realtimepublishers.com®

The Administrator Shortcut Guide™ To

Email Protection

Sybari
Software, Inc.

Paul Robichaux

Introduction

By Sean Daily, Series Editor

Welcome to *The Administrator Shortcut Guide to Email Protection*!

The book you are about to read represents an entirely new modality of book publishing and a major first in the publishing industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical IT topics—at no cost to the reader. Although this may sound like a somewhat impossible feat to achieve, it is made possible through the vision and generosity of corporate sponsors such as Sybari, who agree to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these books does not in any way diminish their quality. Without reservation, I can tell you that this book is the equivalent of any similar printed book you might find at your local bookstore (with the notable exception that it won't cost you $30 to $80). In addition to the free nature of the books, this publishing model provides other significant benefits. For example, the electronic nature of this eBook makes events such as chapter updates and additions, or the release of a new edition of the book possible to achieve in a far shorter timeframe than is possible with printed books. Because we publish our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that although it is true that the sponsor's Web site is the exclusive online location of the book, this book is by no means a paid advertisement. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100% editorial control over the content of our titles. However, by hosting this information, Sybari has set itself apart from its competitors by providing real value to its customers and transforming its site into a true technical resource library—not just a place to learn about its company and products. It is my opinion that this system of content delivery is not only of immeasurable value to readers, but represents the future of book publishing.

As series editor, it is my raison d'être to locate and work only with the industry's leading authors and editors, and publish books that help IT personnel, IT managers, and users to do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at www.realtimepublishers.com, or calling us at (707) 539-5280.

Thanks for reading, and enjoy!

Sean Daily

Series Editor

Copyright Statement

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 1: Email Content Dangers

On March 26, 1999, email administrators were awakened to a new threat to their systems. A macro virus called Melissa was spreading rapidly through their email servers, clogging queues and eating up network bandwidth. By March 29, Melissa had reached more than 100,000 computers. Macro viruses were nothing new by this time, yet this one was different. Melissa was the first major virus to use the Exchange global address list (GAL) and the users' contacts as a mechanism to email itself to others. Though almost any virus can be spread through email if the *dropper* (a program that is infected or spreads the virus) is emailed to another person, this incident was the first time that a virus actually started emailing itself to others.

With an estimated 772 million mailboxes worldwide (Anti-Virus, Anti-Spam, and Content Filtering Market Trends 2003-2007 Report from The Radicati Group), email is an excellent delivery vehicle for computer viruses and malicious content. Knowing how to protect your email systems is critical, and doing so begins with a good understanding of what viruses are, how they're written, how they spread, and how they can be blocked.

Is the Sky Falling?

During the Melissa outbreak, some computer media journalists and industry analysts screamed "The sky is falling! Viruses are the number one threat to computer security! Email servers are going to start crashing worldwide!" There's no doubt that viruses are costly. *Computer Economics* estimated in 2000 that damages relating to virus outbreaks were in excess of US$17 billion (yes billion!) and that the Love Bug virus alone has cost organizations more than $8.75 billion dollars to fight and eradicate. Some experts call these numbers conservative while others dismiss these numbers as wild guesses. Are these claims valid? Tallying the actual cost of an outbreak of any virus is difficult, if not impossible, and an exact cost of any type of virus outbreak is impossible to gauge.

What is fact is that outbreaks of email-based viruses such as the Love Bug, Anna Kournikova, BugBear, and SirCam have caused email systems operated by the United States government, Microsoft, EDS, and others to be shut down, inbound and outbound SMTP to be halted, and IT staff to spend countless hours devoted to clean up. The cost of not having email available is compounded by the fact that for many organizations, the mail system incorporates users' calendars, to-do lists, contacts, faxing functionally, pager gateways, and more. In addition, many email-based viruses not only replicated throughout the internal organization, but also to customers and vendors. In many cases, these viruses have continued to propagate for hours or days after their discovery as a result of email administrators' basic lack of virus knowledge.

Is the sky falling? Not by a long shot. But when the industry analysts, pundits, and media commentators all expound on the topic, even if they don't all agree, it provides evidence that the threat of email-based viruses must be taken seriously. Connecting any email system, especially a system with Microsoft Outlook clients, to the Internet would be foolhardy and irresponsible without a good virus-protection plan in place.

An administrator must be prepared as viruses are taking new forms all the time. "Traditional" viruses spread through floppy disks, then later through email, and now through Web services. "New-fangled" viruses are already finding themselves at home on PDAs, wireless devices, and instant messaging clients. Worms such as Nimda are exhibiting characteristics of both worms and viruses by finding multiple ways to infect a computer, then spreading the infection to other computers. Most Windows and Exchange administrators have only a cursory understanding of viruses, how they spread, and—most important—how to protect their organizations from the differing strains and types of viruses out "in the wild." Fighting viruses is a little like fighting in a darkened room with an opponent who has night vision goggles—you don't know from which direction the next attack will come nor how you will be attacked, you just know that there will be another attack.

