THE CUTTING EDGE

(Editor's Note: This quarterly column is compiled by JCO Technology Editor Ronald Redmond. To help keep our readers on The Cutting Edge, Dr. Redmond will spotlight a particular area of orthodontic technology every three months. Your suggestions for future subjects or authors are welcome.)

This month's Cutting Edge article examines an area of increasing importance in today's orthodontic world: the preservation of our practice data. Drs. Ameet V. Revankar, Narayan H. Gandedkar, and Sanjay V. Ganeshkar take an in-depth look at "malware", a term comprising all types of program code that attempt to render our data and computers useless. Attacks by this form of cyberterrorism are growing exponentially, usually aimed at stealing protected information such as financial records or disrupting access to your practice data, thereby compromising your patients' care and your own well-being.

I commend the authors for attempting to use language that will be understandable by most computer owners. Still, this technologically advanced article may not be an easy read, and I encourage you to take the time to go through it twice. By the second time you read it, I hope the true purposes of firewalls and antivirus software will become apparent, and the efforts you have expended in updating your computer protection daily will have a greater perceived value. Guarding your data against assault is no easy task, and the difficulty continues to increase. This is a fight we must be determined to win!

W. RONALD REDMOND, DDS, MS

Securing Your Digital Data Against Computer Threats

Computer technology has come to permeate all aspects of orthodontic practice. As patient records have moved from paper to electronic form, the means of storing and protecting them have also evolved. Maintaining the integrity of electronic data is now crucial to the success of any orthodontic office.

Unfortunately, threats to data security have become increasingly complex. The expansion of the Internet has brought an explosion of "malware"—software that can corrupt data and damage files, including those that are critical to the operating system. Infection with malware is the most common cause of electronic data loss. The present article describes a variety of techniques for securing your data against this growing threat.

Types of Malware

"Malware", a portmanteau term combining "malicious" and "software", refers to various forms of hostile, intrusive, or annoying software or program code, some of which can cause catastrophic


Dr. Redmond


Dr. Revankar


Dr. Gandedkar


Dr. Ganeshkar

TABLE 1
PRODUCTS AND PROGRAMS MENTIONED IN THIS ARTICLE

AV-Comparatives, Innsbruck, Austria; www.av-comparatives.org.

CCleaner, Piriform Ltd., London, England; www.ccleaner.com.

Computer Hope.com, West Jordan, UT; www.computerhope.com/issues/chsafe.htm.

Data Recovery Doctor, Pro Data Doctor; www.datadoctor.in.

ESET NOD32 Antivirus for MS-DOS, ESET, San Diego, CA; www.eset.com.

HijackThis, Trend Micro, Cupertino, CA; www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis.

Ice Sword, XFocus; www.antirootkit.com/software/IceSword.htm.

Knoppix, Knopper.net, Schmalenberg, Germany; www.knoppix.com.

Recover My Files, GetData Software Development Company, Hurstville, NSW, Australia; www.recovermyfiles.com.

Stay Safe Online, National Cyber Security Alliance, Washington, DC; www.staysafeonline.info.

Stinger, McAfee, Santa Clara, CA; http://vil.nai.com/vil/stinger.

Symantec, Cupertino, CA; http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym.

The Live CD List, FrozenTech, Santa Barbara, CA; www.livecdlist.com.

Ubuntu, registered trademark of Canonical Ltd., London, UK; www.ubuntu.com.

USB FireWall, Net Studio; www.net-studio.org/application/usb_firewall.php.

USBAntiVirus International Inc.; www.usbantivirus.net.

Windows CleanUp!, Steven Gould, Dallas, TX; www.stevengould.org.

Windows, Microsoft Corporation; www.microsoft.com.

computer failure and data loss if appropriate and timely action is not taken.[1] The term "computer virus" is often used by the layperson to refer to all types of malware. Technically, however, although all viruses are malware, the reverse is not true. Some of the newer forms of malware include rootkits, Trojan horses, keyloggers, spyware, and dishonest adware.

