reset the computer to its original condition.

The technician walked Joanne through the process. At first, everything seemed fine. Joanne reinstalled her software and started using the computer again. The next day, she realized she had a bigger problem. In her haste to get rid of the virus, she had neglected to back up some important documents. On top of it, the computer still seemed slow. Joanne wondered if maybe her computer was infected with a worm instead of a virus.

How the Attack Works

Even when you have all the tools you need, sometimes you can be your own worst enemy. No tool works effectively if you turn it off or

misconfigure it. To effectively deal with viruses and Trojan horses, you not only need to make sure your system is well protected, but also keep up on maintenance to ensure it stays that way.

First, make sure your virus protection software is installed and running. If you don't have virus protection software installed, please set this book down, go pick up a copy now, and install it. Now that you're back and have virus protection software installed, please make sure it's running. Recently, when I was driving through Pennsylvania, I went through several long tunnels and had to turn on my headlights. As I exited the tunnel, I noticed a sign reminding me to check and see whether my headlights were still on. Some people could benefit from a similar sign popping up periodically to ask whether the virus protection software is still running.

Many people install the software and leave it running, but people might turn off their virus protection for various reasons. During software installation, many products recommend disabling virus protection software. A call to a technical support technician might result in temporarily shutting down virus protection to diagnose a problem. As with Greg, this temporary shutdown might be done to get a little more performance out of the machine. Whatever the reason, turning off virus protection can expose a dangerous vulnerability; however, this vulnerability is simple to fix if it's caught before it can be exploited.

An even more common occurrence is to install virus protection software and have it running, but not keep it up to date. Many people are used to upgrading software annually. However, the idea of updating software weekly or monthly often seems foreign. Although most virus protection software can be configured to update automatically, when users don't realize automatic updating is important, it becomes an easily missed step.

When a virus is released, variants—slight variations of the original virus—are usually produced immediately. Often, these variants perform the same actions as the virus; they're just packaged differently. Even if your system is protected against the original virus, if you don't keep the software up to date, the variants can do the same damage.

With huge numbers of viruses and their variants being produced, keeping up with the latest updates to virus protection software is critical. If you keep up with this task regularly, it's easy to do. The longer you go without updating your virus protection, the longer it takes to get the latest information and the higher the risk of your system being compromised.

With all this talk about what viruses can do, there's a people-related risk that can cause more damage than a virus. This risk, which happens in two major forms, is damaging a system to protect against a nonexistent virus.

The first form is a series of hoaxes that have been passed through email for years. A typical hoax email describes a newly discovered virus that's ravaging people's computers and explains how to find out if you have the virus. Usually, you're instructed to look for a file that the virus has stored on your computer and find out, to your horror, that the file does exist on your computer. The email then explains how to remove the virus, which often includes deleting the file in question. The problem is that the file isn't a virus; often it's an operating system file that's needed for the computer to operate properly.

The second form is "computer experts" who are taking the path of least resistance. This is what happened to Joanne. Instead of the technician tracking down the real source of the problem, it was easier to create fear about a mysterious virus that may or may not exist. Reformatting the computer and reinstalling programs from the original CDs will clear up any software problems, whether or not they're virus related. However, this method carries a high potential for data loss, and the resulting damage could be substantially more extensive than what a virus would have caused.

An Ounce of Prevention

For virus protection to do its job and inform you of hostile code, it must be running. Don't turn off or disable your virus protection software unless it's absolutely necessary. Most of the time, virus protection should be left running and checking for hostile code.

The most notable exception is when you're installing new software applications. Many installers recommend turning off virus protection so that it doesn't interfere with the installation process. If you're installing software you've downloaded from the Internet or received from a family member or friend, I strongly recommend scanning it for viruses before installation. Then if you need to disable virus protection during installation, you reduce your risk during that time. The key is to make sure you re-enable the virus protection after the installation is completed. Don't allow yourself to become distracted by other activities, especially checking email or browsing the Internet.

After you have ensured that your virus protection is running and will remain enabled, you need to make sure it's up to date. Updating falls into two distinct areas. First, make sure you're using a current version of the software. This part of the equation is no different from upgrading any other software, such as your word processor or golf game. Keeping your virus protection software upgraded enables you to make use of the latest tools to combat hostile code.

