

An Introduction to Viruses and Malicious Code, Part Two: Protection

Brad Griffin 2000-12-27

An Introduction to Viruses and Malicious Code Part Two: Protecting Your Computers and Data

by Brad Griffin gryphonn@austranet.com.au

last updated Dec. 27, 2000

In [part one of this series](#), we introduced you to viruses and other forms of malicious code. We discussed the various ways in which viruses can enter your computer and how they can affect your important data. We will now cover ways in which you can help prevent a virus 'attack'. This is not another 'how-to use an anti-virus program' article; rather, it is intended to be a base reference for you to develop a safe computing policy for your business. The third and final installment in this series will discuss what to do in case of an infection.

Invariably, the weakest link in the security chain is the human link. Safe computing habits are the best defence against malicious code. How you handle e-mail attachments, floppy disks, CDs and other external media can mean the difference between a clean computer and an infected one. Likewise, the way you set up your chosen anti-virus software will determine whether it detects a virus, or completely bypasses an infected file. Furthermore, the installation of unnecessary software on a computer can provide an entry point for malicious code.

Anti-Virus Programs

Anti-Virus software is an absolute must. However, just having anti-virus software is not enough. First and foremost, individuals should purchase a quality anti-virus program that is appropriate for their system. If your present budget prevents you buying an anti-virus application, you can download a free anti-virus program from a number of vendors on the World Wide Web. It should be noted that most of these products are free for personal use only and should not be used in a business environment. Whatever their situation, users should purchase the most comprehensive package their budget will allow. Remember, this software is the primary defence against data loss as a result of malicious code. Don't settle for second-rate software.

Users should conduct thorough research in order to obtain the best anti-virus package for their needs, taking into account the vendor's reputation and how the software rates in independent

anti-virus testing. They should also seek the opinion of people who do not have a vested interest in any particular software package. Resources for objective information include newsgroups such as [alt.comp.virus](#) and mailing lists such as SecurityFocus.com's [Security-Basics list](#). There are also organizations that conduct regular testing of anti-virus products. The following sites may assist buyers in the decision-making process:

- [Virus Bulletin](#)
- [ICSA Anti-Virus Lab](#)
- [West Coast Labs](#)

Choosing Anti-Virus Software

When choosing anti-virus software, users should look for two key functionalities: real-time scanning and virus updates.

Real-Time Scanning

Real-time scanning means the software will automatically run in the background on an ongoing basis, monitoring and checking files as they are opened or executed, and in some cases, checking e-mail as it is downloaded. Some products check files and directories when they are opened through Windows Explorer.

Virus Updates

The only good anti-virus program is an up to date anti-virus program. Look for a product that offers daily updates. Users should only buy anti-virus products whose vendors offer free updates from their web-sites. It is also vital that the software is updated regularly, depending on the size of the network and the amount of traffic that utilizes it, this could mean daily updates for small to mid-size offices or weekly updates for small offices or home offices, or for family or personal computers. With the current explosion in macro and script-based viruses, updates that address the latest threats are essential. Users may also find that while some vendors include updates and/or upgrades as part of the purchase price, others will charge a monthly or yearly license fee for the service.

A number of anti-virus vendors and their products are listed in the relevant links section at the end of this article.

Configuring Anti-Virus Software for Optimal Protection

As with any tool, in order to be effective, anti-virus software must be used properly in order to be effective. Once users have installed their chosen product, you should look at the configuration options and modify them to ensure the product will do a thorough job of scanning for viruses. Some products have a default list of file types that are automatically scanned that may not provide optimum protection. Adjust the settings to scan **all** files. Also, ensure that real-time scanning is enabled by default. Further, if the anti-virus product gives you the option of creating a recovery/reference/cure disk, do so. Don't pass them off because it slows down the installation process, because these disks could become your only hope of recovering from a virus infection in the future.

Finally, 'Read the Manual'. This may sound obvious, but it is essential that you get to know your anti-virus program. Most products have advanced options and configurations that will not be understood without reading the details.

Methods of Infection

In order to know how to prevent infection, it is necessary to know how viruses are spread. Traditionally, viruses have been spread by e-mail. However, as viruses are becoming more complex, their methods of infection are diversifying.