A rootkit is a type of malware designed to take control of a computer system ("root" access in Unix; "Administrator" access in Windows) surreptitiously and without the system owner's authorization. A Trojan horse is a form of malware disguised as a legitimate program, such as a screen saver, that, upon installation, installs other components to allow unauthorized, "backdoor" access to the computer. A keylogger is an application designed to record the keystrokes made on the machine on which it is installed. Keyloggers are used by law enforcement for surveillance, but they are also used illegally to obtain passwords and encryption keys. Spyware and dishonest adware are privacy-invasion programs that were originally designed to secretly monitor behavior such as Web browser activity. These types of malware can now install additional software, redirect Web browsers to potentially dangerous sites, or divert advertising revenue to third parties. Spyware can also change computer settings, resulting in reduced connection speeds, unwanted pop-up advertisements, and loss of access to the Internet or other programs.

A preliminary report issued in 2008 by Symantec, a leading manufacturer of security software, stated that "the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications".[2] According to F-Secure, another provider of Internet security services, "As much malware was produced in 2007 as in the previous 20 years altogether."[3] Malware's most common pathway from criminals to users is via e-mail and the Internet.[4] In an institution such as a dental school, malware can spread rapidly, even to non-networked computers, through the use of flash drives to transfer data. This is the most common pathway at our school for the spread of malware infections.

Protecting Data from Malware Infection

Orthodontic practices can take several steps to prevent infection by computer viruses and other malware, as outlined below.

Address Operating-System Bugs

Most operating systems contain "bugs" or vulnerabilities that can be exploited by malware. A typical example is a "buffer overrun", in which an interface designed to store data in a small area of memory allows the caller to supply too much and then overwrites its internal structures. A piece of malware may take advantage of this situation to force the system to execute its code.[1] Therefore, the first line of defense against malware is to "immunize from within"—that is, to rectify the inherent vulnerabilities of a computer's software, especially the operating system. The easiest and most effective way of patching these holes in a Microsoft Windows operating system is to activate the "Automatic Updates" feature (Fig. 1), which allows the PC to automatically download and apply any critical updates to the software.

Use an Anti-Malware Security Suite with Proper Firewall Configuration

The second line of defense is an integrated anti-malware suite consisting of antivirus and anti-spyware programs, along with a firewall. Many such security suites are available, including both

Fig. 1 Activating "Automatic Updates" in Microsoft Windows operating system.

freeware and subscription software. Try to select one that not only identifies actual malware, but has a low rate of false positives; some anti-malware suites will flag legitimate programs as malware, especially other security software such as rootkit revealers. In addition, the suite should not consume too much system memory. An independent anti-virus-testing website like AV-Comparatives can help guide your decision (Table 1). Such programs can be effective, however, only if the "virus signature" database is frequently updated, since new forms of malware will precede the virus-definition updates in the security suite.

The firewall is an important component of any anti-malware suite. A firewall is a dedicated machine or a software package that inspects network traffic passing through it and uses a set of rules to permit or deny passage. To be effective, the firewall must be configured to the "interactive" rather than "automatic" mode. This prompts a pop-up window to open each time an application attempts to connect to the Internet. The user can then decide whether to allow or deny the connec-

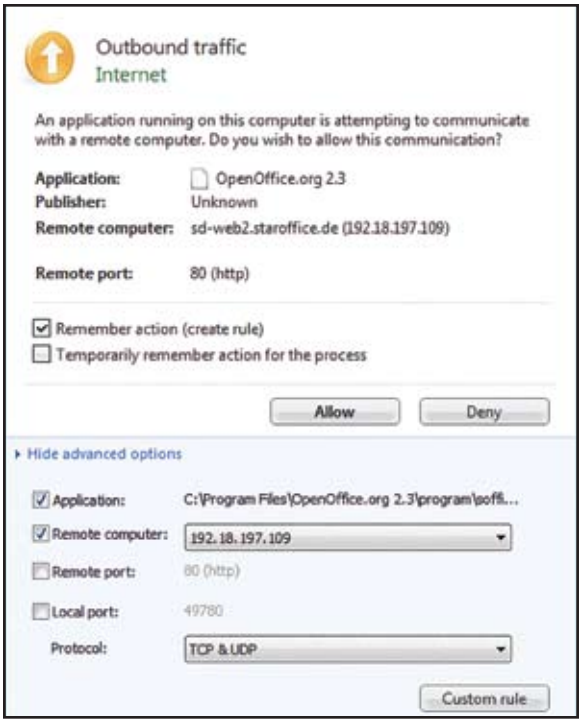


Fig. 2 Pop-up box allowing user to permit or deny connection to parent website of OpenOffice.org program.

