

Getting Facts that Win Cases

. . . a monthly update for clients from Richard Schenkar—January 2004

In this issue:

How to handle viruses—1

What was that unrecognizable file?--5

How to Know What Files Will Cause Problems—7

How to handle viruses

Recently, Internet security experts found a new version of the Mydoom computer virus that is different enough from the first version that it cannot be detected. But because it is focused on attacking www.microsoft.com, Microsoft Corporation's main website, as well as the website of US-based software vendor SCO (the target of the original Mydoom virus) response is more deliberate. Experts took only ninety minutes to crack the new virus code. Its new feature, cutting off access to websites of several anti-virus software firms, makes it more incidious.

The experts tell you to use a clean computer to download the virus fixes to a floppy disk and then administer the digital medicine to the infected computer. That is a wonderful idea—except when you have only one computer or only one that uses the current software that you need. The best practice is to maintain the antivirus protection on your most-used computers (at least weekly) and update the recovery disks you maintain for when your system crashes (you *do* have recovery disks, don't you?).

To get some sense of the impact of the MyDoom virus, consider that it caused over 100 million infected e-mails to be sent.

In Europe the percentage of e-mails infected exceeded 33 percent.

Unlike most computer virus outbreaks, MyDoom continued spreading even after a day and a half.

Copyright 2004 by Richard Schenkar, 2 Maple Lane, Mercer Island WA 98040-4045.

Phone: 206-232-2282, Fax: 206-232-3020. Email: Richard@RichardSchenkar.com.

Website: <http://www.richardschenkar.com>. Page 1. Richard Schenkar connects you with information you need to be effective through consulting, presentations, and writing.

One of the purposes of Mydoom is to relay spam (unsolicited e-mail advertisements) through e-mail attachments and downloads from the file-sharing services that let Internet users share content with for free. By faking a human face as an error note with the main text message attached, users are encouraged to open the attachment, launching the virus.

How to minimize virus problems:

It is prudent to review some basic precautions and procedures to keep yourself from being bothered by these irritations. If you have noticed that your computer has slowed down, files have been changed mysteriously, or the startup sequence for the computer is different, you may have been hit with a virus. Antivirus software is appropriate first aid for such a problem, but if you follow these suggestions, you can minimize the frustration.

Passwords

Your password is your (literal and figurative) key to the Internet. Most computer violations are accomplished by cracking passwords. Keep your passwords secure and change them often. Most experts suggest a password of six characters or longer--I have one that is fifteen characters long. Do not use words or strings of adjacent keyboard keys--scanning for words and keyboard strings is a common feature of password-cracking software. Mix numbers, lowercase letters, uppercase letters, and standard symbols (the ones on your keyboard already) to create a complex password matrix, write it down so you remember it, and keep the written record of your passwords secure.

Computer Placement

Where you place your computer can put your machine at risk. If you have a terminal connected to your network in the lobby or reception area of your office, who can look at the screen? Is it visible from

the public area (thus compromising your clients' confidentiality)? Reposition the screen so it is not a security risk. Is there a lock with a key on that keyboard and the central processing unit (if it is there) so that the machine can be locked when office staff walks away from the area? Make sure that all persons who access all computers in the office are aware of these risks and think in terms of keeping computers and data in them secure.

Make and Keep Backups

This can and does save hours of work and frustration. Backup your entire hard disk at regular intervals (depending on the nature of your practice) using a tape drive or large-capacity disks. I have used many floppy disks for multiple backups; sometimes I feel like I am drowning in floppy disks, but the backups have saved me time and money often enough that the practice of backup is worth the few minutes investment.