Just the Facts, Ma'am

Although there are many unknowns in the world of viruses, there are at least a few knowns. The following list highlights a few of these facts (and commonly held opinions masquerading as facts) about viruses and some recent virus outbreaks—perhaps you can use them to justify the purchase of virus protection for your organization:

- The first IBM PC-compatible virus, Brain emerged in 1986 from Lahore, Pakistan; it was written by two brothers, Basit and Amjad Alvis. This virus was only 3.5KB and infected the boot sectors of 360KB floppies. By comparison, the Slammer worm was smaller than 400 bytes.
- In 1990, it is estimated that there were fewer than 500 DOS/Windows viruses in existence, including exceptionally rare viruses. By 1994, there were more than 5000 viruses, and in mid-2003, Symantec estimates that its antivirus software detects more than 64,000 viruses.
- Antivirus software company Sophos estimated in 2002 that there were more than 70,000 viruses: 26.1 percent were macro viruses, 26.1 percent were Trojan horses, 19.2 percent were executable, and 6.8 percent were script viruses. The remaining 21.8 percent were boot sector, worms, file, UNIX, and Macintosh viruses.
- The Cooperative Association for Internet Data Analysis (CAIDA—http://www.caida.org), who analyzes and develops tools for the Internet infrastructure, estimates that the Code Red worm affected more than 359,000 hosts during the first 14 hours of its spread. At its peak, it was spreading at approximately 2000 hosts each minute. As if that weren't scary enough, CAIDA estimates that the Slammer worm at its peak was scanning 55 million systems *per second*. It is interesting to note that both the Code Red and the SQL Slammer worms exploited well-known vulnerabilities in software for which fixes had been published *months* before the worms were released.
- Sophos estimates that it analyzes about 1200 new viruses each month.
- The 2002 SQL Slammer worm spread worldwide in approximately 10 minutes. In the early stages of infection, it was doubling the number of infected hosts every 8.5 seconds.
- The British version of the magazine *PC Today* distributed a copy of its magazine with a floppy disk to more than 50,000 people. The floppy accidentally contained a copy of the DiskKiller virus.

- Some parent viruses can spawn more than 50 varieties of child viruses that cannot be detected by the same virus signature as their parent. Many virus protection companies consider these children to be a separate virus and, thus, these companies report larger numbers of detected viruses.
- The SANS Institute (http://www.sans.org), one of the world's leaders in security research and education, estimated in late 2001 that more than 86,000 hosts on the Internet had been compromised and had helped spread the Nimda worm. About 43 percent of these hosts were in the United States.
- SecurityPortal.com, a company that tracks piracy and safety news for both individuals and companies, estimate that more than 40 variations of the Love Bug virus existed within a year after it was unleashed on the Internet. Macro viruses, such as the Love Bug, include their source code, so it is easy for a recipient to modify them and release the modified version into the wild.
- The British Broadcasting Corporation (BBC) estimated that the Love Bug virus affected at least 45 million users.
- A San Francisco FBI Computer Intrusion Squad survey summarizes that 273 companies that responded to the survey had *quantifiable* losses in excess of $265 million as a result of computer viruses.
- Market research company The Radicati Group (http://www.radicati.com) estimates that malicious code (viruses, Trojans, and worms) will cost more than $28 billion in 2003. By 2007, that cost will nearly triple to an estimated $75 billion. A 2002 survey by the company found that protecting against viruses was the number one priority of email systems administrators (reducing spam was second).
- Viruslist.com (http://www.viruslist.com) estimated that the undisputed leader in virus threat sources was email with a whopping 96.4 percent of all infections. The Internet accounted for 2.3 percent and portable media accounted for 1.3 percent.

Virus 101

So you know that viruses are a very real threat, but perhaps you don't know an email-based virus from a polymorphic logic bomb. If you don't know how viruses are developed or even how they propagate, don't worry—this section is for you.

What Is a Virus?

Like viruses in carbon-based life forms, a computer virus is capable of replicating itself within the host computer and finding a method to move from one host to another. Viruses reproduce and spread without users' consent, and usually without their knowledge.

Viruses are programs that are usually small and difficult for the layman to detect. When executed or accessed, a virus loads itself into the computer's memory, overwrites another program, attaches itself to another program, or writes itself to the master boot record of the computer. The virus might take other actions that can be malicious, innocent but annoying, or innocent but accidentally destructive.

Viruses differ from worms in an important way: virus infections are persistent because the virus writes itself to permanent storage, like files or documents on disk or messages in an Exchange mailbox database. Worms are transient; if you turn off an infected computer and reboot it, it won't be infected again (as long as you've fixed the security hole that let it become infected in the first place).

In the early days of viruses, viruses were usually written with low-level programming tools such as assembler or C. As a result, viruses could be especially small and efficient, and were able to infect components of the computer that a script could not. Most of the more annoying viruses recently have been written using some variant of a scripting language, such as VBScript or JavaScript, although worms are usually still written in low-level languages. The fact that many viruses are now script-based also means that less-skilled programmers can write viruses.

After the introduction of Microsoft Office 95, macro viruses became increasingly prevalent. These viruses use the built-in Office scripting language (now called Visual Basic for Applications—VBA) to do their dastardly work. The most common macro-type viruses were the Concept family of viruses and Wazzu; both of these viruses were Word macro viruses (they attach themselves as macros to Word documents). On each new computer, these macro viruses copy themselves to the master template, normal.dot. From that point forward, any document created or edited on that computer will contain the macro virus as well.

Usually document content was not altered by macro viruses; these viruses were little more than an annoyance, but oh, what an annoyance! Increased document sizes were occasionally problematic as was document corruption; however, the biggest annoyance (and embarrassment!) was to accidentally send an infected document to a customer or vendor. By the late 1990s, infected Word documents (and data files created by other Microsoft Office suite of applications) were a daily occurrence for IT personnel. I even received a CD-ROM from Microsoft that had documents with the Concept virus. Office 2000 and later versions have some significant protections against macro viruses, which we'll explore in a later chapter.

