Computer intrusions and attacks

Many library computers are now connected to each other through networks and to the rest of the world through the Internet. Current information of unprecedented scope and scale is now available on the computer screen. There is, however, a dark side to all this computer interconnectivity, since it increases the possibility of deliberate unsolicited intrusion into library computers.

When such an intrusion occurs, it may come in the form of a computer virus playfully invented by some computer hacker, or it may come as an uninvited e-mail message from an eager online salesman. There are even some spiteful, vengeful, paranoid attackers who aim to cause destruction. Some intrusions can damage valuable computer-stored information; others may simply divert the attention of a computer user. Protective measures should be taken to avoid some intrusions; others can simply be ignored. In this article, we take a look at some frequently encountered computer intrusions.

1. Viruses

A computer virus is a computer program that can reproduce itself and may cause undesired effects in computers where it is active. For example, a virus may simply pop up a window containing unkind words, or it may destroy files stored on the computer's hard drive.

To do its malevolent work, the virus program has to run (execute its code). Usually viruses are located together with other code that is likely to be executed. For example, the virus could be placed in a disk with code that must be executed whenever the disk is started up. When the disk code is executed, the virus is also activated.

A virus may also be attached to a macro. Macros are programs that can be executed in word processors, spreadsheets and other packages whenever a document is opened. When a word processing document infected with a macro virus is received and opened, the infection can immediately affect not only word processing at that computer, but also the operation of the entire system. As long as the virus is active on the computer, it can copy itself to other files or disks when they are used.

Viruses are frequently spread via floppy disks or other media that users can exchange, or in software obtained from untrustworthy sources. Although it is impossible for a virus to exist in normal e-mail text, viruses can be spread via e-mail because the virus can be carried in a file attached to the e-mail, and the virus spreads when the file is opened.

2. Worms

A worm is a type of virus that does not change any existing program or file to spread itself. Instead, it makes copies of itself within an infected computer and spreads to become active on other systems. The latest example of a widespread worm is AutoStart 9805, which affects certain types of MAC computers. This particular worm can be transmitted via almost any disk, including floppy disks, most removable cartridge drives, hard disks, and even disk images. The worm also spreads across networks.

Infected disks contain an invisible application file in their root directory. When the infected disk is mounted on a suitable MAC system, the worm is automatically launched. It then copies itself to the extensions folder of the active system and changes the name of the copy to 'Desktop Print Spooler'. The worm file is invisible, and when running is not shown in the applications menu.

The AutoStart worm is able to corrupt certain graphic files. It is intentionally destructive, overwriting portions of the files with random data. This damage is not repairable, so the files must be reinstalled or restored from a backup. The response of antivirus vendors to this worm has been reasonably rapid. Nevertheless, the worm has created serious problems even without unleashing its full destructiveness. In 1998-99, several companies that use MACs for graphic applications in the St Louis area spent thousands of dollars to clean out the AutoStart worm.

3. Java applications

Java is a computer language designed to run on virtually any computer. You may have heard that programs called applets, written in the Java language, cannot be used to spread viruses. That appears to be true. However, in addition to applets, the Java language can also be used to write application programs and these can carry virus infection. For example, when a Java application program infected with a virus known as Strange Brew is run, it looks for other, uninfected Java files in the computer's directory. The virus then copies itself into these files, modifying them so that, when they are run, the virus will take control. This virus can cause damage to some of the files it infects so that they no longer run properly.

4. Trojan horses

Sometimes called vandals, trojan horses are pieces of computer code that may be downloaded to a computer while Internet sites are being accessed. The code may be in the portable Java computer language or in the equally portable Microsoft

ActiveX language. It may be harmless, but it could possibly delete an important file from the computer, plant a harmful virus, or even steal users' passwords. Unlike viruses and worms, a Trojan horse cannot replicate itself.

Several hundred trojan horses are believed to currently be in circulation, and the number of trojan horses capable of stealing passwords appears to be increasing. When an e-mail password is stolen, the attacker can send out e-mail as if it came from the victim. This makes all sorts of fraudulent schemes possible.

Trojan horses are often sent out as part of programs that Internet users download in hopes of getting better access, free access time, or enhancements for viewing online services. Trojan horses may also be distributed with e-mail. Another distribution method is to embed a trojan horse in a word processing file. When the user opens one of these files, the trojan horse enters the user's computer system. Once inside a computer the trojan horse can access passwords, screen names and other personal information and then distribute this confidential data to the attacker. This kind of attack can be prevented by avoiding any use of programs from untrusted or unknown sources. Programs that have been posted to an Internet newsgroup are particularly risky.

5. E-mail spamming

Spam is unsolicited and unwanted e-mail. It is the Internet equivalent of junk mail. Some e-mail services use filters to screen out spam. These services try to keep track of active spammers' addresses and then exclude any mail from those addresses. This is never fully effective because recalcitrant spammers continue to find new ways to evade these filters, and new spammers are constantly appearing.

If your organisation is using e-mail, and the amount of spam received becomes a problem, there are some steps that can be taken to minimise the spam. For example, you can send polite e-mail asking the spammers to remove you from their e-mailing lists. If that doesn't work, try sending e-mail to the Internet Service Provider the spammers are using. Thus, if the spam comes from mrspammer@themall.net, try sending a polite complaint to abuse@themall.net. Unfortunately, spammers don't always give their actual return e-mail address.

There are some e-mail practices that tend to invite spamming. For example, spammers often raid mailing lists to obtain e-mail addresses for new victims. If you or your organisation are on any mailing lists, and you are experiencing spamming problems, contact the list keepers and inform them of the problem. Remind the list keepers that lists may be kept private or public, but only the public lists can be easily raided for addresses. To avoid spam, give your e-mail address only to those who need to use it. Keep the address out of Internet directories like Four11, WhoWhere, American Directory Assistance, Bigfoot, Internet Address Finder, SearchAmerica, Switchboard and World Email Directory. These services will remove your e-mail address if you request them to do so. However, if your organisation wants to encourage e-mail contact with colleagues and patrons, it may be more important to advertise the e-mail address as widely as possible than to conceal it.

Software that offers some defence against e-mail spamming is available. For example, the Novasoft SpamKiller package ($30 from www.spamkiller.com) comes with a list of 3000 spam sources that it screens from incoming e-mail. The vendor adds new sources to the list via the Internet without charge.

By the way, you may want to take care not to become an inadvertent spammer yourself. That can happen if you get in the habit of circulating chain letters, or of overusing the 'reply to all' option of your own e-mail service.

6. Hoaxes

Of the tens of millions of computer users who use the Internet, many are novices who have little knowledge of computers, networks or software and are vulnerable to unfounded hoax rumours. Increasing numbers of virus hoaxes are propagating across the Internet. Hoaxes have become so common that users are more likely to bothered by these false rumours than by actual viruses.

A hoax is typically propagated through a phoney e-mail message that warns of a virus that can accompany e-mail messages and will cause damage to recipients' computers. The message urges users to forward the warning to all their friends and colleagues. In fact, this virus does not exist. However, the hoax message can take on virus-like characteristics as it spreads from user to user via e-mail.

Remember, the only way it is possible for viruses to spread via e-mail messages is through files attached to the e-mail, not through the messages themselves. However, any real viruses are far outnumbered by the growing number of hoax warnings.

7. Cookies

A cookie is a small text file that may be placed in a computer when an Internet site is contacted. The ostensible purpose of a cookie is to facilitate communications between the computer and the Internet site. Thus, a cookie may be used to record items put into a shopping cart at an Internet shopping site, or it may be used to keep track of user preferences at a site that offers choices such as location of weather information.

Internet browsers can be easily set to refuse cookies, or to notify the user before each cookie is accepted.

However, if cookies are refused, users may find it inconvenient to fully access certain sites, and it can be quite annoying to be confronted with cookie notification displays while surfing the Internet.