Antivirus Software

Install antivirus software--software that can detect and delete viruses safely. Be aware that as viruses change, you need to update your software regularly with new virus signatures that you may obtain off the web site of the software producer. Search the extensive archives of ZDNet, <http://www.zdnet.com> from Ziff-Davis, the publishers of many computer magazines, for free antivirus software, shareware, and software for sale. Consult the documentation of your antivirus software for more information about updating and plan to do it at least monthly--and more often if you do a lot of work online or are continuously connected to the Internet. As you shop for new or upgraded computers, you might consider asking about hardware antivirus protection as well, but because there are always new viruses created, you cannot stop with a hardware antivirus solution.

Avoid Attachments

Most of the recent problems that have ravaged the hard disks of people on the Internet have revolved around viruses that ride on attachments to electronic mail. Sending documents as attachments is convenient for lawyers because they can isolate their own comments from the contents of the document. Do not open attachments from people you do not know. Do not open attachments with filenames ending in the extension ".exe" or ".com" because they are EXEcutable files or COMand files that might destroy your system. It is prudent to quarantine all suspected files. If you must look at quarantined files, transfer them to a floppy disk. On a separate computer, run antivirus software against the disk and, with a DOS word processor (that you can download off the ZDNet web site), look at the file on that separate computer.

Check Out Rumors Before Spreading Them

Every time we get some alarming rumor, the first impulse we have is to tell it to everyone we know. It is much easier to do that now with stored electronic mail lists that we all have. Let's take a minute to check rumors out before passing them on. If the rumor relates to a particular software or hardware vendor, chances are that the vendor already has some response posted on the vendor's own web site. Start there and look. After you check that site, check the U.S. Department of Energy's Computer Incident Advisory Commission web site at <http://www.ciac.org> . It is careful and credible in its suggestions. In addition, ZDNet <http://www.zdnet.com> and CNET <http://www.cnet.com> have resources to check out such rumors. In many cases, the news of credible virus attacks will break on either ZDNet or CNET.

Consider Source Credibility

Before you hit that key to pass that hot rumor on, consider the

credibility of the information you are using. Before you download software, make sure you are using credible sources. Anyone can put anything online regardless of credibility. Would you rely on those data or sources in your practice without objection?

What *was* that unrecognizable file?

Have you ever received a file that you could not open or that looked like gibberish when you looked at it with your word processor? In most cases, that is because the file is in a different format than those recognized by your word processor.

Some of these frustrations are easier to solve than others. The best place to start is to look at the name of the file, concentrating on the file extension. That is the two- or three-letter designation to the right of the period in the file name. The easy situations include files with the .pdf file extension (meaning Portable Document Format) that you open with the Adobe Acrobat file viewer available at adobe.com. Many government documents already use the Adobe Portable Document Format. That is why it is probably prudent to download and install that viewer (even for your handheld computer or personal digital assistant).

Microsoft PowerPoint presentation files (designated with the .ppt file extension) may be opened with PowerPoint viewers available on the Microsoft website, www.microsoft.com, or with the Impress presentation application in the OpenOffice software suite, available for free download at www.openoffice.org. There are viewers on the Microsoft website for Microsoft Excel files (file extension: .xls), Microsoft Visio files (file extensions: .vsd or .vdx), and Microsoft Word files (file extension: .doc).

Apple Computer's QuickTime Player, available at www.apple.com/quicktime, is a multimedia player that will play a number of different formats, including the QuickTime format (with the .qt file extension) and MPEG audio and video format.

Compressed Files

File compression allows you to transmit and receive files faster and squeeze more data into limited storage. Because many resources were developed on small computer systems with extremely limited specifications (especially by today's standards), you will discover many useful materials online in compressed formats.

File compression works by eliminating redundancy. The programs create a dictionary and a short reference mapped to each item. That short reference substitutes for the item in the compressed file. By this procedure, the average text file compresses to about one-half its original size.

Utilities that compress and expand files (using the .zip file extension) include WinZip (for the Windows operating system), available at www.winzip.com, Stuffit (for the Apple Macintosh operating system), available at www.stuffit.com.

If things get complex. . .