tion (Fig. 2). The firewall can be set up to remember previous decisions regarding a particular application, so that the user does not have to repeat the instructions each time the application is opened. Even if a piece of malware such as a keylogger has been successfully installed on a computer, the firewall can prevent it from transmitting any information to its author, thus rendering it useless.

Use a Limited Account on the Internet

No security-software suite can provide total immunity to malware, even if the database of virus definitions is kept up to date. In the high-risk environment of the Internet, vulnerability can be reduced by using a restricted, limited, or standard user account with a software-restriction policy in force, rather than a full-privilege system-administrator account.[5] In other words, log in to your administrator account only when performing administrator functions.

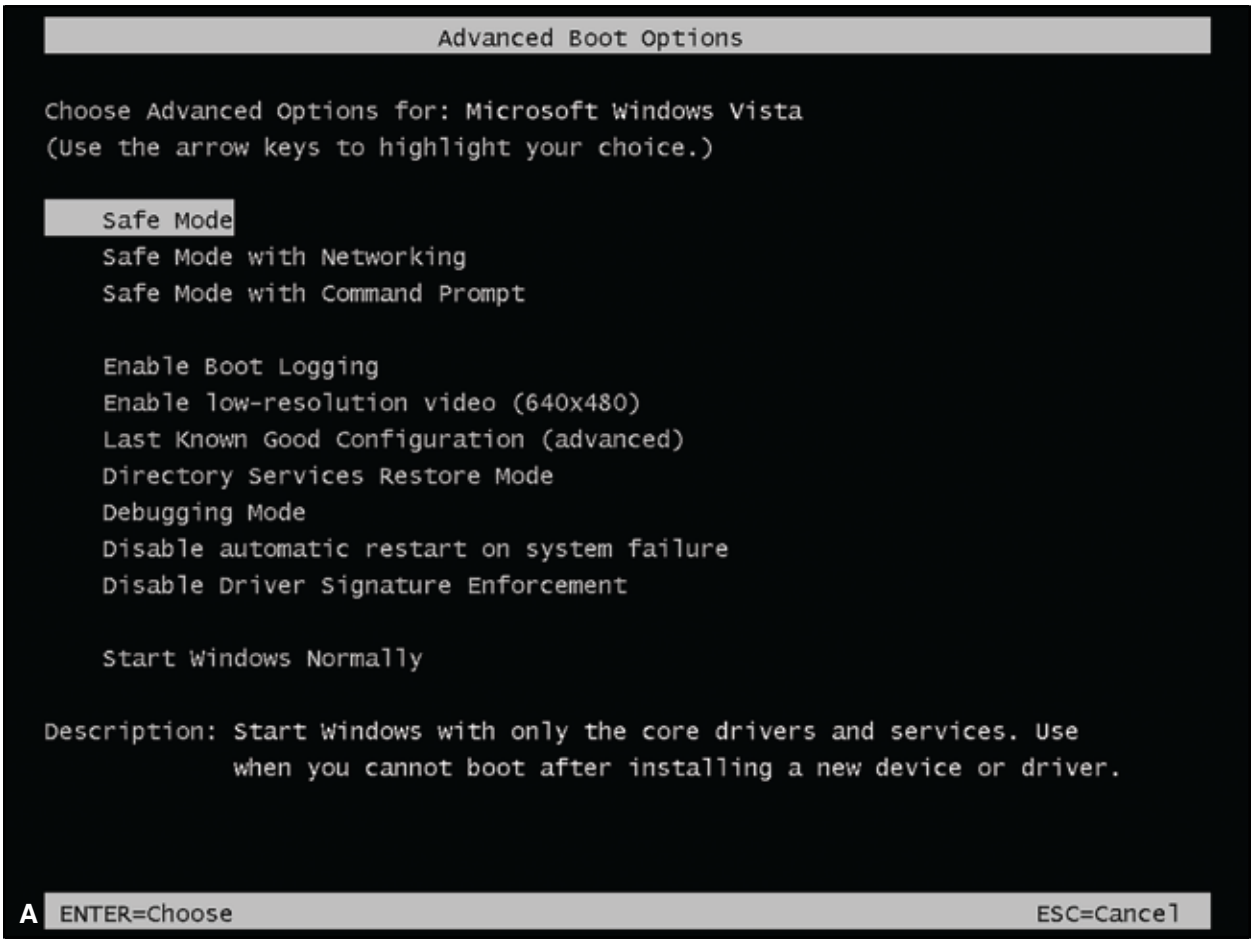
Restrict Auto-Launching of Code from Removable Drives