Cookies can be used to collect information on how individuals use their computers. For example, cookies can record an audit trail of the Internet sites accessed by a computer. Cookies can be used to direct advertising to likely consumers. They can also be used to collect personal information on individual users by keeping and interpreting records of Internet use, and later matching this data to existing public and private database information on the individuals. Information items such as name, address, phone number, health, salary, eating habits and mortgage status have been gleaned in this manner.

8. How much intrusion protection is needed?

E-mail spamming and hoaxes can be annoying and time-wasting, but they appear to offer little threat to basic library operations and can usually be safely ignored.

Cookies seem to be more beneficial than harmful. Cookies may pose a potential threat to some businesses on the Internet, and they are certainly of concern to individuals who use the Internet from their own computers. However, the ability of cookies to monitor Internet use at libraries does not seem to have any threatening implications.

Computer viruses, worms, and trojan horses may indeed pose serious threats to library computer networks because they can spread from one computer to another and may damage files. With increasing amounts of paperwork now performed on library computers, destruction of files can be measured in loss of hours of intellectual and clerical effort. As computer storage assumes its place as one of the regular repositories for library collections, loss of files becomes as important as loss of physical materials. Protection against such losses seems prudent.

9. Virus protection software

Antivirus software can continuously examine all computer activity for signs of viruses, worms and trojan horses. Scanning a large number of files can take a long time so most packages allow antivirus scanning to take place in the background when no other work is being processed by the computer. Antivirus software may also operate in an on-demand mode where users initiate the examination of files for viruses. Most antivirus packages allow the user to define a set of antivirus procedures, save that combination of procedures, and execute them on a schedule set by the user.

Virus protection software can be certified by the International Computer Security Association (ISCA). To receive ICSA certification, packages must detect 100% of the viruses currently known to be publicly circulating.

New viruses appear all the time and the only way to protect against them is to keep your antivirus software up-to-date. Fortunately, most antivirus package vendors maintain Web sites from which their users can download free antivirus updates. Some packages also offer e-mail notification to users whenever they are recommending updates.

9.1. Network antivirus software

When individual computers are protected by antivirus software, a separate software package must be purchased for each computer. However, when computers are connected by a local network, it is possible to purchase network antivirus software that will protect every computer in the network.

When only a few computers are involved, it is probably most sensible to purchase an individual antivirus package for each machine. Single-computer antivirus packages generally cost less than $50 each.

If there are more than a half dozen computers on the network, it probably makes sense to consider a network antivirus package. This may save some money but, even if there is no cost reduction, network packages offer the advantage of central management. With single-computer packages, antivirus operations and updating have to be performed separately at each computer. With the network package, antivirus control and updating can be performed once, at one computer, to keep all the network computers protected.

9.1.1. Command AntiVirus

This package provides automatic notification if a virus infection is found. Discovered viruses are automatically isolated to a quarantine folder and e-mail notification can be specified. Protection from Office 97 macro viruses is provided. Virus protection updates from the vendor's Web site can be received automatically and then installed on users' network-connected computers from a shared centralised directory.

Command AntiVirus allows network administrators to display virus scan statistics and a log of scanning events. Antivirus scans can be set for a single user, a group of users, or throughout the entire network. Groups and users are displayed in a tree view. Scans can also be scheduled by logged-on users for their own machines. Scanning can be set up on a scheduled, on-demand and on-access basis. Specific file types can be included or excluded.

Command AntiVirus for one network server lists for $239 (for NetWare) or $170 (for NT). Also required is Command AntiVirus for user workstations, which lists at $49.95 each. A single-user version also lists at $49.95. The vendor is Command Software

Systems Inc., Jupiter, FL. Tel.: +1 561 575 3200. www.commandcom.com.

9.1.2. Dr Solomon's Management Edition

This is a network antivirus package that provides support and central administration for a variety of different computers connected to a network. Whether the individual computers use Windows 95, NT, 3.1 or 3.11, this package will supply antivirus protection to all of them.