E-mail Attachments

If you or your organization use e-mail, you will most likely receive a virus-infected message or attachment at some stage in the future, if not already. The vast majority of malicious code is passed on via e-mail; therefore, it is most important to develop safe e-mail handling practices. In order to minimize the possibility of infection, it is recommended that users take the following steps in handling e-mail:

1) Create a Quarantine directory

Create a directory and save any e-mail attachments you receive into that directory. This can be your 'quarantine' folder. The purpose of the quarantine folder will be explained shortly.

2) NEVER open the attachment immediately.

Do you know who the sender is? If not, delete it. Don't be tempted to open it. It may merely be a sales brochure from a potential supplier. However, are you willing to take the chance that it could be a virus or worm? If you do not know the sender, delete the e-mail immediately.

If you know the sender, were you expecting an attachment from them? In other words, did they inform you that they would be sending you an attachment? Many viruses and worms spread by infecting a victim's address book and forwarding itself to all the contacts listed in the address book without the victim's knowledge. In this way, your spouse, parents or best friend may have sent you an infected e-mail without their knowledge. For this reason, you must not assume that because the source of the e-mail is trusted that the e-mail itself is to be trusted. As a general rule, never open an attachment that you have not specifically requested or that a contact has not notified you about in advance.

3) Determine what type of file the attachment is prior to opening it.

There are many file types that can carry malicious, 'executable' code, such as those with the suffix .doc, .xls, .ppt, .com, .bat, .pif, .vbs, .shs, and .exe. These are just a few of the many file types that can carry dangerous code. (For a more thorough coverage of infectable file types, see 'Infectable Objects' in the Focus-virus pages.)

Do NOT open ANY attachment without first checking it for known viruses. Save the attachment to your 'quarantine' folder. Use your anti-virus software to scan the attachment. If you are still unsure of the attachment after your scanner has given it the all-clear, contact the sender and ask them if they sent the attachment and that they are aware of the contents.

Vulnerabilities in E-mail Clients

While attachments are the primary source of e-mail infection, they are not the sole culprit. Some e-mail clients contain programming weaknesses known as vulnerabilities that will allow malicious code to run when the user merely reads an e-mail message. The Kak worm has been around since mid-1999; however, it is still the most prevalent piece of malicious code on the Internet. Users of Microsoft mail software such as Outlook must ensure that they have the latest security updates for this software, this is generally available at:

<http://www.microsoft.com/technet/security/bulletin/ms99-032.asp>

Non-Essential Software

Non-essential programs can act as pathways for virus infection. Accordingly, in a business environment, it is good practice to restrict the programs that the employer permits to be installed on a system. This simply allows systems administrators to ensure that the programs that are installed on a system are not vulnerable to infection. Of course, it may happen that programs that are installed on the system may still be vulnerable, but if the system administrator is aware of the presence of those programs he or she can take the necessary steps to minimize the risk of infection.

Messaging Programs

Instant messaging and 'chat' software such as Mirabilis/AOL's ICQ, AOL Messaging, Microsoft Chat, Internet Relay Chat (IRC) clients and others allow for transfer of files and documents and as a result, may allow viruses or other malicious code to circumvent AV software or user scrutiny. Many Internet worms use IRC software to spread their code. If this type of software is not necessary for your business operations, do not allow users to install it. It is a good idea, as part of the development and implementation of security policy to make clear to users - employees, etc - that they are not to download or install any non-essential or non-approved software. It should be explained that this is not to limit their activities, but to limit the opportunity for potentially damaging intrusion, attack or infection.

Remote Access Applications

There are commercial applications that allow you to manage your computer systems from remote locations. Symantec's PC Anywhere, Laplink 2000 and the free VNC application allow you to operate a remote computer as if you were sitting at the computer itself. These programs are essentially legal Trojan horse programs, which means anyone could use the same software to take control of your computer or a computer on your network and/or upload malicious code to your computers. If you find a need for this type of software, ensure you use strong passwords and restrict access only to those who need it.

Floppy Disks

All computer users should be aware that floppy disks from outside sources are potential virus carriers. All floppy disks and CD ROMs should be scanned for viruses prior to accessing any files on the disks. Consider any outside media as potentially infected.