To reduce the security risk from the use of flash drives, you can install software that restricts automatic launching of all code from removable drives. This is the basis of software such as USB FireWall and USB Drive Antivirus, which can also protect non-networked computers from "in-the-wild" threats because they work according to a set of rules rather than signature updates. These programs are applicable to all "write-allowed hot" removable media, including flash drives and removable hard disk drives. They may not be applicable to "cold" media such as compact discs, but the risk of malware transmission by CDs and DVDs is lower because data must be actively written onto these media using "writer" software and hardware. In contrast, data transmission to flash drives occurs as soon as the drive is connected, whether the connection is authorized or not.

Practice Safe Internet Behavior

Regardless of the quality of your security software, the more contaminated the environment, the higher the risk of infection. Because the risk is nowhere greater than on the Internet, safe Internet behavior is essential. Following are the top eight safe cybersecurity practices:

1. Protect your personal information, including credit-card numbers, Social Security number, user names and passwords, and other sensitive data. Do not store any of this information on your computer, and disable the password "remember/auto-complete" function in your Web browser.
2. Know the companies with which you are dealing online. Do not disclose your identity or sensitive information to strangers or to websites that are not verifiably secure.
3. Use a highly rated security suite with an up-to-date database of virus definitions. Using outdated virus definitions will leave you exposed to security threats.
4. Use only the most recent versions of operating system and browser software, which often incorporate security patches.
5. Back up your important files regularly. Offline and online backup tools are readily available.