Most of your frustrating situations you encounter will be handled with the resources already cited. As you push further onto the World Wide Web (and off the Web--into massive text archives not indexed by generally-used search tools), you will encounter files in many different file formats with file extensions different than the ones above. You will need some way to discern the format, obtain the proper viewer, download and install the viewer, and test it to make sure that it is working properly. With those two or three letters of the file extension in mind, start with the Graphics File Formats Page, at www.dcs.ed.ac.uk/home/mxr/gfx/utils-hi.html (high resolution version) or www.dcs.ed.ac.uk/home/mxr/gfx/utils-lo.html (low resolution version). From the list of graphic file extensions, pick the one that applies and there is a hypertext link to relevant helpful sites. There is also a helpful FAQ (frequently asked questions)

list, a section on explanations of file formats and a comprehensive list of hypertext links.

Once the necessary viewers are installed on your system, you might want to test them to make sure they work properly. For that, head to the WWW Viewer Test Page at www.eng.llnl.gov/documents/wwwtest.html where you can get an instant online test of the operation of viewer you have selected.

How to Know What Files Will Cause Problems

By knowing what to look for in the file stream cascading through your practice, you can guess, with reasonable certainty, what files could cause you problems. You can then isolate them, test them on other computers not connected to your network, or examine them independently to satisfy yourself that they are problem-free.

What you look for are executable programs that can launch themselves or that use other programs already on your system to launch themselves and do damage. In most cases, you can tell the suspect programs by looking at the file extension—the three-character series to the right of the dot in the filename. The bad news is that there are over 1600 file extensions in use. The good news is that you have to worry about only eight.

The eight you have to worry about will be described here. There are two major archives online that you can use to decode the rest. The website at www.extsearch.com.

Watch for These File Extensions

These are the file extensions that you should note. Do not get paranoid or assume that every file with these extensions deserves exorcism. Perfectly good programs are distributed with these file extensions every day with no problems. Those suspect file extensions include, but are not limited to, the following: .vbs (Visual Basic

Script); .asp (Active Server Pages); .bat (BATch file); .com (COMmand file); .exe (EXEcutable program file); .html or .htm (Hypertext Markup Language); .js (JavaScript); and .pl (PERL Script (Practical Extraction and Report Language)).

Visual Basic Script (.vbs) files are used in many web sites to accomplish many tasks and effects automatically. Because they are versatile and are accepted without question by many browsers, it is easy to slip destructive code into them. Some browsers allow you to block visual basic script files or make a decision on which ones you will accept. If you have an option, make sure you find it, understand it, and exercise it.

Active Server Pages (.asp) are hypertext markup language files with scripts in them that run on servers, rather than on client computers. Here, we should note that "server" computers are often larger computers that do heavy tasks like data housing and searching; "client" computers are generally the computers we see and work on daily. If you have a server in your office, you should watch for active server pages. This is Microsoft technology and is part of its Internet Information Server. These files may also run on the Microsoft Personal Web Server.

Batch files (.bat) are lists of commands that call up programs for execution one after the other. They are often used to automate tasks and introduce efficiencies. They are particularly accessible to most of us because they use programs that are already on your computer and integrate those programs helpfully. That is what makes them insidious. Since they are always text files, you should examine each line of the batch file to understand precisely what the command on that line will do to your system before you release it.

Command files (.com) are executable programs. You probably will not

be able to inspect or back-engineer them (unless you write them yourself and compile them using computer programming languages and compilers). The best you can reasonably do is to get them from reliable sources and know what they are supposed to do. A good practice is to try them on a computer that is not going to ruin your practice if it crashes. (That is a good reason to keep an old computer around the office. You can get used computers from salvage agencies and some stores that specialize in recycled computers. But know what you are getting and be ready to fix it if you must.)

Executable program files (.exe) have the same properties and should be handled with the same cautions as command files.