Virus Types

Viruses are classified in several ways. Many of the "viruses" in the wild today are not truly viruses but worms or Trojans horses; many worms in the wild have characteristics similar to viruses. (The term *in the wild* refers to viruses that are currently spreading to production systems rather than a virus that has only been identified in a lab environment.) This section has some basic definitions for virus types; they are not universally agreed upon by all virus experts, so don't be surprised if you come across different definitions from antivirus software companies:

- *Malware* is a broad term used to describe any type of malicious code. This code could be in the form of a virus, worm, Trojan horse, hostile Java code, hostile Web script, or hostile ActiveX control. Malware may disrupt the computer's operation, replicate itself to other computers, steal information, or initiate a denial-of-service (DoS) attack.
- A *Trojan horse* is not usually a virus but rather a program that appears to do one thing but in reality is doing some nefarious task behind the scenes. The program may claim to be a fun game, and in reality, it is searching your hard drive for important data files and mailing them to an outside person. Users are often tricked into running a Trojan horse. Trojans may be just as destructive as a virus, but they don't have the ability to reproduce themselves. The most common use of Trojans is to allow an attacker remote access or control over your computer.

- A *worm* is a program that usually has its own built-in method of replication. It is not associated with any single host program and actively searches for systems to infect. Nimda and Code Red are examples of worms.
- A *macro virus* is not a standalone program but rather code (usually scripts) embedded in a data file such as a Microsoft Word document or Excel spreadsheet. When the document is opened, the macro is run. Macro viruses are generally easier to write and spread quickly. In 1998, it is estimated that there were about 1000 macro viruses. Today, it is estimated that about 75 percent of all viruses are macro viruses. Well-known macro viruses include the Concept virus and the infamous Melissa virus.
- A *blended threat* is malware that combines characteristics of worms, viruses, and Trojan horses. By using a combination of methods and techniques, this type of malware can spread more quickly. Many of the virus/worms that have caused the most harm in the past few years have been blended threats.
- A *dropper* is a program that is responsible for depositing a virus' malicious code on a target system. The dropper itself may be a virus or it may be a Trojan horse.
- A *stealth virus* is a virus that attempts to conceal itself. Most viruses are stealth to at least some degree. Some viruses will even protect the area of the disk on which the virus is stored.
- A *polymorphic virus* is a virus that goes to great lengths to conceal itself by changing itself every time it replicates. These viruses make it more difficult for antivirus software to detect and remove them.
- *Adware* and *spyware* cannot really be considered viruses, but they are often annoying and can offer potential security risks. Adware is a term used for a program that resides on your computer and sends pop-up advertising to the console; the adware program may also install spyware. Spyware is generic term for software that is designed to sit on your computer and monitor your computer usage. The software then reports that information back to the organization that originally installed the software. Although the violation of privacy is enough to concern most computer users, the potential for even greater harm exists. Any program that runs in the background on your computer has the potential to scan for sensitive information, collect keystrokes, and make modifications to your computer. Spyware-type programs are not currently spread through email; they are downloaded when a user loads something from a Web site. File-sharing giant Kazaa is notorious for placing Spyware that changes default start pages in the Web browser of users' computers and sends pop-up advertising. These programs can also contribute to computer performance problems and can actually break some real software if the Spyware is removed. Spyware that does so is often referred to as *scumware*.
- *Companion viruses* rename an existing executable file to something else, then put themselves into that program's place. When the program is executed, the companion virus first executes, then runs the intended program.
- *Keystroke loggers* are not specifically worms or viruses. A keystroke logger can either be hardware or software. The keystroke logger captures all keystrokes that a user types when using a computer, including anything typed in to a document or spreadsheet as well as usernames and passwords.

The evolution of spyware and adware is just getting rolling. Expect to see this type of threat become more prevalent on both personal home computers as well on the corporate desktop computer. You can find more information about spyware and adware at http://www.adware.info and http://www.cexx.org/adware.htm.

Lavasoft is a small company that provides a tool called Ad-Aware that can detect and remove spyware and adware from your computer. You can find more information at http://www.lavasoft.de.

Virus Names

You might be confused about why you hear viruses, worms, and Trojan horses referred to by different names. For example, the SQL Slammer worm was also known as the W32.SQLExp.Worm, DDOS.SQLP1434.A, W32/SQLSlammer, Sapphire, and W32/SQLSlam-A. Contrary to popular opinion, the virus author often does not name the virus. The reason viruses are often named so differently is that each antivirus software vendor assigns the virus a name. The companies rarely pick a name that has much to do with the name that the virus author might have assigned to the virus; they usually pick a name that will help to identify the virus, the platform it affects, and the type of virus. Therefore, tracking a virus can become confusing if you subscribe to notification lists from more than one vendor. Alternative names for viruses can be found on many antivirus vendors' Web sites.

A good location to cross-reference virus names is the vgrep page at http://www.virusbtn.com/resources/vgrep.

Why Create a Virus?

The question that begs to be answered is why would someone write a virus? Most of the viruses that I have come in to contact with were written by someone with a good degree of programming and computer skills. Why would a skilled programmer waste time writing a virus that inconveniences hundreds or even millions of computer users?

I suspect that most viruses have been nothing more than a challenge for a bored programmer. Virus programmers might want to see whether they can achieve a particular result by writing something a certain way. Or they might want to see how far the virus will spread. The virus writer might want to exploit a weakness in a particular platform or application.

Other virus writers have a more mischievous perspective. They don't want to cause any real harm but see their creations as pranks or practical jokes. The financial costs associated with cleaning up their mess are probably lost on these programmers. (For an example of such a virus artist, see the sidebar "You've Lost that Lovin' Feeling.")