The second area is unique to tools such as virus protection. You need to keep the software itself updated. Virus protection software contains a database of all known virus *signatures*. These signatures are identifiers that the virus protection software uses to compare to the files on your computer to see whether any of them match known viruses. Think of it as a fingerprint search that you might see on *CSI* or other forensic television shows. The virus protection checks to see whether there's a match with the signatures in its database to determine if your computer is infected. When you update your software, you're refreshing that database to ensure that you have the latest signatures for catching the newest viruses or variants.

The update process can be completely automated and configured to run behind the scenes and keep signatures updated on a regular basis. By using this process, you can ensure that your virus protection software is up to date without expending a great deal of time or energy making sure it's been done.

Above all, don't use email messages as your knowledge base for dealing with virus attacks. Virus protection companies don't send emails with updates or steps for removing virus-infected files. Go to the virus protection software's Web site and use the resources there. You'll find ample information on how to deal with viruses and virus-related issues and news of many of the virus hoaxes that prevail on the Internet. Going directly to a Web site is a much better technique than following the steps outlined in an email forwarded by a friend or a friend of a friend.

A Pound of Cure

If you have been infected with a virus because of disabled or obsolete virus protection software, follow the same steps for dealing with the problem that you would use if you had no virus protection software at all. The same steps for booting your computer, running the software, and obtaining updates discussed in the previous section still apply.

The important thing is not to overreact and cause new problems when you're already in the middle of one. Rely on the virus protection Web site rather than an email message for information. Follow a methodical process for checking your computer and disks, and you can deal with the issue upfront, remove the virus threat, and move on.

Checklist

- ✔ Avoid turning off your virus protection software.
- ✔ When it's necessary to disable virus protection—for example, when installing software—make sure it's turned back on after the installation.
- ✔ Use the automatic update feature to keep your signatures current.
- ✔ Never rely on email messages as your source of virus news.
- ✔ Gather information before overreacting, even if you think you've already done something wrong.

Not What I Say, But What I Do

Although virus protection is an important and necessary weapon in the arsenal to defend against email attacks, it's easy to become too reliant on it. When a suspicious file doesn't trigger a virus alert, the file doesn't magically become less suspicious. Yet many people trust the file because virus protection found no problem with it. With the number of new viruses and strains being released, you might face a virus at some point that your virus protection software doesn't yet know about. Recognizing the symptoms of viruses and following safe computing practices, regardless of what virus protection indicates, can help reduce your risk of serious infection.

Case Study 3-7

Judy was a technician at a computer store. Her job description basically entailed fixing everything people did to their computers. Just last week, she had removed three Legos and a stick of gum that an ingenious two-year-old had managed to cram inside a floppy disk drive.

Judy looked at the computer in front of her. The sheet on top said that the user was having a hard drive problem. Judy grabbed some disks off the shelf that she used for diagnosing hard disk failures. About 30 minutes later, she had fixed the bad sectors and began running the company diagnostic software on the machine. Basically, this software did a quick check of everything before a machine was sent back to the customer.

Everything came back fine except the printer port. The computer was having problems accessing the printer, but the user hadn't complained about the problem. Strangely, this computer was the third one to exhibit the same problem that week.

How the Attack Works

One drawback to virus protection software is relying too much on the software to tell you when something is wrong. I remember my parents telling me that I should learn to do the math myself rather than rely solely on a calculator. Reliance on antivirus tools is similar because many people forgo common sense if their antivirus tool isn't warning them of any problem.

Just because antivirus alarms aren't going off doesn't necessarily mean that a virus has been eliminated as the culprit of a problem. Antivirus tools are always a step behind virus creators because they rely on producing signatures to find the virus and users updating their system with the latest signatures. Instead of relying solely on virus protection tools, using them along with sound methods for dealing with files is a much better approach.

At one of my first computer jobs, we had a problem very similar to what Judy noticed. We ended up getting a floppy disk infected with a virus that wasn't yet known to any antivirus tools. This particular virus was a boot sector virus, which means the virus loads itself into the area of the disk that's read whenever a disk is inserted into the computer. When the infected disk is inserted into a computer, it immediately infects the system. If a floppy disk is inserted into an infected computer, the floppy disk becomes infected.

Although we routinely ran virus protection software, because the software hadn't detected a problem, we sometimes ran things a little more loosely than we should have. For example, some diagnostic disks weren't write-protected. We had scanned the computer for viruses first, so it didn't seem as important to write-protect the disks that were put in later.

