Published on *InfoWorld* (http://www.infoworld.com)

Typical Windows user patches every 5 days

By Gregg Keizer
Created *2010-03-04 04:38AM*

The typical home user running Windows faces the "unreasonable" task of patching software an average of every five days, a security [1] and vulnerability [2] research company said today.

"It's completely unreasonable to expect users to master so many different patch mechanisms and spend so much time patching," said Thomas Kristensen, the chief security officer of Secunia. The result is that few consumers devote the time and attention necessary to stay atop the patching job, which leaves them open to attack.

[This week Microsoft tried again with the patch linked to Windows blue screens [3]. | Learn how to secure your systems with Roger Grimes' Security Adviser blog [4] and newsletter [5], both from InfoWorld.]

According to Secunia, of the users who ran the company's Personal Software Inspector (PSI) the last week of January, half had 66 or more programs from 22 or more different vendors on their machines. PSI is a free tool that scans PCs to produce a list of vulnerable software, but does not itself initiate updates. Instead, users are directed to the approprite vendor patch site. Nearly 2 million copies of the tool have been downloaded since Secunia debuted it in 2007.

After comparing the software portfolios on each machine with the bugs Secunia tracked during 2009, Secunia determined that the typical user faced nearly 300 vulnerabilities during the year, and with the number of vendors represented on the PC, had to deal with approximately 75 patch incidents annually.

That averages out to a patch action every 4.9 days.

"It surprised us that there were so many applications on the systems," said Kristensen, "and that then there were so many updates they had to do in a year." Also important, he said, was that the typical user had to master 22 different patch mechanisms, one from each of the 22 software makers whose programs were on her PC.

"That's why we called for software vendors to create a unified patching standard last year," said Kristensen, referring to a pitch Secunia made at the RSA Conference [6] in 2009. The company's offer didn't go over well. "A few vendors said 'We want to hear more,' but a lot just

ignored us or turned down the idea outright."

Rather than wait on software makers to come up with a single patch mechanism -- something unlikely in any case -- Secunia has stepped up to produce a patching tool that will eventually handle 70 percent to 80 percent of the software on consumers' Windows machines.

In the next six weeks, Secunia will release a technical preview of PSI 2.0, which will include automatic updating functionality similar to what Microsoft [7] provides for Windows and other software. Before the end of the year, Secunia should have PSI 2.0 wrapped up. "Updating is complicated, and we need to get it out to users so they can give us feedback," said Kristensen. PSI 2.0 will be free to consumers.

PSI 2.0 is based on technology in Secunia's Corporate Software Inspector with Microsoft's Windows Server Update Services (WSUS), which entered beta in January.

"We want to promote patching," Kristensen said when asked why Secunia is expending resources on a product it's giving away. People know Microsoft's patch service, Windows Update, but that's not the only updating mechanism they have to deal with, he continued. "They have to patch Adobe software three, four times a year, and QuickTime, which is frequently exploited. That's why we think this will make a difference."

Secunia has published a white paper that details its PSI scan findings (download PDF [8]).

Gregg Keizer covers Microsoft, security issues, Apple, Web browsers and general technology breaking news for Computerworld. Follow Gregg on Twitter at @gkeizer [9] or subscribe to Gregg's RSS feed [10] . His e-mail address is gkeizer@ix.netcom.com [11] .

Read more about security [1] in Computerworld's Security Knowledge Center.

Security Central Windows Microsoft Applications Patch management Windows

Links:
[1] http://www.computerworld.com/s/topic/17/Security
[2] http://www.computerworld.com/s/topic/85/Spam, Malware and Vulnerabilities
[3] http://www.infoworld.com/d/windows/microsoft-tries-again-patch-linked-windows-blue-screens-425?source=fssr
[4] http://weblog.infoworld.com/securityadviser/?source=fssr
[5] http://www.infoworld.com/newsletter/subscribe.html?source=fssr
[6] http://www.computerworld.com/s/article/9162458/Full_coverage_RSA_Conference_2010
[7] http://www.computerworld.com/s/article/9137060/Microsoft_Update_Latest_news_features_reviews_opinions_and_more
[8] http://secunia.com/gfx/pdf/Secunia_RSA_Software_Portfolio_Security_Exposure.pdf
[9] http://twitter.com/gkeizer
[10] http://www.computerworld.com/s/feed/keyword/Gregg Keizer
[11] mailto:gkeizer@ix.netcom.com