You've Lost that Lovin' Feeling

Onel de Guzman, a 24-year-old college dropout in Manila, "accidentally" unleashed the email-based Love Bug (ILOVEYOU) computer virus on the world and attributed it to "youthful exuberance." Considering that the Love Bug spread worldwide in less than 24 hours and cost an estimated $10 billion to clean up, this virus creator has a gift for understatement. Though he was never prosecuted, those of us who spent many hours cleaning up the aftermath of the Love Bug (saturated WAN links, tens of thousands of queued copies of the message, and so on) while users pounded on the data center doors would like to see him expend some of that youthful exuberance elsewhere.

Some virus programmers have set out to make a political statement; one Microsoft Word macro virus displayed the message "Stop all French nuclear testing in the Pacific!" Virus writing as activism is thankfully rare, although some public pronouncements by the US government indicate that they're worried about the use of targeted malware that attacks critical infrastructure. The recent BugBear worm functioned as a dropper that installed a keystroke logger on target machines, provided that they were on the network at a number of specifically targeted banks.

Fairly few viruses truly cause direct harm to the computers they infect. There are no recorded instances of viruses causing harm directly to the hardware of a computer, though some viruses may be able to damage a computer's CMOS. The real harm associated with viruses is usually indirect. Some of the dangers and direct or indirect costs include:

- Viruses that deposit Trojan horse programs or that install keystroke loggers offer a potentially significant security breach.
- Sophisticated viruses (worms and Trojans included) can leave agents that mine information from infected computers and send that information to someone outside of the organization.
- Computers infected with viruses may operate more slowly as a result of increased memory usage or problems due to a virus being attached to the program or a document.
- Email viruses and worms can cause increased WAN bandwidth usage.
- Viruses can chew up a significant amount of disk space, especially viruses that spread themselves via email.
- Labor costs to clean up a virus outbreak can be significant if there are many servers or desktop computers that must be inspected.
- Loss of user productivity.

A Brief History of Viruses

Computer viruses have been around almost as long as computers themselves, though we did not really call them viruses until the mid-1980s. Viruses have evolved over the years to become more complex and more dangerous. Viruses are becoming more and more difficult to detect and eradicate, the method that viruses (and worms) are using to spread is increasingly more efficient, and the increased dependency on personal computers and corporate desktops are giving complex viruses the ability to potentially compromise security.

Even early IBM 360/370 machines had primitive, self-replicating, self-propagating programs. According to Eugene Kaspersky of antivirus company Kaspersky Labs, in the late 1960s there were programs on mainframes that cloned themselves and occupied system resources. These programs were called ‘the rabbit.’ In 1981, a 9th grader in Pennsylvania named Rich Skrenta wrote a virus called Elk Cloner that infected Apple II floppy disks and displayed a harmless message. There were also viruses that were developed as “proof-of-concept” viruses, including one developed for the UNIX-based VAX machine by Fred Cohen and Len Adleman, who coined the term *computer virus*.

The first IBM PC-compatible virus is generally accepted as being the Brain virus that was allegedly developed by two brothers in Pakistan. This virus, like most of the other viruses in the early days of computer viruses, was a boot-sector infector. It embedded itself in to the master boot record of a floppy disk, then infected any computer that used that disk. This virus even had stealthy characteristics: if a program attempted to read a disk sector of the master boot record in which the virus was located, Brain would move that sector to another place within the master boot record.

Shortly after the Brain virus appeared in 1986, the Virdem virus appeared along with a Trojan horse program masquerading as the PC-Write word processor for DOS. This nasty little Trojan destroyed the disk’s file allocation table and initiated a low-level format.

By 1988, there were more boot-sector infector viruses (including the pervasive Stoned virus that hung around for many years) as well as file infector viruses and Macintosh viruses. November 1, 1988, saw the “accidental” release of the first major Internet worm—the Robert Morris worm. This worm caused many computers on the Internet to be isolated or shut down. Of course, there were relatively few computers (about 60,000) on the Internet.

The year 1991 saw the arrival of the first network aware virus, the GP1 virus, which attempted to steal Novell NetWare passwords. The first polymorphic virus, Tequila, also arrived on the scene in 1991.

In 1992, the Michelangelo virus appeared amidst media hysteria and fears of massive damage. A lot of print was wasted for what amounted to almost nothing. In 1995, the first Microsoft Word *macro virus*, Concept, appeared. The first Microsoft Excel macro virus, called Laroux, was released in 1996.

1996 and 1997 saw the release of the Staog and Linux.Bliss viruses, showing that even the Linux platform was vulnerable. In December of 1997, a new type of worm emerged called an mIRC worm. These worms took advantage of an early version of the Windows Internet Relay Chat (IRC) client.

In 1998, the Strange Brew virus gained the dubious distinction of being the first Java virus. Also released in 1998 was the Back Orifice Trojan, which, if executed, could allow an intruder to take remote control of a computer on which the Back Orifice infector had been run.

March of 1999 saw the first email-based virus; this Word macro virus was called Melissa. It could use either Outlook or Outlook Express to send itself to recipients in the Exchange GAL or the user’s address book. Melissa actually required the user to open the attachment. Bubbleboy, released later that year, executed if someone merely opened a message in Outlook (or even previewed the message in the Outlook Express Preview Pane). Corner, also found in 1999, was the first Microsoft PowerPoint-based virus.

As the 21st century dawned, new types of viruses have been introduced. These include viruses that spread through Adobe PDF files, file-sharing systems, IRC worms, and instant messaging (viruses that send themselves to everyone in a victim's buddy list), and viruses or Trojans that infect PDAs.

In 2001, a whole new breed of virus/worm was introduced, including SirCam, Code Red, and the infamous Nimda. Although Nimda was a worm, there were reported cases in which it was spread through email. Nimda primarily used a vulnerability in the Microsoft Internet Information Server (IIS) 4.0 or 5.0 server to infect an IIS server. Once that server was infected, it would then begin scanning IP ranges looking for other IIS servers to infect. Nimda could also infect Web pages so that if someone opened an infected Web page, the user's computer would become infected and begin attempting to spread the infection. Finally, if Nimda discovered an Outlook or Outlook Express address book, it would attempt to mail itself to others.