As soon as a computer was infected with the virus, one symptom was that the printer port became disabled. At first, it just seemed odd that several users' printer ports had stopped working. At that point, I don't think I'd ever seen a printer port fail, and yet in three weeks, I had seen several. Then I had a breakthrough.

Unfortunately, as with many breakthroughs, things got worse before they got better. I ended up inserting one of the infected disks into the computer I used to print the report on what had been fixed. Suddenly, I couldn't print my reports. It wasn't exactly a "Eureka!" moment, but it had the same impact. I realized that something was going on that had nothing to do with a few broken printer ports.

We ended up booting off a clean, write-protected bootup disk. When we did this, the printer started working again. When we booted up from the hard disk, the printer port wasn't functional. With this simple test, we ended up confirming that a virus was at work and provided a useable, although temporary, workaround. Within a few weeks, the virus had been identified and included in the virus protection software, and we were able to expunge this annoyance from the company's systems.

Luckily for my company, this problem happened more than 10 years ago, and our customers were loyal. In today's environment, our company would probably have been sued over infecting our customers' computers and not having the proper processes to prevent it. Protection against viruses is important for everyone, whether in a home or corporate environment. However, when you're in a position of trust, the responsibility that goes with that position means you must consider the security of the computers in your care.

An Ounce of Prevention

The important lesson here is not to rely too much on tools, but to make sure you use common sense as well. If it looks like a duck, walks like a duck, and quacks like a duck, don't believe it's a cow just because a tool says it is. You don't want to fall into a virus-behind-every-bush mentality, but if everything is screaming "virus," act as though your system is infected until you learn otherwise. In this case, assuming "guilty until proven innocent" could keep you from spreading a virus any further. If it turns out the problem isn't virus related, you're none the worse for wear.

At the same time, make sure your virus protection is up to date and running. You don't want to run the risk of your antivirus tool telling you there's no virus simply because you haven't updated its information. By keeping antivirus protection up to date, you'll be able to confirm whether you have a problem if the software detects that you're infected with a new virus or variant.

A Pound of Cure

If you have been infected with a virus that's not being detected with the latest updates, don't be afraid to bring in some outside help. For a company computer, you might have resources who have more extensive experience in dealing with computer viruses. For a home PC, see whether a local repair shop has a technician who has gone through this before and can provide assistance.

Avoid taking any drastic measures unless you have determined that the problem is definitely virus related. Reformatting your computer and starting over will remove a virus from your system. However, if it has infected your disks or backups, when you reinstall your software and data, you'll be right back where you started. If you don't have good backups, you run the risk of losing your data and having to reinstall and configure all your software. That outcome is probably as bad as the damage a virus could have caused.

Finally, if it seems you have been infected with a new virus or a new variant, contact the company that makes your virus protection software. User reports are a major way that companies find out about new variants, when they're first reported as being "in the wild." These companies might be able to help you determine whether this virus is something new or one they're currently building a signature for.

Checklist

- ✔ Don't rely solely on automated tools. Common sense is an effective tool, if you use it.
- ✔ Keeping up to date with virus protection is still important.
- ✔ Avoid taking drastic steps such as reformatting unless the problem is definitely virus related.
- ✔ Use outside help, such as a computer technician, to make sure the problem isn't a simple hardware or software failure.
- ✔ If it seems you have a virus that your virus protection doesn't detect, contact the company that makes your virus protection software. You might have a new virus or a new variant.

Beware of Email Bearing Gifts

Much of the focus on malicious code is on viruses and worms, but another type of malicious code can take over your computer—*Trojan horses*. Just like the story from the *Iliad*, a Trojan horse appears to be one thing on the outside, but contains a destructive force inside. In computer terms, a Trojan horse is a program that masquerades as a game or tool, but includes malicious code that can perform many of the same attacks as a virus payload. This section discusses Trojan horses and what steps you can take to avoid becoming their next victim.

Case Study 3-8

Angie logged on to her computer to be faced with a laser-wielding three-headed alien. "David and Alex!" she called out at the top of her lungs. No matter how many times she told them that her computer was for work, her two sons always managed to get access to her computer to play games.

Angie logged in to the network at work and checked her email. "This telecommuting thing is pretty good," she thought as she sipped a cup of coffee. About an hour into the work day, her connection to the network dropped. She tried several times to get connected, with no luck.

Angie called the network support team. They asked her to bring her computer in so that they could check it out. Angie needed to stop by the office that afternoon, so she took the computer in then. Before she left work to pick up her computer, her boss called her into his office.