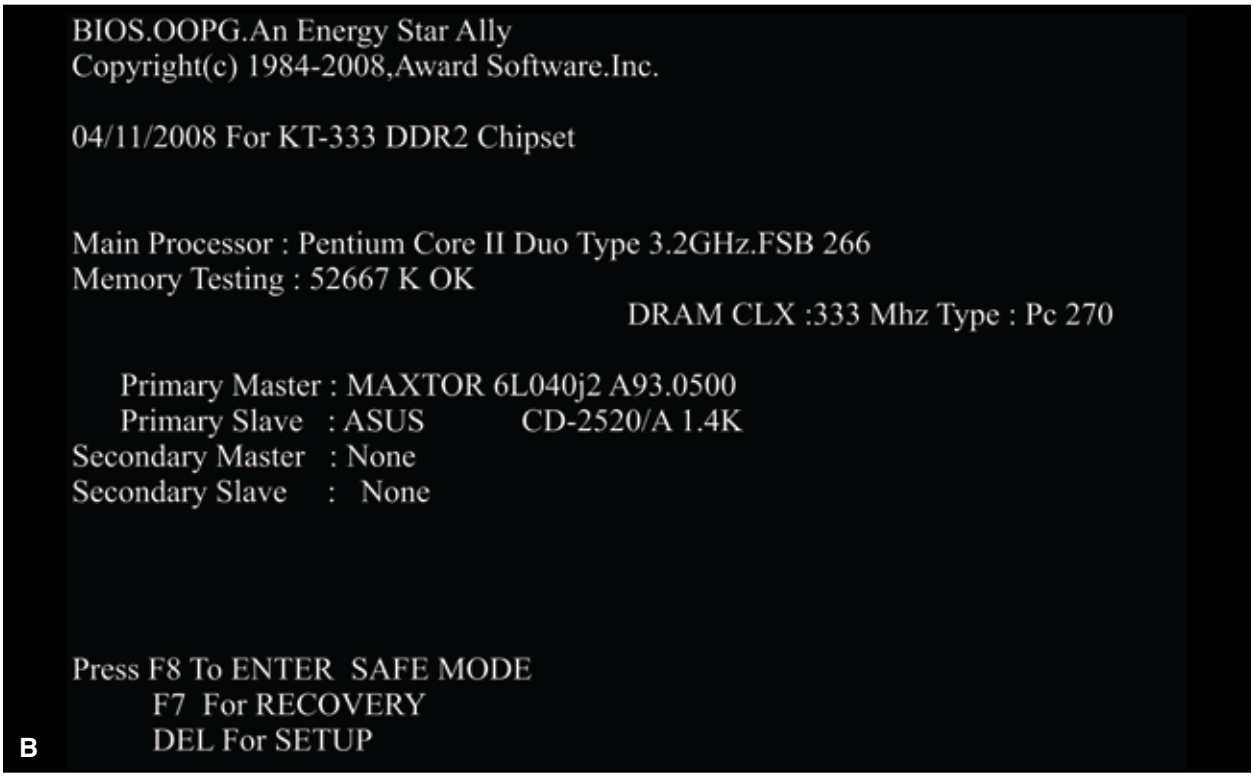


Fig. 3 A. Entering safe mode from "Advanced Boot Options" after rebooting computer. B. Prompt to press F8 key to enter safe mode.

6. Do not download or install software from unknown sources, including programs received as e-mail attachments. Note that many fake "anti-malware" suites exist that, if installed, will actually infect your computer with malware.
7. Do not install pirated software or attempt to use a "crack", "patch", or "keygen" to convert trial software into a full version of the program. This practice is illegal as well as extremely risky.
8. Do not visit websites that offer free downloads of movies, software ("warez"), and so on. These sites tend to be infested with malware.

More details on safe Internet practices can be found at Stay Safe Online, a website of the National Cyber Security Alliance.

Combating a Malware Infection

Even the best preventive measures cannot guarantee immunity to malware infection. If an infection occurs, the following remedial steps apply to computers running Microsoft Windows.

1. Reboot the computer and enter the safe mode. The first step is to reboot (restart) the computer. The boot (start-up) screen will identify the key to be pressed to enter the "safe mode"; on most systems running Microsoft Windows, this is the F8 key (Fig. 3). In the safe mode, the system loads only the most critical drivers, so that if another driver is infected, it can be disinfected. Additional information on entering the safe mode in all versions of Microsoft Windows can be found at ComputerHope.com.

2. Turn off "System Restore". In a Microsoft Windows operating environment, the "System Restore" control is located in the "Performance" section of the control panel. This control should be turned off before running a malware scan, because it may otherwise restore the malware after the system has been disinfected.

3. Run a full-system anti-malware scan in safe mode. Once you have entered the safe mode and turned off "System Restore", run a full-system anti-malware scan with updated definitions. Another option is to run a DOS-based anti-malware scanner such as ESET NOD32 Antivirus for MS-DOS, which can be purchased on the Internet. The advantage of a DOS-based scanner is that the operating system need not be loaded, making even critical system files available for the scan. This is akin to physically connecting the system disk to a different system and doing a "scan from the outside".

4. Install and run a temporary file cleaner and stand-alone malware shredders. Before or after the anti-malware scan, install and run a temporary file cleaner to remove the unnecessary files that Windows generates in the course of its operation. Effective cleaners such as Windows CleanUp! and CCleaner are freely available. In addition, it is wise to run a stand-alone malware shredder such as Stinger, an anti-browser hijacker like Trend Micro's HijackThis, and a rootkit revealer such as Ice Sword to disinfect any malware that goes undetected in the standard malware scan. You can also run online scans at the websites of major antivirus software manufacturers, including ESET and Symantec.

Safeguarding Data in the Event of a System Boot Failure

Data should be stored in a local hard-disk-drive partition other than that occupied by the operating system. For example, if the operating system is in drive C, data can be stored in drive D. This ensures the data's safety if the operating system has to be reinstalled. Reinstallation is often needed if malware causes irreparable damage to system files, which can lead to boot failure, a slow or unresponsive operating system, and other performance errors.