The Dr Solomon central management software is installed onto a Windows NT computer. Computers that are identified as antivirus protected get their updates from directories that store management and antivirus toolkits and components. Remote installation and updating of software on Windows 3.1 computers is handled by supplying a custom computer name for each 3.1 machine when the Management Edition software is installed. Depending on the size and structure of the network there are different strategies for setting up the antivirus software. The user manuals explain the options.

Management Edition gives network administrators a vehicle for installing, configuring and updating antivirus software throughout Microsoft and Novell networks. From the central management computer, the administrator can distribute antivirus software, make updates, receive antivirus event messages, and schedule antivirus events for the individual network computers.

Dr Solomon's Management Edition prices are: 10 nodes, $1159; 25 nodes, $2843. In other words, about $115 per user. Single-computer versions list at $39.95 to $69.95. The vendor is Dr Solomon, www.drsolomon.com.

9.1.3. eSafe Protect

This package is designed to control viruses, trojan horses, Java applets, ActiveX controls, and even modem dialler intrusions that can dial unwanted long-distance numbers. eSafe lets Java applet and ActiveX control programs enter the computer but they are isolated in a protected area on the hard disk called a sandbox. eSafe then runs the programs and checks their activity to determine whether they may cause harm. eSafe has compiled a list of untrustworthy Internet sites, and users can add to that list. The package will prevent contact with sites that appear on the untrustworthy list. The package can also stop selected words from being accessed. The eSafe manual is an Acrobat file that can be downloaded from the eSafe Web site. The manual provides step by step instructions on configuring the package for individual needs. The package also comes with a well-organised and useful help file.

One shortcoming is that real-time scanning for viruses is difficult to disable. eSafe lets users scan drives and folders on demand but not individual files. Groups of files can, however, be selected by file type and then scanned. Also, groups of files can be excluded. The vendor's Web site makes monthly updates to the package available.

A network version of the package with automated network deployment and management is available at prices starting at $49.95 per user for up to 10 users. A single-user version of eSafe lists for $49. The vendor is eSafe Technologies Inc., Seattle, WA. Tel.: +1 206 524 9159. www.esafe.com.

9.1.4. InocuLAN

With this antivirus package, users can select any combination of drives, folders or files for scanning. There is detailed control over which items are to be excluded from scanning. Regularly scheduled scans are set up with the help of a wizard. The software detects many virus types, including macro viruses. Files found to be infected can be moved into a quarantine area where they can be safely examined, and files in this area are excluded from antivirus scans, so they will not trigger further alarms. Level of protection can be set by clicking on a button. When any virus infection is detected, the package automatically goes to the highest level of protection.

The network versions of this software allow for Windows-based grouping of servers and workstations. The software keeps a virus scanning history, including files checked, viruses found, responses taken and updates. InocuLAN is available for Windows NT and NetWare servers and Windows 3.x, Windows 95, Windows NT, DOS and Macintosh workstations.

The list price for InocuLAN for a single computer is $69.For network workstations the price is about $40 each. Versions for network servers are more expensive. The vendor is Computer Associates International Inc., Islandia, NY. Tel.: +1 516 342 5224. www.cai.com/cheyenne.

9.1.5. McAfee NetShield for Windows NT

This package detects virus-infected files moving to and from an NT server to prevent viruses from spreading through the local network. When an infected file is detected, it is automatically logged and either isolated or deleted. NetShield displays provide point and click administration of virus scanning tasks, including notification and reporting.

NetShield for Windows NT lists at $190, for use with 10 nodes. The single-user version lists for $49. The vendor is Network Associates Inc., Santa Clara, CA. Tel.: +1 408 988 3832. www.networkassociates.com.

9.1.6. Norton AntiVirus

This package has an on-demand virus scanner that

lets users control the scan using many options. Folders, file types and individual files can be included or excluded. Within a safe environment for starting program files, Norton AntiVirus uses a search technology from IBM to locate virtually any virus-like files. A scan and deliver feature lets users e-mail a safely wrapped virus to Symantec's AntiVirus Lab. In many cases the process is automated, so the response can be 30 minutes or less. Also in this version, users can incrementally update virus definition files with new information from Symantec, but free updates are limited to a year. After that, an annual subscription to updates costs $4.95. The package comes with a scheduler that automates the updating process. Running of programs and virus scanning can also be scheduled.