📖 An excellent explanation of Nimda can be found at http://www.cknow.com/vtutor/vtnimda.htm.

The year 2002 introduced even more "innovative" approaches to spreading viruses and worms. This generation includes the SQL Slammer worm that used a known vulnerability (and often neglected fix) of Microsoft SQL Server; this worm went worldwide in about 10 minutes. The LFM-926 virus infected Macromedia Shockwave files. The Perrun virus attaches itself to JPG files. New worms, such as Zircon C and I-Worm.Cervinec, that propagate through email were introduced. Figure 1.1 shows a breakdown of the most widespread computer viruses for the year 2002.

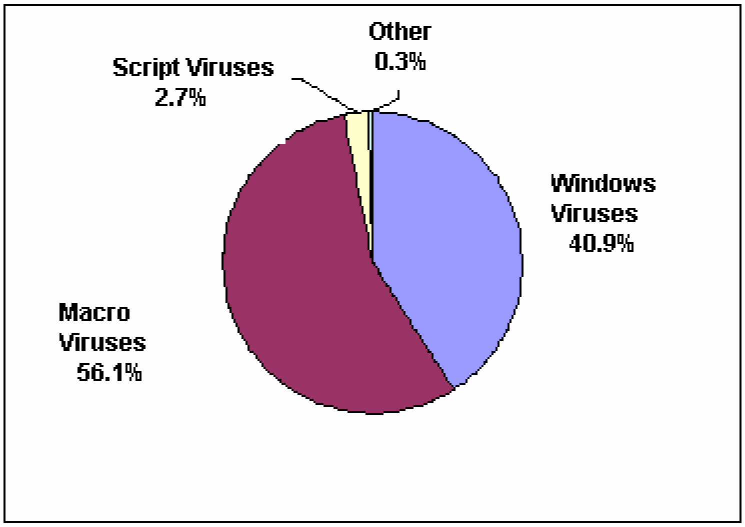

Figure 1.1: The most widespread virus types for 2002 (from http://www.viruslist.com).

What Does the Future Hold?

The folks writing viruses, worms, and Trojans are getting more and more creative. Nimda gave us a great example of just how determined a virus programmer can be to get a virus out in the wild and spreading; Slammer showed just how quickly a well-engineered piece of malware can spread world-wide. Even with warnings in every technology media outlet, email newsletter, and even CNN, email viruses continue to propagate. Users and administrators are becoming more diligent and more restrictions are placed on email content all the time, but the race continues.

Worms will continue to spread as newer and more sophisticated technologies are introduced into the workplace. Almost certainly, viruses and worms that take advantage of wireless networking, PDAs, and cell phones will continue to emerge. The methods that the virus writers use will continue to become more ingenious, creative, and deceptive. Table 1.1 shows a list of the 10 most widespread malware programs of the year 2002 as collected by Viruslist.com. Note that most of these malicious programs were worms.

Rank	Name
1	I-Worm.Klez
2	I-Worm.Lentin
3	I-Worm.Tanatos
4	I-Worm.BadtransII
5	Macro.Word97.Thus
6	I-Worm.Hybris
7	I-Worm.Bridex
8	I-Worm.Magistr
9	Win95.CIH
10	I-Worm.Sircam

Table 1.1: Viruslist.com's 2002 most widespread malware programs.

Are Viruses Dangerous?

Are computer and email viruses truly dangerous? Is the perceived threat much ado about nearly nothing? If you have ever had to remove a virus, you can sympathize with the folks that claim financial loss. Although most do not, there are certain viruses that can (and do!) destroy data on a computer's hard drive. And loss of productivity is difficult to quantify for more organizations. Virus outbreaks can also increase the need for data storage as files get larger or messages get queued for delivery. When these messages begin to be delivered outside your organization, the cost of the bandwidth that will be consumed can inflate the damage. In addition, a virus infection that attacks your organization may be dangerous for other reasons. If an email virus is sent from your company to many of your customers, clients, and vendors, your organization may suffer a significant loss of credibility or public embarrassment.

> ✎ For some organizations, such as law firms, accounting firms, and healthcare organizations, disclosure of confidential information could result in law suits. For an organization such as a government or military, accidental disclosure of information could get someone killed.

Several virus experts have commented over the years that the industry is far more obsessed with viruses and virus protection than they are with topics that present more dangerous and immediate threats to IT operations such as disaster recovery and business continuity. This commentary certainly does not mean that we should ignore the threat of viruses; only that virus protection is one cog in a well-oiled disaster prevention machine. The following list highlights the main potential dangers that can result from viruses:

- Damage to computers' applications or operating systems (OSs)
- Loss of important data
- A carefully crafted and targeted virus could be used to glean information from inside the targeted organization and send the information to an outsider (for example, the recent BugBear virus targeted a number of financial institutions)
- Public embarrassment—imagine having a virus infection that sends infected email to all your clients
- Loss of credibility with customers, vendors, and the public
- Downtime and loss of productivity
- Failing to meet deadlines or customer expectations
- Financial costs associated with cleaning a virus

Hoaxes and Urban Legends

Not a week goes by that I don't get an email from a relative or friend warning me of the latest virus threat. More often than not, these messages are false alarms; in fact, a number of commercial spam filters include an option to automatically screen out common virus hoax messages. Many of these messages instruct me to delete a file out of my computer's Windows directory. Less sophisticated computer users are more than willing to believe that their computer has a virus, and they are more than willing to forward such notices on to many others. Although the people who forward these messages are well meaning, often the files these messages instruct you to delete can do real harm to your OS. Users should be trained that if they receive an alert about a virus, they should verify that alert with their antivirus vendor's Web page or their IT department.