If boot failure occurs and data have not been stored in a separate area of the disk from the operating system, or if valuable data reside on the desktop (which by default is part of drive C), reformatting the disk would lead to catastrophic data loss. In this situation, the system can be booted from a CD drive using a bootable operating system disk ("live CD"), such as Linux Ubuntu or Knoppix (Fig. 4). A list of bootable operating systems is available at The LiveCD List.

Booting from the live disk may require changing the boot order in the BIOS (Basic Input/Output System) settings. The primary function of

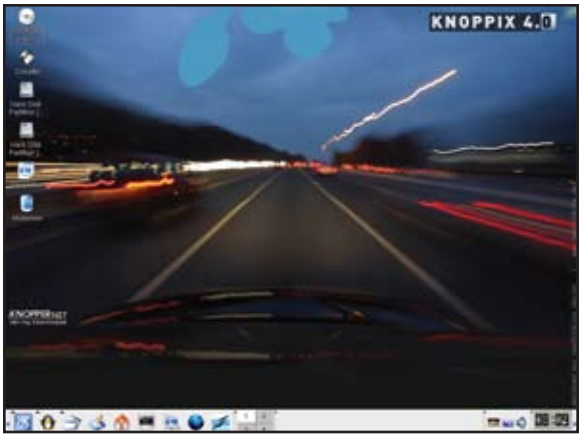


Fig. 4 System booted from Knoppix operating system disk.

the BIOS is to identify and initialize system component hardware (such as the video display card, hard disk, and floppy disk) when the PC is first powered on. A specific boot order is followed when the BIOS searches for the operating system—for example, 1) local hard disk, 2) CD drive, 3) floppy drive. Booting from a live CD requires that the CD drive be designated as the first boot option in the BIOS. To change the BIOS settings, press the key designated for BIOS setup at the start-up screen (in Figure 3B, this is the "Del" key). Once you are logged in, you can use the live disk to access the drives on the local hard disk. Subsequently, your data can be transferred to portable media such as an external hard drive.

Some programs, including Recover My Files and Data Recovery Doctor, allow the recovery of deleted data or data lost during disk formatting. Obviously, frequent backup of important data to physical media such as CDs, DVDs, or high-density disks is a prudent habit that will avoid the need for such programs.

Conclusion

As in many other areas of life, "prevention is better than cure" is a truism in the world of technology. Even the best preventive measures, however, may not be enough to ward off the ever-growing menace of malware. At some point, every computer user will experience its ill effects, whether in the form of operating-system boot failure, data corruption, or other annoying and potentially serious problems. Fortunately, advances in data-recovery software have increased the chances that important data can be retrieved after unexpected damage or loss due to malware.

ACKNOWLEDGMENTS: We want to thank Dr. Ronald Redmond for his valuable suggestions to improve this paper.

AMEET V. REVANKAR, BDS, MDS
Assistant Professor
Department of Orthodontics
and Dentofacial Orthopedics
SDM College of Dental Sciences and Hospital
Sattur, Dharwad 580009
India
drameet@orthodontist.net

NARAYAN H. GANDEDKAR, BDS, MDS
Assistant Professor

SANJAY V. GANESHKAR,
BDS, MDS, MDO RCPS
Professor and Chair

REFERENCES

1. Malware, available at http://en.wikipedia.org/wiki/Malware; accessed July 14, 2008.
2. Symantec Internet security threat report: Trends for July-December 2007 (Executive Summary), available at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf; accessed July 14, 2008.
3. F-Secure Corporation: F-Secure reports amount of malware grew by 100% during 2007 (Dec. 4, 2007), available at http://www.f-secure.com/f-secure/pressroom/news/fs_news_20071204_1_eng.html; accessed July 15, 2008.
4. F-Secure Corporation: F-Secure quarterly security wrap-up for the first quarter of 2008 (March 31, 2008), available at http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080331_1_eng.html; accessed July 15, 2008.
5. Ruin a malware author's whole day with a Software Restriction Policy! available at http://www.mechbgon.com/srp/; accessed July 14, 2008.