NT server, NT workstation and Windows 95/98 versions of Norton AntiVirus each list for $39.95 The vendor is Symantec Corp., Cupertino, CA. Tel.: +1 541 334 6054. www.symantec.com.

9.1.7. Vet AntiVirus

Vet performs rapid antivirus scanning. Users can select as many folders and files for scanning as they see displayed in the current Windows Explorer display. The package scans either all files or only selected file types. It has no scan scheduling capability and it checks files only as they open and close. Users must perform occasional full scans manually in order to ensure the safety of their systems. Vet detects and cleans conventional file and boot sector viruses as well as macro viruses. Vet AntiVirus lists for 595 Australian dollars for one network server (NT, NetWare or DEC Alpha). The list price for workstations is 99 Australian dollars. The vendor is Cybec Pty Ltd, Melbourne, Victoria, Australia. Tel.: +61 3 9825 5600. www.vet.com.au.

9.2. Single-user packages

9.2.1. Guard Dog Deluxe

This package keeps computers from downloading ActiveX controls, Java applets, cookies and viruses. It has an interface that makes it very easy to use. A single dialogue box provides for the available set-up options, which are explained briefly yet clearly. It is easy to determine and select the precise level of protection that is desired and the package alerts users to any downloaded program that exhibits any suspicious activity. Users can schedule virus checks automatically for specific file types. There is a cookie-blocking module that allows users to selectively accept cookies only from trusted or useful sites and reject all others. There is a feature that automatically blocks search requests entered at popular search engines from being forwarded to other sites that track such behaviour. Another feature alerts the user whenever a program attempts to connect to the Internet. The package will clean out the browser's cache, and the list of sites visited, and the history file of Web pages.

Guard Dog Deluxe is priced at $59.95. The vendor is CyberMedia Inc., Santa Monica, CA. Tel.: +1 310 664 5000. www.cybermedia.com.

9.2.2. Integrity Master

Most antivirus packages operate by identifying the various viruses that are known to be in circulation. Integrity Master takes an entirely different approach, based on the characteristics of the files that are stored on the computer. During installation, this package scans all files for viruses. If none are found, the package sets up a coded description of each stored file. Any change to a file will alter this signature. If the signature changes unexpectedly, this alerts the package to possible infection or tampering. This approach not only detects changes due to viruses, but it can also discover file changes that may be due to other types of invasions, or even due to hardware malfunctions. The package generates detailed reports that list all changed files and the errors found by the package, along with possible reasons for these errors. The Integrity Master manual includes considerable material on viruses and the strengths and weaknesses of various antivirus approaches. Unfortunately, this package is unable to remove the viruses it finds. Although it is intended for PCs, it does not function smoothly under Microsoft Windows.

The list price for Integrity Master is $49.50. The vendor is Stiller Research, Colorado Springs, CO. Tel.: +1 719 533 1879. Fax: +1 719 533 1728. www.stiller.com.

9.2.3. ThunderByte

Users of this package can define antivirus scanning to cover the boot disk drive, all local hard disks, all CD-ROM drives and all drives on an editing screen. However, the package does not allow users to schedule scanning in advance. ThunderByte Anti-Virus Utilities list for $99. The vendor is NovaStor-Authentex Software Corp., Kanata, Ontario, Canada. Tel.: +1 613 930 4444. www.authentex.com.

9.2.4. Panda AntiVirus

This package has a scanning system that can examine an entire hard disk in a few seconds. Panda detects more than 13,000 viruses. It scans compressed files, and it detects and removes viruses. The vendor provides updates and a hotline service. The package uses a heuristic scanning method that is said to be capable of detecting new viruses not yet recognised by conventional scan systems. Panda's virtual driver feature oversees file traffic, and it can detect viruses while the user performs other tasks. Panda AntiVirus sells for $45 to $100. The vendor is Panda Software. Tel.: +1 415 392 5950. www.pandasoftware.com.