

“Everything you always wanted to know about computer viruses* *But were afraid to ask”

The last time we wrote about computer viruses in *Occasional Downtime* was in October 1997. Rereading the article today, it's immediately obvious that much has changed since 1997. In 1997 macro viruses were just beginning to become a problem. Infections with boot sector viruses and file viruses were still the most common kind of virus infections. The most common way for viruses to spread was by infected floppy disks or by downloading infected files from bulletin boards and the Internet.

Today macro viruses are by far the most common type of virus in the world. Infections by boot sector viruses and file viruses have decreased dramatically while we have seen the rise of two new types of viruses: Visual Basic Script viruses and JavaScript viruses. The way viruses spread has also changed. Viruses are now spread most commonly by way of email attachments. Email-enabled worms that spread by sending copies of themselves to everyone in an online address book have become a particular problem. Infected diskettes or CD-ROMs and the downloading of infected files from the Internet still appear as vectors of infection, but are much less common. You can read more about the types of viruses and how they spread in another article in this issue of *Occasional Downtime*.

So things have certainly changed. Unfortunately they have not changed for the better. According to the ICSA Labs 6th Annual Computer Virus Prevalence Survey 2000, the likelihood of a company having an encounter with a virus infection has approximately doubled every year for the past five years. ICSA (International Computer Security Association) surveyed 300 companies, comprising government agencies, healthcare, manufacturing, and education, each with more than 500 computers. The number of encounters reported, where encounter was defined as an event or incident where viruses were discovered on any PCs, diskettes, or files, translated into an average of 91 encounters per 1,000 PCs per month. Significantly, half of the respondents had had a virus disaster of 25 or more PCs or servers infected at the same time.

At best, a computer virus infection is a minor annoyance. But at worst, a virus infection can mean days of lost productivity, corrupted files, lost data, computer instability, and system crashes. An outbreak of the MTX virus on the HMC campus in December required several days of work by CIS staff to remove the virus from affected computers. A more recent outbreak of the Hybris worm, which while it actually infected only four off-campus machines that we know of, affected everyone on campus, since the worm sent repeated copies of itself to the faculty, staff, and emergency mailing lists.

What can we do to prevent virus infections? Installing and using an effective anti-virus program on your desktop PC is an important first step. (continued on page 4)

TYPES OF VIRUSES & HOW THEY SPREAD

IN THIS ISSUE

Everything You Always Wanted to Know About Viruses, But Were Afraid To Ask ----- cover

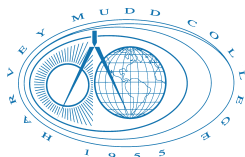
Types of Viruses and How They Spread ----- 2

Editor's Notes ----- 3

Tricks & Tips ----- 6

Q&A ----- 8

Occasional Downtime is composed on a Macintosh G3 computer using Adobe PageMaker 6.5 and Microsoft Excel 98. The primary typefaces used are Times and Optima. We wish to thank Sally Rich Arroyo of the HMC Office of College Relations for all her help.



Viruses can be difficult to classify since an individual virus can often be classified several different ways. In this article we will describe some of the most common types of viruses and how they spread. In the past the most common type of viruses on the PC were boot sector viruses and file viruses. Boot sector viruses infect the boot sectors of floppy disks and the partition sector or DOS boot sector of hard drives. The virus infects the hard drive when you boot the computer from an infected floppy. The virus then becomes resident in memory and infects every disk you put in drive A.

File viruses, on the other hand, attach themselves to files, usually executable files. When the infected file is run the virus is transferred to memory and then begins to infect other programs as they are run. Die Hard is an example of a PC file virus. A multi-partite virus is particularly nasty in that it combines the features of both boot sector and file viruses. It can infect both files and boot sectors/partition tables and spreads using both methods.

With the advent of Windows 95/98 and Windows NT, these viruses have become much less common. These operating systems are different enough from previous operating systems that these viruses are unable to propagate well under them.

Certain types of Macintosh-specific viruses have also become a lot less common. Most operate by infecting particular resources in the system file and cannot infect newer versions of the Macintosh operating system such as System 8.x and 9.x. One of the common Macintosh viruses was the MBDF virus, which is named after the type of resource that it uses to infect files. There are several other Macintosh viruses that use system resources to infect files,



including the WDEF virus, the MDEF virus, and the CDEF virus.

