Citation Rank(R) Database Mode
2/20/96 PCMAG 039 R 284 OF 429 ALLNEWS Page
2/20/96 PC Mag. 039
1996 WL 2091718
(Publication page references are not available for this document.)
PC Magazine

Tuesday, February 20, 1996

Vol. 15, No. 4

Windows 95 Antivirus Utilities: The Latest in PC Protection

Rubenking, Neil J.

As Windows 95 replaces DOS and Windows 3.1 as the operating system of choice, many systems can be left vulnerable to virus attack. That's because there is no antivirus utility supplied with Windows 95.

By one count there are 6,000 new computer viral strains each year, and most are more insidious than the familiar Stoned or Anti.EXE viruses.

We compiled a selection of five currently available Windows 95 antivirus products: Dr. Solomon's Anti-Virus Toolkit for Windows 95 ($125), from S&S Software International; Norton AntiVirus for Windows 95 ($79.95), from Symantec; PC-cillin 95, Version 1.0 ($49.95), from TouchStone Software Corp.; ThunderByte Anti-Virus Utilities Professional Version for Windows 95 ($149.95), from ThunderByte TCT International Corp.; and VirusScan for Windows 95 ($65), from McAfee Associates. We found that each provided at least a minimum level of protection, and each had its strengths and weaknesses.

As a whole, these antivirus programs are a mix of old and new: Each relies primarily on scanning files for signatures of known viruses, and each uses a Windows 95 virtual device driver (VxD) for background processing. Each can scan disks upon access, scan files at start-up, scan programs before execution, and even scan files when they're copied or otherwise accessed.

In addition, each can scan DOS-based programs that load before Windows 95, and each supports some form of DOS-based recovery, in case a virus disables Windows 95. By the time you read this, all five will all be

able to detect macro viruses, such as WinWord.Concept.

Scanning for known virus signatures is only as good as your database of viruses. All five products provide updates to signature files via BBS, Internet, or mailed-disk subscription. PC-cillin and ThunderByte Anti-Virus go a step further and include software to download updates automatically. Annual disk-subscription prices vary widely, from Dr. Solomon's Anti-Virus Toolkit's included first year of updates (each additional year costs $225) to Norton AntiVirus's and ThunderByte Anti-Virus's $99.95 cost. In between are PC-cillin's $9.95 and VirusScan's $69.95 yearly fee.

Three of the programs go a step beyond signature tracking with behavior monitoring, which can detect viruses by their effect on the system rather than by file pattern. Norton AntiVirus, PC-cillin, and ThunderByte Anti-Virus store integrity-checking data about executable files and use the information to raise warning flags when even the slightest file modifications are made.

In addition, Norton AntiVirus, PC-cillin, and VirusScan carry the National Computer Security Association (NCSA) logo, which means they have been certified to detect all of the viruses in the NCSA collection. The others, Dr. Solomon's Anti-Virus Toolkit and ThunderByte Anti-Virus, claim to be able to detect all of the viruses in the organization's collection--and more.

We gave these first five Windows 95 virus scanners a workout, testing them with an array of powerful viruses. We set each product to scan all executable files on our 90-MHz Pentium PC's 800MB hard disk, and to scan compressed files where possible.

Each program was adept at detecting the viruses we used, but we found that ThunderByte Anti-Virus and PC-cillin were the fastest to scan the hard disk, at 41 seconds and 53 seconds, respectively. We also timed how long a product took to scan a floppy disk that contained 60 files. Again, ThunderByte Anti-Virus and PC-cillin were the fastest, at 7 seconds and 11 seconds, respectively.

These five programs offer something for everyone: From Norton AntiVirus's flexible approach to PC-cillin's automatic intervention to ThunderByte Anti-Virus's speed to VirusScan's thorough Windows 95 integration to Dr. Solomon's Anti-Virus Toolkit's ability to detect macro viruses.

Dr. Solomon's Anti-Virus Toolkit for Windows 95

Dr. Solomon's Anti-Virus Toolkit for Windows 95 is a mixed bag: The virus-fighting code is fully Windows 95-aware, but its user interface doesn't make the most of the Windows 95 environment. It was also the only program of the five reviewed here that wasn't Windows 95-certified.

For example, the program's background modules are simply minimized rather than housed in the system tray, there's no Windows 95 uninstall support, and context menus, property sheets, and drag-and-drop support are absent.

