

Current 'Zero-Day' Web Attack Leaves PCs Unprotected

Tuesday , April 03, 2007

FOX NEWS

Millions of PCs around the world were left vulnerable over the weekend as malware writers exploited a weakness in Microsoft's Internet Explorer Web browser.

Microsoft Corp. ([MSFT](#)) sent out a security advisory Thursday warning customers that a vulnerability in ".ani" files — used to change the mouse cursor into an hourglass while a program works, or into a dancing animal or other animation on specially designed Web sites — was allowing hackers to break into computers and install malicious software.

"Overnight we did see the attacks change from limited and targeted attacks to slightly more, but do still categorize it as a limited attack," Mark Miller, director of the software maker's security response group, said Friday.

However, third-party security firms took a more serious view of the matter, especially when it became clear that machines with almost all versions of Microsoft Windows dating back to and including Windows 2000 were vulnerable.

One major company, eEye Digital Security, even put out its own patch for general-user download Friday as no word came from Microsoft about when an official fix would be issued.

eEye said its fix was temporary, and should be uninstalled when Microsoft issues its official patch.

On Monday, Microsoft announced that it would have an official patch the following day, Tuesday, April 3, pre-empting its usual monthly patch cycle by one week. Click [here](#) to read details

On Saturday, Microsoft posted [security advisory 935423](#) about the vulnerability.

F-Secure, another top security firm, advises that PC users avoid using Internet Explorer 6 or 7. Mozilla's Firefox browser does not seem to be affected.

The so-called "zero-day attack," a vulnerability that is discovered before Microsoft has a chance to fix the problem, seems to have been aimed at PCs running [Windows Vista](#), the new operating system the company has touted as its most secure.

The hole has also been found on Windows 2000 Service Pack 4, Windows XP Service Pack 2 and some versions of Windows Server 2003 — including 64-bit versions designed for running on advanced microprocessors.

The full list of affected operating systems includes, according to eWeek.com:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003

- Microsoft Windows Server 2003 for Itanium-based Systems
- Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition
- Microsoft Windows Vista

Once hackers have access to a computer, they can install any number of nasty programs — ones that steal passwords or record keystrokes, which the hackers could then sell to identity thieves.

Microsoft first learned of the vulnerability in December, and has been working on a patch since, Miller said. He did not say whether it would be distributed on its own or as part of a scheduled update.

On Wednesday, security software vendor McAfee Inc. ([MFE](#)) saw a post on a Chinese message board indicating hackers were planning to exploit the hole, which set Microsoft's security advisory in motion.

"It is important to note that while we do think Vista is most secure operating system released, no software is 100 percent secure," Miller said.

Computer users could end up with a malicious program on their PC after a Web browsing session and not know it, said Craig Schmugar, a virus researcher for McAfee Avert Labs, the research arm of McAfee.

While Microsoft urged people to be extremely cautious with e-mail, security companies said they have not seen any instances of attacks via e-mail.

While it's hard to tell what hackers will do once they have access to a computer, a group of Chinese hackers may be plotting to steal login information for the wildly popular multi-player video game, "World of Warcraft."

People who buy the stolen login information can profit by selling items inside the game world, said Ken Dunham, director of the rapid response team at iDefense, the research division of VeriSign Inc. ([VRSN](#))

Dunham said his team learned of the plan on a Chinese hacker message board.

FOXNews.com's Paul Wagenseil and The Associated Press contributed to this report.