The most recent Macintosh-specific virus infection was the AutoStart 9805 worm which appeared originally in Hong Kong and Taiwan in April 1998. You can read more about AutoStart 9805 and its variants in the Viruses and the Mac FAQ at <http://www.faqs.org/faqs/computer-virus/macintosh-faq/>.

Today macro viruses are by far the most prevalent type of virus and are a serious problem for both Macintosh and PC users. Macro viruses infect data files rather than executables. They are also not platform specific, meaning that the same virus can infect both Macintoshes and PCs. Macro viruses typically infect Microsoft Word and Excel documents, although they also can infect PowerPoint documents. Macro viruses use the macro programming language of an application to infect documents and spread.

The Word Concept virus was one of the first macro virus to become widespread. Opening a Microsoft Word document infected with the Concept virus installs the virus macros which then spread to other Word documents when they are opened. The virus does not cause any loss of data

or damage, but it makes Word only let you save documents as templates, which is pretty annoying.

More recently we've seen the spread of script viruses, including Visual Basic Script viruses and JavaScript viruses. These viruses are written in the Visual Basic Script and JavaScript scripting languages. They take advantage of "objects" on Windows machines; some of these objects are part of the Windows operating system and others are provided by a variety of application programs. Most were originally intended to make it possible to automate certain tasks on Windows machines. The viruses take advantage of these objects to propagate themselves and to sometimes damage the host computer.

Stand-alone script viruses are contained inside a file which must be opened to be executed. Embedded script, however, is script code that is embedded inside HTML, which can be part of a Web page or in the body of an HTML email message. Merely viewing the HTML email message could execute the script code. Fortunately, embedded script viruses are currently quite rare and it is usually possible to disable the ability to execute script objects from within an applications such as MS Outlook.

Script viruses and some macro viruses behave in such a way that they are more accurately classified as "worms" rather than viruses. A worm is a self-contained program that can spread functional copies of itself to other computers, usually via network connections. The Hybris worm seen recently on campus is a good example of a worm. The Hybris worm arrived in the form of an email attachment, which, when opened, would infect the host computer. Once a computer was infected with the Hybris worm, the worm would monitor Internet activity, including both incoming and outgoing email, and would send copies of the infected email attachment to all

(continued on page 5)

ditor's Notes

This month's issue of *Occasional Downtime* is devoted to a topic that received a lot of attention on campus this past month: computer viruses. Last month the Hybris worm was sent to the faculty and staff mailing lists via an infected off-campus computer. Several users opened the infected attachments, either on their office or home machines, and infected their computers with the worm. Before the users realized that their machines were infected, the worm sent out multiple copies of the infected email message to several campus mailing lists. While the worm did not cause any significant damage or data loss, it did require a significant amount of time and effort to remove from infected computers.

While this incident actually occurred after we had begun work on this issue of *Occasional Downtime*, it certainly underscored the importance of educating our users on how to be prepared for a virus infection. To that end we've included articles on how to prevent virus infections and on the different types of viruses and how they spread.

We'd also like to emphasize that while it's important to be prepared, it's also important to not become too paranoid! It should be possible to protect yourself from computer viruses, while not negatively impacting your ability to work.

—Elizabeth Hodas

Occasional Downtime is published bimonthly by the Computing and Information Services Department at Harvey Mudd College. It is also available in PDF format on the HMC Web Server. Comments and questions can be directed to downtime@hmc.edu.

Viruses continued from page 1

Installing the anti-virus program is only the first step, however. New viruses are discovered almost every day, so it is crucial to make sure that the anti-virus program is updated regularly. Anti-virus programs use what are called virus signature files to detect viruses. These signature files must be updated whenever new viruses are discovered. Some anti-virus programs update automatically by downloading signature files from the Internet; others must be updated manually by downloading files from a Web site.

At Computing and Information Services we use an anti-virus program by McAfee. We have a site license for McAfee through our Novell Netware license. McAfee's anti-virus software is installed on our Novell file servers and is updated regularly. Any file copied to one of the file servers, such as Kato, Lurch and Igor, is automatically scanned and cleaned if a virus is detected. Users who save their files to the file servers are thus automatically covered by anti-virus software.