These hoaxes play on our fears of computer viruses. Usually they sound quite convincing and make things seem like doom is certain unless you follow their instructions. These hoaxes almost always ask you to forward the message to as many of your friends and family as you possibly can.

The Good Times hoax is probably the most successful hoax in virus history. From some perspectives, Good Times accomplished the same things as modern email based viruses—it managed to get passed from mailbox to mailbox. This hoax originated in 1994, but is still being passed around the Internet today. The author of this hoax instructed anyone who received a message with the subject "Good Times" to immediately delete the message; interestingly enough, if people were following its advice, they would have read only one of these messages. The message claimed that the Good Times virus would send a message to everyone in your address book, then proceed to trash the computer. They then urge you to forward the message on to your friends and local system users.

✎ In 1995, an Australian virus group created a real virus called Good Times that included some of the text from the Good Times hoax message in the source code of the real virus.

The Internet is full of hoaxes, myths, and urban legends. In the early days of the publicly accessible Internet, Darwin awards (some were true, some were simply Internet folklore), warnings of kidney theft rings, and stories of Neiman Marcus cookie recipes occasionally hit my mailbox.

📖 You can find more information about hoaxes, myths, and urban legends at the following Web sites:

📖 http://www.vmyths.com

📖 http://www.sophos.com/virusinfo/hoaxes

📖 http://www.snopes.com

📖 http://www.stiller.com/hoaxes.htm

Email-Based Viruses

Traditionally, viruses were spread only by infected floppy disks. Public email systems, such as the Internet, have given viruses a new method of replicating themselves. Any virus can be spread through email if a user inadvertently sends an infected program or document to another user. However, specific email-based viruses generally have to be written to understand the email client that it will use to propagate itself. When an email virus is executed, it scans the user's address book and sends a copy of itself to everyone in the user's address list. In the case of clients such as Microsoft Outlook or Outlook Express, an email-based virus may send itself to the entire Outlook GSL as well as the contacts in user's personal address book and contact folders. In the case of Outlook Express, the virus sends itself to the recipients in the Windows Address Book. In some organizations, a single user opening an email virus could cause a message to be sent to tens or hundreds of thousands of mail recipients.

💣 Not all viruses simply use the Exchange GAL as a source for email addresses. Some viruses now look at the Outlook Inbox and Sent Items folders and gather email addresses from messages you have sent and received. One virus even scans your hard drive looking for HTML files that contain email addresses.

Most email-based viruses work by sending themselves as an attachment to an email. Most unsuspecting users will open this attachment, and the virus begins its infecting and spreading phase once again. The attachment may be an executable file, script, or some other type of file that might be able to automatically execute a macro or perform some action as a result of the file being loaded. Even registry files could possibly be used to help a virus spread; however, there have been viruses that could execute even if the message was merely displayed in the Outlook preview pane. To help better understand how email-based viruses propagate, I will discuss in more detail a few of the more common email viruses.

Melissa

Melissa (also known as W97M.Melissa) is a Microsoft Word 97 macro virus, but it has some of the characteristics of a worm. Melissa got its name from a stripper in Florida that the author, David Smith, knew. In the code of the virus, the author identified himself as Kwyjibo; Kwyjibo is a word that Bart used in a game of Scrabble in an episode of the TV show The Simpsons.

```
"WORD/Melissa written by Kwyjibo
Works in both Word 2000 and Word 97
Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
Word -> Email | Word 97 <-> Word 2000 ... it's a new age! "
```

Melissa arrived with a subject of “Important Message from” and the sender’s name. The attachment initially was a file called LIST.DOC, but the virus can be spread by any file attachment. When the user opened the file, a macro executed that looked for Outlook address books. The virus would then send a copy of itself to the first 50 people in your address book.

The Simpsons reference would occasionally be included in the currently open Word document if the document was opened when the day of the month matches the current minutes value on the clock (for example 15th of the month and 15 minutes after the hour). In this case, the user would see Bart’s quote after he used the word Kwyjibo to win a game of scrabble, “Twenty-two points, plus triple-word-score, plus 50 points for using all my letters. Game’s over. I’m outta here.” There are now a few dozen variants of the Melissa virus.

> 🕮 If you are interested in learning more about Melissa, visit http://www.softpanorama.org/Antivirus/AV_Secrets/Vgallery/melissa.shtml.

Happy99

Happy99 (Happy99.Worm, Trojan.Happy99, I-Worm.Happy, W32-Ska, and Happy00) is officially an email-based worm, but it has characteristics of a virus and a Trojan Horse. The program (Happy99.exe) arrives in an email message. When opened, it displays “Happy New Year 1999!!” and fireworks (see Figure 1.2). The fireworks are merely a diversion while the virus installs itself to the local hard drive, configures itself to run each time the computer restarts, and emails itself to addresses in the address book or Exchange GAL. Happy99 is one example of a worm that will reload itself after a computer reboots.