Hypertext markup language files (.html or .htm) are interpreted by web browsers to create images, text, and other features on your screen. Even though they are written in ASCII (American Standard Code for Information Interchange) which is plain text, they can include scripts where destructive code can hide. Inspect the file with a word-processor in non-document or programming mode or check it out on that old computer mentioned above.

Javascript files (.js) and Practical Extraction and Report Language (PERL) Script files (.pl) are interpreted by web browsers to accomplish various tasks. Be sure you know what they do and why they are on your system.

Have You Been Spammed By This Hoax?

If you are like most of us, you have probably received many pieces of electronic mail with the following curious words somewhere near the bottom:

"This message is sent in compliance with the email bill section 301. Under Bill S.1618, TITLE III, passed by the 105th U.S. Congress this message cannot be considered Spam as long as we include the way to be removed (Paragraph (a)(c) of S.1618). Further transmissions to

you by the sender of this email may be stopped at no cost to you by sending a request to be removed to ."

If you have been curious about this allegation, you will soon be satisfied. This legalistic allegation is a hoax. Although the bill passed the U.S. Senate on May 12, 1998, it was referred to the U.S. House Committee on Commerce on October 21, 1998, where it died. Since this writing will eventually appear on the Internet, there is no utility in repeating the precise verbiage of the Senate bill. That repetition would perpetuate the hoax. We still have to deal with these undesired interruptions (called "spam"). Electronic mail is so inexpensive to use. By the use of anonymous remailers and by constantly changing the addresses from which electronic mail is dispatched, one can avoid detection except from the most studious and persistent tracker. Your mere presence in the electronic community (evidenced by your use of your electronic mail address) means that you become vulnerable to the loss of productivity that arises because you have to handle this electronic rubbish. Also, the resources on your system and on every step of the electronic information-handling transaction are burdened by handling this garbage.

There are some practical actions we can take to manage these frustrations. They include the following:

- 1) Do not respond at all to unsolicited electronic mail. It does not matter how strongly you feel about its offensiveness.
- 2) Never respond to the invitation to "remove" your name by sending a "remove" instruction. That process validates your address and you will get more offensive mail.
- 3) If you are curious about an offer made with a hypertext link, do not click on that hypertext link. It is better to type the Uniform Resource Locator (URL, or the given citation) into your browser separately. Since many tracing programs can attach your electronic mail address to your entry into a website when you enter directly by

clicking on a hypertext link, the practice of a separate entry into the target website does not give the offending mailer the satisfaction of a connection with the offending electronic mail.

4) Do not try to figure out who or what is sending you the offending mail. You can spend considerable amounts of time trying to parse the headers of electronic mail. It really is possible to trace electronic mail through every single electronic "hand" it passes through, but that process is generally not worth anyone's time (unless one is preparing for litigation).

5) What you can and should do is try to filter your electronic mail. Some electronic mail programs allow you to sort your mail automatically into folders and allow you to automatically block or delete mail from particular addresses. The sorting function is particularly helpful when your incoming mail flow reaches torrential levels.

The blocking function can be helpful if you notice that you are getting offensive mail from a particular source. Because there are so many anonymous sources of offensive mail and they change daily, you may discover that attempts to block mail will leave you with a long list of addresses to block-absorbing resources on your hard drive while the offensive mailers have gone on to other addresses. Rather than trying to block every offensive mailer, your better practice is simply to delete offensive mail and forget about it.

If you are ready to spend some time and effort in tracing electronic mail, either for yourself or for your clients, there are some technical tools you can use to interpret electronic mail headers and footers. You will find information about them in the SPAM FAQ (Frequently Asked Questions file) at

<http://www.cs.ruu.nl/wais/html/nadir/net-abuse-faq/spam-faq.html>.

There are data about filtering and blocking tools at

<http://spam.abuse.net/spam/tools>.

A warm personal note—even in a virus:

Deep in the code of the MyDoom virus was encrypted this message
"Andy; I'm just doing my job, nothing personal, sorry."