The company had a strict policy against using corporate computers for personal use. The game the boys had installed had actually been a Trojan horse. When Angie had logged in to the corporate network, the Trojan horse had gained access to the company's internal network. Angie realized that her ability to keep telecommuting was probably in jeopardy.

Case Study 3-9

Ted had received a little cartoon movie in a email from a friend. The movie required installing a small video player software application, which Ted was able to do quickly. The cartoon was funny, so Ted forwarded the email on to some friends.

A few weeks later, Ted received an official-looking envelope in the mail. It was a notice from his cable company that his cable modem was being taken away. Ted called the number at the bottom of the letter to find out what was happening.

The lady who answered informed Ted that the cable company had received numerous complaints from major Web sites around the country about his computer launching attacks against their sites. Ted tried to explain that he hadn't hacked anyone, but the cable company had lots of proof that he or someone with access to his computer was doing just that.

How the Attack Works

You've most likely heard the phrase "If it's too good to be true, it probably is." This certainly applies to the category of programs known as Trojan horses. Of the many resources available on the Internet, software is a key component. Whether it's commercial software, try-before-you-buy deals, shareware, or freeware, being able to download software and have it available immediately is a major draw for a lot of people.

There are Web sites listing thousands of programs available for download that range from games to productivity software to utilities. If you can imagine it, chances are good there's a piece of software out there that does it. Having this huge repository of software is invaluable when you need that one special tool at 3:00 a.m.

However, with all this opportunity comes a great deal of risk. Besides the issue of checking software you download for viruses, there's the added concern of a hidden agenda. Trojan horses aren't viruses, in that they don't replicate themselves. The only way they can move from machine to machine is if someone copies them. To get people to copy the software to their computer, Trojan horses offer two faces: one useful and one malicious.

The first face is a useful software package that people would want to use. It might be a game, a utility, or other software tool that people might download and install. The user downloads the software and installs it. Like any legitimate software, the Trojan horse executes the program and runs the game or utility as the user intended.

The malicious part of a Trojan horse is what happens behind the scene with the software package's second face. A Trojan horse's hidden side takes some other action, such as exposing your system to hackers, deleting files, or intercepting passwords. Although the program that was downloaded and installed seems useful, this hidden agenda can be devastating.

In Angie's case, a Trojan horse contained in a game her boys downloaded from the Internet was able to wreak havoc on the corporate network. Although this Trojan horse probably wasn't designed specifically for Angie's company, some Trojan horse programs are designed to look for certain types of files or data within files. A common technique of Trojan horses is simply to allow a hacker future access. For example, in Angie's case, either the Trojan horse would connect to the attacker to let him know the site had been compromised, or the attacker would just scan blocks of computers looking for ones that had his Trojan horse program running.

This technique of scanning blocks of computers is known as *port scanning*. Many of the hits on a firewall are this type of attack, which is similar to walking down a street and trying all the doors on all homes to see whether any are unlocked. If one is, that home is added to a list to come back and enter later. An attacker tries to connect to his program on a large number of computers. Any computer that responds is added to a list of systems that give the attacker easy access whenever he chooses.

Many people's first response to the possibility of being hacked is that they don't have any sensitive information a hacker would want, so they don't consider themselves a target. What many people don't realize is that the information on their computers might not be the target at all. The growing trend is for attackers to gain access to large blocks of computers for launching future attacks. A Trojan horse gives an attacker control over your home PC as well as thousands of other PCs. When he wants to launch an attack or send spam, instead of using his own servers and risking detection or being blocked, he uses this block of PCs to do the dirty work. If he's detected, it is the owners of these PCs who will be blamed. If an ISP blocks traffic from the attacker, it is these PCs that will be blocked, not the actual attacker's computer. These blocks of PCs have been used to launch many denial-of-service attacks against large Web sites over the past few years.

An Ounce of Prevention

The first way to prevent Trojan horses from taking control of your computer is to avoid downloading and installing software. A lot of good software is available on the Internet, and you might want to avail yourself of this resource, but by using caution first, you'll limit your exposure.

Also, the other rules for preventing virus infection apply here as well. Most virus protection tools detect common Trojan horses, and a good backup can be helpful if the Trojan horse performs malicious actions on your file system. If you follow these basic rules, many of the problems that Trojan horses cause can be limited or eliminated.