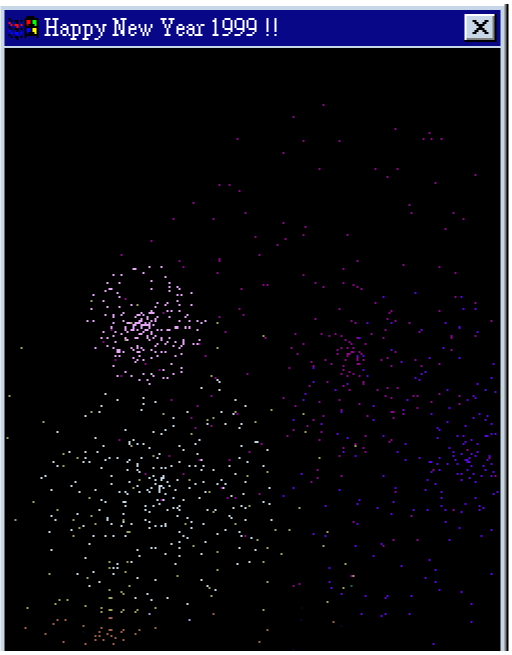

Figure 1.2: Happy99's seemingly harmless output.

PrettyPark

PrettyPark is one of the new breed of hybrid viruses that have worm characteristics. It behaves similar to the Happy99 worm in that it is able to reload itself after a reboot. This virus arrives in a user's mailbox with the attachment PrettyPark.exe. When the file is executed, it might display the Windows 3D Pipes screen saver. It also creates a new Files32.vxd in the \Windows\System folder, and modifies the registry so that this file is included as a Windows shell option. It then attempts to email itself to addresses in the Outlook address book every 30 minutes, and connects to an IRC channel once every 30 minutes. The worm can then transmit information about your computer to this IRC channel and can receive instructions from someone in the IRC channel.

Mylife

The Mylife worm/virus caught a lot of even the most attentive administrators off guard. It was first discovered in April 2002. This message arrived with the innocuous message indicating a funny screen saver is attached. When the attachment, usa.scr, was opened, it displayed the graphic that Figure 1.3 shows.

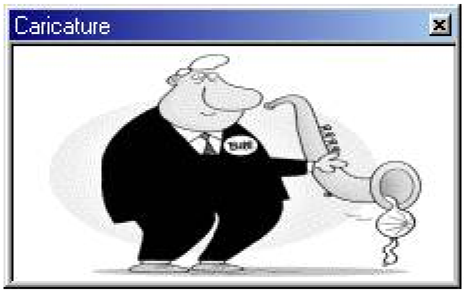

Figure 1.3: The Mylife caricature seems harmless.

The caricature graphic was not even particularly funny, so most users would close it and move on, assuming that it was just another boring email attachment. In the background, though, the .scr attachment added itself to the registry, copied itself to the Windows system directory, and mailed a copy of itself to all of the addresses in the Outlook address book and the MSN Messenger contact list, if available. When the Mylife scr file is run from the Windows system folder, it deletes all the files and folders on the C: drive.

Nimda

Nimda (admin backwards, in case you were wondering) arrived on the scene in September 2001; it or its variants have been making our lives difficult ever since. Nimda is classified as both a virus and a worm, but it behaves more like a worm. This worm introduces a whole new range of ways that a worm can spread itself. Copycats have been developing worms ever since, attempting to use the same techniques.

The worm attempts to use a known (and patched) bug in Microsoft IIS 4.0 and 5.0 that allows malformed URLs to access files and folders that are located anywhere on the same logical drive as the Web server folders. This vulnerability allows the worm to infect the Web server, replace Web pages, or even add itself to Web page content. The worm then uses that Web server as a platform for scanning IP address ranges, looking for other Web servers with the same vulnerability.

After unsuspecting clients connect to an infected Web server, the clients are prompted to download an .eml file (email file). This file contains the worm as an attachment. When the clients download and open the message, their computers become infected and start looking for other computers to infect. In addition, the worm will scan Outlook address books and any HTML files on computers looking for email addresses to which it can send itself. Nimda has a built-in SMTP server that sends outbound messages, so it can bypass some of Outlook's built-in antivirus features. Nimda also scans the network looking for other computers with open shared folders. If it finds the folders, it attempts to transfer the file RICHED20.DLL (which is used by Outlook and Word when creating email) to the remote shared folders. If a user opens a message and the new version of RICHED20.DLL is in the path, Outlook or Word uses the new version of the file and begins to infect computers with the worm. For a 57KB virus, Nimda has some impressive features.

Scanning for Viruses

Depending on the vendor, virus scanning software can take one of a couple of different approaches to finding and repairing viruses. However, at the heart of all virus scanning systems are the virus signatures. The *virus signatures* are a database of all known viruses as well as something unique about each of those viruses. For most vendors, the publicly released version of this database changes weekly; during periods of high virus activity or when multiple new strains of a virus are being discovered, updated versions of the signatures database may be released several times a week. Internally, the database may change several times a day, as virus specialists reverse engineer the viruses that are discovered daily.

Secondary to the virus signature database is the scanning engine itself. The scanning engine is the technology that actually scans for viruses. Keeping the scanning engine up-to-date is almost as important as keeping the signatures updated. As new viruses are discovered and viruses get harder to detect, older scanning engines will not be able to detect viruses accurately.

Virus scanning software uses the signature database as it scans files on the hard drive to look for signs that a virus has infected a file. Most scanners simply open the designated files and search for the patterns of known viruses. Virus scanners can be configured to scan the hard disk for all files or only files with specific extensions. Virus scanners also scan the computer's memory and master boot record looking for viruses. A virus scanner should also be capable of real-time scanning of the file system (hard drives, removable drives, and floppy disks). When a user accesses files on the file system, the virus scanner should scan the file.

Virus scanners also employ a number of techniques beyond just simple file scanning to detect viruses. More sophisticated scanners can examine executable files looking for something out of the ordinary in the file, such as an instruction at the beginning of the executable that instructs the computer to immediately go to the end of the program. Scanners with *heuristic detection* capabilities work on the assumption that a virus will attempt to conceal itself (such as stealth or polymorphic viruses). Client scanners are also email-aware. These scanners can detect when an email client opens a message, then scan that email message for viruses.