Users who save files to their local desktop, however, should be using an anti-virus program on their desktop as well. CIS installs the desktop client anti-virus software by McAfee on all PC's that we set up. The desktop client software can be configured to update its virus signature files either at startup or at scheduled intervals. (Not sure how to update your anti-virus program? Check out this month's *Tricks & Tips* section for help.)

Unfortunately, while the anti-virus software installed on the file servers will scan and clean Macintosh files (e.g. for macro viruses), McAfee does not have a desktop client for the Macintosh. CIS thus does not have a site license for a Macintosh anti-virus program. Of the anti-virus programs available for the Macintosh, CIS recommends Dr. Solomon's Virex.

Installing and updating anti-virus software is not the only way that users can protect themselves against viruses, however. While anti-virus programs are an effective protection against known viruses, new viruses can spread so quickly that anti-virus programs cannot be updated in time and are of limited use against them. In particular, viruses or worms that spread by sending copies of infected email attachments to all addresses in a user's electronic address book can spread across the Internet within hours. The Melissa virus is of course one of the best-known examples of this type of virus. Melissa was released on March 26, 1999, a Friday, and spread rapidly around the world over the weekend. Tens of thousands of computers were infected and many companies, including Microsoft and some of the Claremont Colleges, were forced to shut down their email servers to contain the spread of the virus.

So what can users do to protect themselves? Well, we've all heard of "safe sex." Users must now practice "safe email." It is no longer enough to screen email attachments based on whether we know the sender or not. Since these email-enabled viruses use the personal address books of our friends and colleagues to spread, we must be suspicious of ALL email attachments that we receive. Users should only open email attachments if they are actually expecting to receive the attachment. Otherwise they should confirm with the sender that the sender actually meant to send them the attachment.

Many viruses take advantage of security holes in popular software programs such as Internet Explorer, Netscape, and Microsoft Outlook in order to spread. Microsoft Outlook is particularly vulnerable to viruses. These security holes are often actually programmed as "features" of the software and can be modified or turned off completely by the user in order to make the software less vulnerable to viruses. For example, Microsoft Outlook has a feature

called “Preview Panes” which automatically opens email messages and attachments as soon as you select the message. This is a feature that you would definitely want to disable!

Other programs, such as Microsoft Word have features that will warn you if a file has embedded macros in it and allow you to disable them before you open it.

CIS is also considering other options, such as installing anti-virus software on our mail servers and filtering messages sent to campus mailing lists. 🐾

Virus Types continued from page 3

email addresses it saw. Copies of the infected email were sent to the faculty, staff, and emergency mailing lists several times, all by people who did not realize that they were infected.

Another virus type you may come across is a Trojan horse. A Trojan horse is not actually a virus, but a computer program that appears to be a useful program but which is actually destructive. Trojan horses do not generally replicate so they are not as much of a problem as viruses. Once it becomes known that a program is actually a Trojan horse it is easy to avoid. 🐾

SOURCES

GENERAL INFORMATION

CERT® Coordination Center Computer Virus Resources

http://www.cert.org/other_sources/viruses.html

Computer Virus FAQ for New Users <http://www.faqs.org/faqs/computer-virus/new-users/>
Frequently Asked Questions on Virus-L/comp.virus

<http://www.faqs.org/faqs/computer-virus/faq/>

EICAR (European Institute for Computer Anti-Virus Research) <http://www.eicar.com/>

ICSA (International Computer Security Association) <http://www.icsa.net/>

Virus Bulletin <http://www.virusbtn.com/>

The Wildlist Organization International <http://www.wildlist.org/>

WHITE PAPERS

Bridwell, Lawrence and Peter Tippett, ICSA Labs 6th Annual Computer Virus Prevalence Survey 2000, ICSA, 2000.

Kennedy, Mark, Script-Based Mobile Threats, Symantec AntiVirus Research Center, 2000.

TruSecure Anti-Virus Policy Guide, Version 3.5.0, TruSecure Corporation, 2000.