As we discussed in the first article in this series, boot sector viruses can be particularly troublesome. One way to reduce the risk of an infection by these viruses is to change the boot order of your computers. Normally, a system is set to first check the floppy disk drive (drive A) for boot information before checking the main 'C' drive. In order to do this, you will have to go into your initial, BIOS settings. This is usually done by pressing one of the function keys (F1, F2 etc) or the 'delete' key when your computer is just starting up (a message 'Press (key) to enter set-up' is typically shown at the bottom of the screen). When the system enters the set-up options, look for the 'boot options' menu and change these so that the hard drive is checked first.

Don't forget to save the settings when you've finished. If you ever need to boot from a floppy disk, you will have to change these settings again. Some computer suppliers build in automatic password protection on the BIOS settings. If this is the case for you, contact your computer manufacturer or supplier for assistance.

User Education and Awareness

Viruses and malicious code are created and spread at an alarming rate. In order to effectively defend your systems, you need to be aware of the latest threats and security issues so you can take protective measures to avoid becoming a victim. Don't rely on standard media (newspapers, television etc) to alert you to virus threats. They are usually at least a week behind when reporting a problem and usually report only when the damage has been done. Most mass-media outlets ignored the 'Chernobyl' virus until after it had damaged thousands of computers worldwide. This time lag can be overcome by updating your software regularly and by checking virus and anti-virus sites daily for frequent updates. Many anti-virus programs make this task easier by having an application included in the program that will allow you to check for updates 'on-demand' when you are connected to the Internet.

If your anti-virus vendor offers an alert notification service, subscribe to it. Check other vendors to see if they have an alert list as well. Some anti-virus developers will release warnings ahead of others and therefore, it may be good practice to subscribe to a number of lists. Microsoft offers a security bulletin mailing list as well. Subscribing to this list will allow you to stay on top of security related patches and could prevent problems such as falling victim to the previously mentioned Kak worm. You can subscribe to the notification service here:

<http://www.microsoft.com/technet/security/notify.asp>

SecurityFocus.com offers a number of security-related mailing lists which can help you stay on top of virus and related issues. See <http://www.securityfocus.com/virus> for further details.

Remember, you are responsible for the security of your computers. You should be aware of the latest virus threats so you can implement preventative measures before you become a victim. If you run a network in your household or business, or if many users share the same computer, you should implement regular user education sessions so that everyone in your computing environment becomes aware of the risks of viruses and malicious code. You will find that once you have an education program and a well thought out computing policy implemented in your workplace or home, that infections from malicious code will be very rare to non-existent.

Security Policy

A key component in user education is the development of a security policy. No matter how good the anti-virus software you implement on your system is, if the users are not aware of the risks posed by viruses, their behaviour can counter the strengths of the most effective software. For this reason, it is vital that security policies be developed. Every company and even families should take the time and effort to develop and implement a comprehensive security policy so that users are made aware of what the risks are of infection, and the best ways to avoid infection. A security policy can outline some of the issues that this article has touched upon, such as proper use of computers, acceptable use of computers, what programs are acceptable to install on a computer and how users should handle e-mail and external media. As we shall see in the next instalment of this series, a security policy should also educate users how to recognize a potential virus infection and what steps can be taken to remove the virus and limit the damage that it causes.

Conclusion

Computer viruses are a fact of life in today's Internet connected world and every day, the risk of falling victim to some type of malicious code increases. However, if you take proper precautions such as using quality anti-virus software and keep it up to date, treat all outside files with suspicion and implement user education sessions and policies in the workplace/home, your risk of infection will be greatly reduced. Further, if you are well prepared for a possible infection, recovery will be far easier, as we shall see in the next installation of this series.

Remember, as the old saying goes: prevention is the best cure - especially for computer

viruses.

To read **An Introduction to Viruses and Malicious Code, Part Three: Detecting and Resolving Virus Infections**, click [here](#).

Relevant Links

For more articles and information on viruses, please visit the [SecurityFocus.com Virus focus area](#)

Links to Anti-Virus vendors

[Aladdin Internet Security](#)

[Alwil Software](#)

[Computer Associates](#)

[Command Software Systems](#)

[F-Secure Corporation](#)

[AVG Anti-Virus - Personal](#)

[AVG Anti-Virus - Commercial](#)

[Kaspersky Labs](#)

[MacAfee Anti-Virus](#)

[Network Associates International](#)

[Sophos Anti-Virus](#)

[Symantec \(Norton\)](#)

[Trend Micro](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus