

Unpatched software flaws put PCs at risk, security vendor finds

Deborah Gage, Chronicle Staff Writer

Friday, January 11, 2008

Ninety-five percent of personal computers are vulnerable to attack by hackers due to unpatched flaws in their software applications, according to data released on Wednesday by Secunia, a Danish security vendor.

The data was collected this month and comes from 20,000 computer users who used Secunia's tracking tool, Software Inspector, for the first time. The tool runs off Secunia's Web site and tracks which applications on a user's PC are insecure, meaning they have a hole for which a patch has not been applied.

The report is the latest development in the continuing battle between hackers and computer users. Software flaws have increased the past several years, say several security researchers, making it more challenging for PC owners who are trying to keep their machines secure.

According to Secunia's data, less than 5 percent of the scanned computers had software applications that were considered secure. About a quarter of the computers had as many as five flawed applications, and another quarter had as many as 10. Forty-two percent of computers had more than 11 insecure applications. About 1.8 million applications were scanned.

"Here's hard data to support what we announced" more than a year ago, said Alan Paller, director of research for the SANS Institute, an independent researcher in Bethesda, Md. "Attackers had moved to the applications, and nobody was patching them."

There are plenty of examples of troubled software.

In Microsoft Office, for example, the number of flaws jumped 300 percent between 2006 and 2007, according to data from SANS. Most of that increase came from hackers who were exploiting flaws in Excel, Microsoft's spreadsheet, by e-mailing infected spreadsheet files to people and trying to trick them into opening the files.

Now attackers have grown more sophisticated. Recent attacks have focused on planting malware - software intended to spy or infect users - on Web sites, some well known. The malware tries to download itself onto any computer that visits the site.

During the last week, for example, thousands of Web sites, some belonging to government agencies and schools, have been embedded with malware developed in China that is designed to exploit a flaw in Real Networks' RealPlayer, a software program that plays audio and video files. SANS Internet Storm Center is one of several research organizations tracking the attack.

Last year, the Miami Dolphins' Web site was the unwitting host of malicious banner ads just before the Super Bowl.

Malware, in attacks like these, is usually invisible to computer users, said Mary Landesman, a senior security researcher at ScanSafe, a security company in San Francisco. The malware may be planted through a flaw in the Web site's software or inserted into banner ads, which are then placed on the site.

Any computer that visits the site, and has an unpatched software flaw that the malware is able to exploit, gets infected, Landesman said. Often, the malware opens a back door in the machine that allows hackers to track keystrokes and ship out passwords and other valuable data.

"You have vulnerabilities on both ends," the computer and the Web site, she said. Well-known Web sites are just as vulnerable as



those from smaller businesses. Even though most Web sites are safe, she said, "People should understand that these attacks are happening and take precautions."

As attacks increase, software vendors are getting better at handling flaws, said Secunia CEO Thomas Kristensen.

Microsoft, the biggest target, has become the best at notifying users of flaws in its software and delivering patches, he said. Patches from Microsoft are now downloaded onto some PCs automatically. Microsoft said it has worked closely with Secunia on flaws because Secunia notifies Microsoft when it finds flaws and supplies updated, accurate information.

Apple, Adobe and Mozilla, which makes the Firefox browser, also deliver patches through automatic downloads and say they have worked to improve the way they patch their software.

Still, in 2007 the average window of exposure for vulnerabilities affecting software from big vendors - the time during which the software was unpatched and could be exploited - was 55 days, up from 47 days in the second half of 2006, according to Symantec, a security company in Cupertino.

As the biggest vendors get better at securing their applications, the smaller vendors become targets, Kristensen said.

Last January, Secunia found a small program, or widget, embedded in applications from more than 30 vendors. Only four or five vendors responded when notified about the problem, he said, and no vendor, including the company that made the widget, would take responsibility for fixing it.

When Secunia believes an application can be exploited but can't be fixed, all the company can do is tell computer users so they can put pressure on the vendor to fix the problem, he said.

"In many cases, unfortunately, it's the only way to teach a vendor to update the software and notify users about it," he said.

Pc protection

What you can do to keep your computer safe:

- Don't keep software on your computer that you don't use. Uninstall it.
- Disable JavaScript in your browser. It is a vector for many attacks that come from Web sites.
- Check regularly for software patches.
- Keep your anti-virus software current.

Source: Chronicle research

E-mail Deborah Gage at dgage@sfgchronicle.com.

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/11/BULJUDB53.DTL>

This article appeared on page **C - 1** of the San Francisco Chronicle

San Francisco Chronicle Sections

Go

© 2008 Hearst Communications Inc. | [Privacy Policy](#) | [Feedback](#) | [RSS Feeds](#) | [FAQ](#) | [Site Index](#) | [Contact](#)