> 💾 Do you want to test your virus scanner? The European Institute for Computer Anti-Virus Research (EICAR) has a test file called eicar.com. It is not a virus, but most virus scanners will recognize and detect this file. It can be found at http://www.eicar.org.

A Matter of Trust

Just as if your machine had been attacked and compromised by a skilled hacker, once a sophisticated virus (or worm or Trojan horse) has taken over your machine, you may not be able to completely trust the machine again. The virus may have left components that are not yet detected and cleaned up by antivirus scanners. The component may lie dormant for some period of time, reactivate, and re-infect the computer.

For this reason, integrity checking products are becoming more popular for critical computers such as servers. An integrity checking program works by scanning the hard disk of a computer that you know can be trusted. The program calculates a checksum for each of the executables and dynamic link libraries (DLLs) on the server's disk and records this information to a log or database file. If the machine is ever compromised, a checking program can analyze the hard drive and determine whether any other critical OS or applications have been compromised of which you are not aware. The limitation of integrity checking programs is that each time a service pack or OS update is released, the integrity checking program must recalculate the checksums of the files.

> 📖 A good explanation of integrity checking and what to look for in an integrity checking program can be found at http://www.cknow.com/vtutor/vtintegrity.htm.

An Ounce of Prevention

In the early days of viruses, there was not a lot that users could do to protect themselves from viruses. About all you could do was never download files, never install software that was not from a completely trusted source (and this was no guarantee!), and never share floppy disks with anyone else. By 1989, there were a couple of commercially available antivirus software programs, which changed the face of virus protection.

Keeping user's computers—not only their desktop computers at work, but also their home computers—virus free is very important. (Many users work from home occasionally and could introduce malware from their home computers to a corporate computer system.) The following list provides important steps that you and your end users can take to help ensure that you remain virus-free:

- Purchase and install an antivirus scanner that does real-time antivirus scanning of the computer's file system and detect floppies when they are inserted.
- Keep the antivirus software and virus signature database up-to-date. Doing so might require updating the signature database a couple of times per week.
- If you receive files that you do not expect via email, don't open them.
- If you are using Microsoft Outlook or Microsoft Outlook Express, download the latest version or the security updates.
- If a message or attachment from someone seems to be out of character for that person, don't open it. For example, your boss is hopefully not going to send you a message with the subject ILOVEYOU.
- If you are sending a message with an attachment, send the message and attachment, then send a second message letting the user know that you sent them a legitimate file. Use S/MIME digital signatures to further guarantee the authenticity of your message.
- Do not forward junk mail or chain messages.
- If a Web site you are visiting prompts you to download software or run a program, don't do it! Only download software that you have specifically requested.
- Do not download software from the Internet if you do not have an antivirus program running on your computer.
- Exercise extreme caution when using Internet file-sharing services. These services are a major source of viruses, Trojan horses, spyware, and adware.
- Keep regular backups of your important data.
- Verify the sender of emails. If Microsoft, Apple, IBM, Amazon, your bank, your credit union, or any other entity that you may have an online relationship with sends you an email and advises you to download something, view that messages with a good degree of skepticism. If you choose to follow the link, make sure that it takes you to that vendor or company's Web site.
- OS updates and fixes are usually installed by an organization's IT department; avoid following the advice of email messages telling you that your computer is insecure and need updates. Especially on your company's network.

References and More Information

When I was writing this chapter, several excellent references reinforced my knowledge and taught me new facts. If you want additional information, these Web sites are great starting points.

Carnegie Mellon University's Computer Emergency Response Team Coordination Center (CERT/CC) (http://www.cert.org) is one of the best places to look for information about security, viruses, Trojan horses, and worms.

The WildList Organization International (http://www.wildlist.org) has a great Web site that includes information about which viruses are currently spreading and which are fading from the radar.

The SANS Institute (http://www.sans.org) is an excellent source of information not only about viruses and worms but also about security information in general.

Computer Knowledge's Virus Tutorial (http://www.cknow.com/vtutor) is an excellent starting place for learning more about the basics of viruses as well as for articles written by industry experts.

Current virus alerts, virus news, statistics, advice, and information about hoaxes can be found at Viruslist.com (http://www.viruslist.com).

EICAR helps to coordinate the activities of private and public organizations, security experts, and government agencies when fighting computer viruses. You can find the organization on the Internet at http://www.eicar.org.

The Internet USENET newsgroups include alt.comp.virus. A culmination of information from these newsgroups is organized in the group's FAQ at http://www.faqs.org/faqs/by-newsgroup/alt/alt.comp.virus.html. If you plan to join any of the virus-related newsgroups, you should read the FAQ first.

Want to know how your antivirus program stacks up? Visit AV-Test (http://www.av-test.org). This project is a combined effort of the Business-Information Workgroup at the Institute of Technical and Business Information Systems at the Otto Von Guericke University in Magdeburg, Germany.

Summary

Computer viruses have evolved dramatically over the past 20 years. They are sneakier, more powerful, and spread more quickly. In addition, virus writers will continue to make viruses more and more difficult to detect and more powerful. These writers will undoubtedly continue to find new ways to spread their malware. Emerging technologies such as wireless communications, PDAs, tablet computers, cell phones, and other handheld devices will undoubtedly become targets for virus writers.

As we've explored in this chapter, the challenge of virus protection is going to continue. Hopefully, the background information about viruses as well as knowing which types exist and how they work will help you protect your organization's desktop computers, file servers, database servers, Web servers, and email servers.