Another step that works particularly well for Trojan horses is installing a *firewall*, which is typically a small piece of software that restricts access to your computer. This is a good piece of software for all computers that connect to the Internet, but especially for those that use a broadband connection. With dial-up connections, you might get a new IP address every time you call in. With broadband connections, you might get a permanent address or at least keep your temporary address for long periods.

A firewall is the first step toward keeping hackers out of your computer and network. They also are helpful in preventing Trojan horses from establishing themselves on your computer. If you restrict access to the few services you use, such as Web access and email, a program that starts opening new connections to the Internet will be blocked. You can use firewalls not only to protect you, but also to act as a warning system that a Trojan horse might be at work (see Figure 3.1).

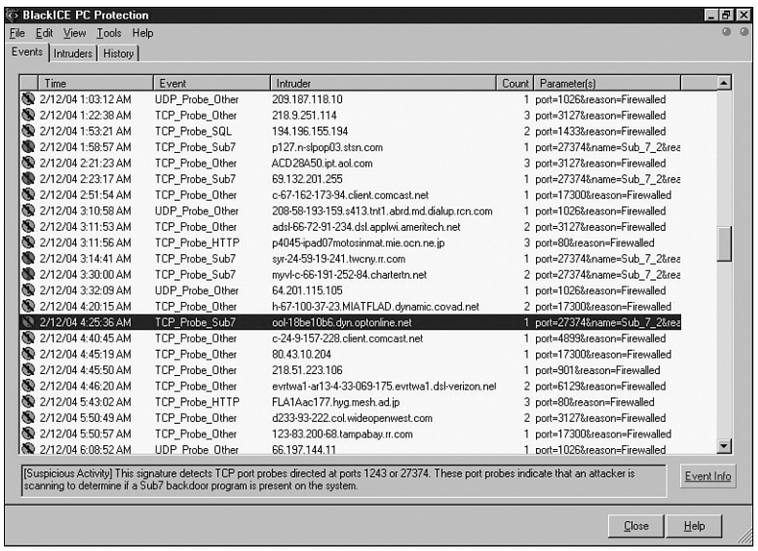

Figure 3.1 *Firewall log showing Trojan horse attack.*

You can also install a *hardware firewall*, which is a computer with the sole purpose of protecting your network. The operating system hardware firewalls run and the software installed on them are all configured for the

purpose of blocking unwanted traffic from entering your network. Some devices for granting wireless or broadband access can also double as a hardware firewall. Whether you choose a hardware or software solution, the important thing is to protect your network from outside attack and from being used as a launch platform for attacking others.

A Pound of Cure

If you believe you already have a Trojan horse installed, the same steps mentioned previously for prevention can help you fix the problem. Even if an attacker has already gained access to your computer, adding a firewall can block any further communication. Also, if your virus protection software detects a well-known Trojan horse, it can assist in removing the offending program from the computer to prevent further use by attackers.

Again, don't be afraid to use outside help if you believe your system has been compromised. This is a serious issue that needs to be resolved as soon as possible. By dealing with it quickly and correctly, you can limit your exposure and minimize the damage.

Checklist

- ✔ Avoid downloading software from unknown sources.
- ✔ Install virus protection because most virus protection packages can detect common Trojan horses.
- ✔ Install and configure a firewall.
- ✔ Bring in outside help if needed. Trojan horses are a problem you don't want to mess around with.

Summary

After spam, viruses are probably the most discussed email problem, and the thought of files being corrupted or deleted or computers being damaged is a frightening prospect for many computer users.

Many computer problems mistakenly get blamed on viruses, and sometimes this misdirected blame does more damage than a virus would have. Even hoaxes about viruses have become attacks and caused computer problems for many people.

Virus-infected attachments are opened for a variety of reasons, such as trusting the source, believing the source would be innocent, or being seduced by what you think the attachment contains. Therefore, keeping

your virus protection running and up to date is essential. If you disable your virus protection software or fail to keep it up to date, you're not allowing the tool to do its work.

On the other hand, you can become so reliant on virus protection that you fail to recognize clear virus symptoms. In addition, viruses often get blamed for problems that are just common computer glitches. When you fall for a hoax or find a virus behind every bush, you can do more damage than most viruses can.

Trojan horses hide behind the promise of a software tool and do their damage behind the scenes. The damage caused by this malicious software can affect your own computer and be used to launch other attacks.

This chapter should have convinced you to install virus protection software and keep it up to date. You should also be cautious about opening attachments or downloading software, whether through email or directly from the Internet. These steps can help a great deal in protecting you from this type of attack.