VIRUS DATABASES

Data Fellows F-Secure Security Information Center <http://www.datafellows.fi/virus-info/>

Dr. Solomon’s Virus Central <http://www.drsolomon.com/vircen/index.cfm>

McAfee.com Virus Information Library <http://vil.mcafee.com/>

Symantec AntiVirus Research Center <http://www.symantec.com/avcenter/>

HOAX DATABASES

Data Fellows Hoax warnings <http://www.datafellows.com/virus-info/hoax/>

McAfee Virus Hoaxes <http://vil.mcafee.com/hoax.asp>

Symantec Virus Hoaxes <http://www.symantec.com/avcenter/hoax.html>

Tips & Tricks

Tricks &

UPDATING VIRUS SIGNATURE FILES

As we mentioned in the cover article of this month's *Occasional Downtime*, it's not enough to simply install anti-virus software on your computer. It's equally, if not more, important to keep the software up to date. In addition to upgrading to new versions of the software as they become available, you also need to update the virus signature files that the software uses to detect viruses. As new viruses are discovered, the manufacturers of anti-virus software release new signature files that must be downloaded to your computer.

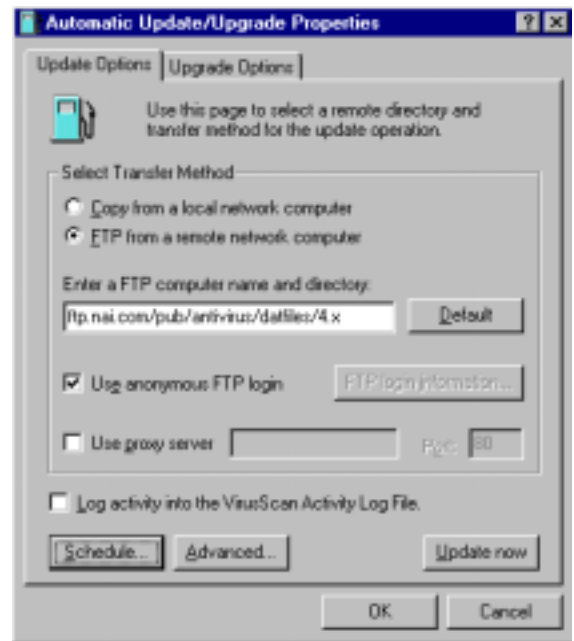
Fortunately most anti-virus software can be configured to automatically download these files so that you don't need to remember to do so.

At CIS we've been using VirusScan by McAfee. This software can be configured to either download updated signature files on a schedule, e.g. once a week, or every time you start up the computer. In the latter case the software would check an FTP site every time you start up your computer, and if there were an updated signature file it would download it automatically.

VirusScan for Windows 95/98 and for Windows NT looks a bit different. For Windows NT first right-click on the VirusScan shield icon in the lower right-hand corner of your screen and select



Console. Double-click on "Automatic DAT Update." Click the radio button labeled



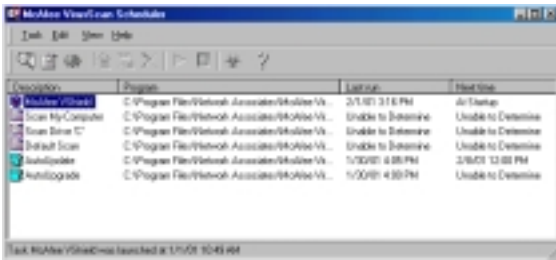
"FTP from a remote network computer." Check the "Use anonymous FTP login" checkbox and make sure that the FTP computer name is ftp.nai.com/pub/antivirus/datfiles/4.x. If not, you can click the Default button.

The next step is to click the Schedule button. In the Schedule dialog box first click the "Enable scheduler" checkbox and either click the "At Startup" radio button or choose a time you would like to schedule the update. Once a week is a good choice. Click OK.

