Windows 95 Virus Reported... And More Microsoft Word Macro Viruses; Technology Alert, Vol. 96, No. 1, March 1996

American Institute of Certified Public Accountants. Information Technology Membership Section

TECHNOLOGY ALERT

Vol. 96 No. 1
March 1996

Windows 95 Virus Reported...

And More Microsoft Word Macro Viruses

Yet another virus has been unleashed that is plaguing PCs worldwide. This latest virus, called "Boza," attacks Windows 95 users and is not believed to affect DOS, Windows 3.x or Windows NT files. The virus, although not contained in Windows 95, infects the program when a Windows 95 user downloads a file from the Internet, an electronic bulletin board or an online service. It also can spread when using an infected floppy disk that is inserted into a PC.

According to a recent report in *Newsbytes* (February 6, 1996), Microsoft reports that so far Boza isn't a widespread problem. If it does strike, it can infect up to three 32-bit Windows 95-based applications in the current directory, such as word processing, spreadsheet, or database software. Presently, the virus seems fairly harmless, as it will sometimes display a dialog box that contains messages about the virus from the author. The virus itself contains programming errors, and may cause infected programs to not run correctly. Some experts believe the virus was designed to demonstrate that Windows 95 is subject to infection.

WinWord/Hot Microsoft Word Macro Virus Discovered

Meanwhile, Sophos Plc., a software security company in Abingdon, England reported in a recent *Newsbytes* (February 1, 1996) that it has detected the existence of a fifth Microsoft Word macro virus. The latest virus, WinWord/Hot is the first seriously destructive Microsoft Word macro virus to hit the PC world according to Paul Ducklin, a senior virus analyst at Sophos. WinWord/Hot comes with an affliction that sets a "hot date" 14 days from the date it hits the PC and, when it becomes active, so giving the virus time to spread before detection. On the 14th day after infection, the virus then starts to randomly delete documents on the PC's hard disk.

The first virus, DMV, was very much an experiment, since it popped up Word dialog boxes all around the screen. The next, Concept or the "prank virus," was the first mainstream one. It infects a Word application by making its "Save As Feature" turn all files into infectious templates. Then came Colors, which messed with desktop colors and the fourth virus was Nuclear, which due to its own "bugs" prevented it from doing any significant damage.

Editor's Note: Symantec Corp., publishers of the Norton AntiVirus software program, has released a free "virus definition update" designed to help PC users detect whether Boza is present. It is available through online services and Symantec's Web site at http://www.symantec.com. In addition, IBM and McAfee Associates Inc. have posted virus scanners on their Web pages to detect Boza at http://www.ibm.com and http://www.mcafee.com, respectively. Information Technology Section members are once again advised to practice "safe computing" and to check all files and floppy disks before downloading any files.

TECHNOLOGY ALERT

© 1996 AICPA Information Technology Membership Section

Vol. 96 No. 1
March 1996

Threats to Java Discovered

Virus protection software companies have begun to worry about the next possible threat, either viruses or other destructive programs that will attack through the Java Internet language, according to a recent article in *PC Week* (February 12, 1996).

Until recently, the only real threat to Java was worms, programs that replicate in the memory of one machine and then go over the Internet to replicate in another machine, reported Carey Nachenberg, a senior software engineer for Norton AntiVirus. Worms can affect network traffic, but wouldn't necessarily damage data.

However, in a recent issue of *Computerworld* (March 11, 1996), it was reported that there was a breakdown in the security of Sun Microsystems, Inc.'s Java programming language. (See Technology Alert, vol. 95, no. 9 for more details on Java.) It appears that Java "applets" can be made to disguise themselves in a way that would allow them to go places they weren't supposed to go.

According to an alert issued by the Computer Emergency Response Team (CERT) at Carnegie Mellon University, Java applets can connect to arbitrary hosts previously thought to be in accessible, i.e., hosts behind a firewall. Java was designed in such a way that a Java program or applet could not access any computer other than the "server" that produced it and sent it to the "client." It was discovered that it is possible to produce a harmful applet that contains the IP (Internet protocol) address of a machine to be attacked rather than the correct home address of the server that launched it.

Editor's Note: Netscape Communications Corp has a "patch" available for its browser, Navigator at http://home.netscape.com/newsref/std/java_security.html, and Sun reported that it will have a fix for its Hot Java browser posted to its web site shortly at http://java.sun.com. For further information on the security alert released by CERT, see their web site at ftp://info.cert.org/pub/cert_advisories/CA-96.05.README.