Dr. Solomon's Anti-Virus Toolkit (along with PC-cillin and VirusScan) can search for viruses hidden when an infected program is compressed with PKLITE or a similar utility. It also searches files multiply archived in formats, including .ZIP, .ARC, and .LHA.

The program includes a protective macro for Word for Windows that warns you when a document is infected with a macro virus. Power users can use Dr. Solomon's Anti-Virus Toolkit's viewers to peek directly at boot sectors or into suspected files.

One minor flaw is that Dr. Solomon's Anti-Virus Toolkit's virus-alert pop-up window can't be seen when a full-screen DOS box is running. The system is still protected, but the user will see only an "Access Denied" message. The alert pop-up is visible as soon as the user switches out of the full-screen DOS box.

At 1 minute 31 seconds to scan our hard disk, the program tied with VirusScan as the slowest virus scanner but was closer to the average on checking floppy disks. All in all, Dr. Solomon's Anti-Virus Toolkit prefers to straddle Windows 95 and Windows 3.1 rather than fully embrace the new operating system.

Dr. Solomon's Anti-Virus Toolkit for Window 95. List price: $125 (includes four quarterly updates). Requires: 4MB RAM, 10MB hard disk space, Microsoft Windows 95. S&S Software International Inc., Burlington, MA; 800-701-9648, 617-273-7400; http://www.drsolomon.com.

Norton AntiVirus for Windows 95

A thoroughly modern program, Norton AntiVirus for Windows 95 installs easily and goes right to work. Its Auto-Protect and Scheduler modules use the Windows 95 Taskbar, and at any time you can drag a suspect file onto the scanner for a quick checkup.

A promised update early this year should let Norton AntiVirus detect

macro viruses within Windows 95. Norton AntiVirus currently detects macro viruses by using the DOS-based scanner.

A host of option settings lets the user control just about every aspect of scanning, including the frequency of scanning, the file types to be scanned, and the response when a virus is discovered. Norton AntiVirus alerts come through loud and clear, even in a full-screen DOS box. And Norton AntiVirus's Virus Sensor technology allows it to detect unknown viruses by simulating execution in a completely separate--and protected--memory space.

Norton AntiVirus will not detect a virus in a compressed program file if the virus was present before compression. It will, however, detect viruses that reside inside an archive, such as a .ZIP file.

Norton AntiVirus was able to check our hard disk for viruses in 1 minute 19 seconds, which was about average. On the whole, Norton AntiVirus delivers a fully up-to-date method for ferreting out viruses.

Norton AntiVirus for Windows 95. Estimated street price: $79.95. Requires: 4MB RAM, 12MB hard disk space, Microsoft Windows 95. Symantec Inc., Cupertino, CA; 800-441-7234, 503-334-6054; http://www.symantec.com.

PC-cillin 95 1.0

TouchStone's PC-cillin 95, Version 1.0, is designed to make virus protection as simple and automatic as possible. Once installed, it decides where and when to scan based on the degree of threat: Using floppy disks or CD-ROMs, or connecting to another computer via network or modem, all raise the threat level. After a virus is found, PC-cillin goes into a high-intensity Virus Watch mode for 90 days.

PC-cillin checks for viruses in places that most scanners don't. For example, it scans files within archives such as .ZIP files and even compressed files within .ZIP files. It also scans uu-encoded attachments to e-mail messages.

PC-cillin can protect against infected downloads by scanning serial data as it arrives at your PC, before it makes its way to your hard disk. Other vendors argue, however, that there's no point in scanning for viruses until the data becomes a file on-disk, or until the attachment is uu-encoded into a file. But if you're concerned about getting a virus through the Internet, this feature may calm your nerves.

Another reassuring feature is PC-cillin's countdown to the next recommended update. The program automates the actual update process as well. Press a button and PC-cillin downloads new virus signatures.

To trap unknown viruses, its VICE (Virus Instructional Code Emulator) technology scans program code for virus-related instructions and also monitors for viruslike actions by a running program. If a virus is detected, the Clean Wizard walks you through its cleanup and broadcasts an e-mail message to warn your correspondents, checks all accessible disks for infection, and checks disks you regularly use.

PC-cillin was second only to ThunderByte Anti-Virus in terms of scanning speed; it was able to scan our hard disk in 53 seconds. If you're looking for a way to react quickly and automatically to a variety of virus threats, look no further than PC-cillin 95.