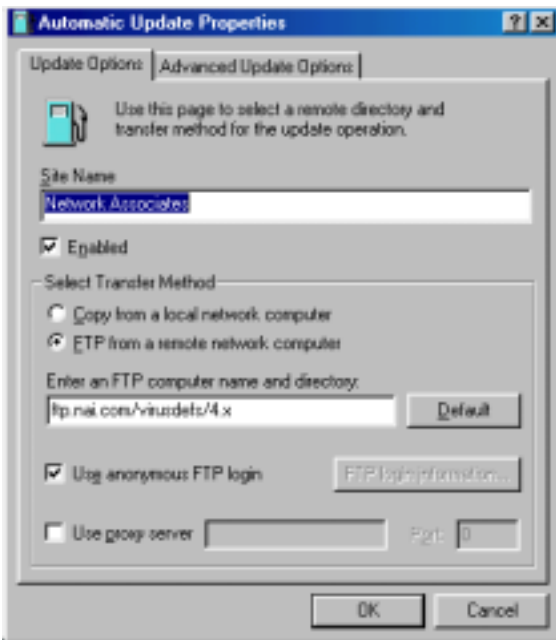


Tricks & Tips

& Tricks



On Windows 95 and 98 go to the Start menu and select Programs/McAfee VirusScan/McAfee VirusScan Scheduler. Double-click AutoUpdate.



In the Task Properties dialog box click the Configure button. Select Network Associates and then click the Edit button. Click the “Enabled” checkbox and the “FTP from a remote network computer” radio button. The FTP computer name should be ftp.nai.com/virusdefs/4.x. If not, you can click the Default button. Click the checkbox labeled “Use anonymous FTP login” and then click OK to go back to the Task Properties dialog box.

The final step is to click on the Schedule tab. Click the Enable checkbox and then pick a schedule time. VirusScan for Windows 95 and 98 does not have the option to update automatically at start up,

so you'll need to choose a day and time of the week that will work for you. Click OK.



Another important step in setting up VirusScan is telling the software which files you want it to scan. On Windows NT simply right-click on the VirusScan shield icon in the lower right-hand corner of your screen and select Properties. In the Properties dialog box select the option you want.

On Windows 95 and 98 select Programs/McAfee VirusScan/McAfee VirusScan Scheduler from the Start menu. Double-click McAfee VShield and click the Configure button. Click the Wizard button and go through the steps. 🐱

QUESTIONS *and* ANSWERS

Q: The date on my Palm Pilot is not advancing correctly. Is my Palm Pilot broken?

A: Some Palm V and Palm IIIx organizers can experience this problem. Usually it is caused by a low battery. Recharging the battery on the Palm V or replacing the batteries on the Palm IIIx followed by performing a soft reset often fixes the problem. To perform a soft reset use the reset tip tool (unscrew the metal barrel from the stylus quill of your stylus) or the tip of an unfolded paper clip to gently press and release the button inside the reset hole on the back of the Palm Pilot.

If this doesn't solve the problem you may need to perform a hard reset. For instructions you can visit the Palm Web site at <http://www.palm.com/support/helpnotes/hardware/dateadvanceprob.html>.

Q: My spouse and I both have email accounts and want to use Eudora at home to check our mail. How do we setup Eudora so that our email is kept separate?

A: Normally when you configure Eudora with your email account information, Eudora retrieves email from that account and downloads it into your Inbox. Your Inbox and other mailboxes are stored inside the Eudora directory. In order to have multiple users on the same PC or Macintosh you'll need to create separate settings files and email directories for each user.

On the PC first quit Eudora. Create a new mail directory for the second user. You can name this directory whatever you like and it can be located wherever you

like. Inside the original Eudora mail directory you'll find a file called eudora.ini. Make a copy of this file and put it into the new mail directory. Then for each user create a shortcut to the Eudora executable (eudora.exe). You can put these shortcuts on the desktop and rename them to reflect each user's name (e.g. Jane's Eudora and Bob's Eudora). Right-click on the shortcut for the new user and select Properties. Click on the Shortcut tab and in the Target field, add the path to the new user's eudora.ini file. Finally, double-click on the new user's shortcut and, before checking mail, select Tools/Options and change the account information to reflect the new user's email account.

On the Macintosh first quit Eudora. Open the System Folder on your hard drive and create a new folder inside the System Folder for the second user. You can name this folder anything you like. Locate the Eudora folder inside the System Folder and double-click it to open it. Find the Eudora Settings file and make a copy of it (Command + D). Drag the copy into the new folder you created and change the name of the file back to Eudora Settings. In order for this to work you must launch Eudora by double-clicking the Eudora Settings files instead of the Eudora application file. The best way to do this is to create aliases to each of the Settings files and place them on the Desktop or in the Apple menu items folder in the System Folder. Rename the aliases to reflect each user's name. Finally, double-click on the alias to the new user's Settings file to launch Eudora and change the email account information for the new user by selecting Settings from the Special menu. 🐾