PC-cillin 95, Version 1.0. List price: $49.95. Requires: 2.5MB RAM, 4MB hard disk space, Microsoft Windows 3.1 or Windows 95. TouchStone Software Corp., Huntington Beach, CA; 800-531-0450; http://www.antivirus.com.

Thunderbyte Anti-Virus Utilities Professional Version for Windows 95

ThunderByte Anti-Virus Utilities Professional Version for Windows 95 was the fastest of the five programs we reviewed and in some respects the most thorough. By default, ThunderByte Anti-Virus scans Word for Windows .DOC (document) and .DOT (template) files, so there's no need to search every file to trap a Word for Windows macro virus.

ThunderByte Anti-Virus is known for its innovative heuristic viral analysis ("Windows 95 Utilities: Picking Up the Pieces," November 21, 1995). To detect unknown viruses, it analyzes program code by simulating execution and looking for suspicious, viruslike activities, such as going memory-resident, attempting to distinguish .COM from .EXE files, and a program's directly accessing the system's hard disk.

Simulated execution is useful in dealing with an encrypted virus, which must decrypt its own instructions before executing them. This forces such a virus to expose itself to the antivirus program. A file with sufficient suspicious activities will be flagged.

ThunderByte Anti-Virus is unusual in that it doesn't attempt to remove viruses from within Windows but rather works through DOS. If a virus is found, it offers to rename the file, delete the file, or delete the file with no possibility of undeletion. To remove the virus, you must boot the system from a clean DOS disk and use the supplied DOS version of

ThunderByte Anti-Virus.

This two-pronged approach lets known viruses be eradicated using known methods. The DOS-based ThunderByte Anti-Virus has other options for cleaning unknown viruses. For example, it can simulate the virus's execution to make the virus repair the file, because every successful virus must make the host program seem to be functioning normally. Another option is file repair using information stored before the infection, including file size, a checksum. and several kilobytes of stored code from the beginning of the program.

The fastest of the five tested programs, ThunderByte Anti-Virus was able to scan our hard disk in 41 seconds, about twice as fast as the others. All in all, ThunderByte Anti-Virus is a very speedy and advanced first line of defense against virus attack.

ThunderByte Anti-Virus Utilities Professional Version for Windows 95. List price: $149.95. Requires: 4MB RAM, 2MB hard disk space, Microsoft Windows 95. ThunderByte TCT International Corp., Massena, NY; 800-667-8228, 613-930-4444; http://www .thunderbyte.com.

VirusScan for Windows 95

Longtime users of McAfee's VirusScan may not recognize this version because it has been so well INTEGRATED into WINDOWS 95.

There are context-sensitive menus for files, drives, and directories, as well as a properties page for .VSC (VirusScan Configuration) files that includes an additional page for defining what action to take when a virus is discovered. Right-click on a file identified as infected and you get a context menu that includes options to clean, delete, or move the file.

VirusScan detects macro viruses and installs protection directly in Word for Windows. The scanner relies on the System Agent, available in the Windows 95 Plus! Pack, for scheduled scanning; setup is a simple matter of creating a .VSC file and defining the desired scan options.

Numerous option settings allow customization: You can set the scanner to try to clean infected files automatically or delete them automatically; VirusScan's report will let you know which files were deleted, permitting you to restore them from a clean backup.

McAfee takes virus scanning to the Internet by offering WebScan, a $65 program that examines downloaded files and e-mail in an isolated holding

pen. A free evaluation copy, which includes Mosaic and the Pegasus e-mail client, can be downloaded from the company's World Wide Web site.

VirusScan took 1 minute 36 seconds to scan our hard disk, the slowest time of the group; its floppy disk scan time was the slowest as well.

VirusScan for Windows 95. List price: $65. Requires: 4MB RAM, 10MB hard disk space, Microsoft Windows 3.1 or Windows 95. McAfee Associates Inc., Santa Clara, CA; 800-332-9966, 408-988-3832; http://www.mcafee.com.

From February 12 to 16, go online to discuss Windows 95 antivirus products with representatives for each reviewed product and Neil J. Rubenking, contributing technical editor of PC Magazine. Type GO EXEC at any CompuServe ! prompt.

---- INDEX REFERENCES ----

KEY WORDS: COMPUTERS

INDUSTRY: Software (SOF)

REGION: United States (US)

Word Count: 2153
2/20/96 PCMAG 039
END OF DOCUMENT