

Hackers aren't just picking on Microsoft - study

By *srlinuxx*

Created *02/05/2005 - 2:58pm*

Submitted by srlinuxx on Monday 2nd of May 2005 02:58:34 PM Filed under [Security](#) [1]

Online criminals turned their attention to antivirus software and media players like Apple Computer Inc.'s iTunes in the first three months of 2005 as they sought new ways to take control of users' computers, according to a survey released on Monday.

While hackers continued to poke new holes in Microsoft Corp.'s popular Windows operating system, they increasingly exploited flaws in software made by other companies as well, the nonprofit SANS Institute found.

As more Windows users agreed to receive security upgrades automatically, hackers looked to take advantage of other software programs that might not be patched as frequently, the head of the cybersecurity training and research organization said.

"Operating systems have gotten better at finding and fixing things and auto-updating, so it's less fertile territory for the hackers," said SANS Chief Executive Alan Paller.

Malicious hackers exploit security holes to lift credit-card numbers and other sensitive personal information from a user's computer, or commandeer it to send out spam and pornography.

More than 600 new Internet security holes have surfaced in 2005 so far, SANS found.

Of those, 20 were deemed most dangerous because they remain unfixed on a large number of Internet-connected computers even though software makers quickly made patches available.

As always, Microsoft products were a popular target.

Hackers found ways to take control of a user's computer by tunneling through Microsoft's Web browser, media player and instant-messaging software, as well as Windows software for servers and personal computers.

But software by Oracle Corp. and Computer Associates International Inc. also made the list, along with media players like Apple's iTunes, RealNetworks Inc.'s RealPlayer, and Nullsoft's Winamp.

Anti-virus products from Symantec Corp.. F-Secure, TrendMicro and McAfee Inc. proved vulnerable as well, a prospect Paller found particularly discouraging.

"We ought to do better in our industry -- we should be a model for others," he said.

The complete list can be found at sans.org [2].

[Source](#) [3].

[Security](#)

Source URL: <http://www.tuxmachines.org/node/800>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/59>

[2] <http://www.sans.org/top20/Q1-2005update>

[3] http://today.reuters.co.uk/news/newsArticle.aspx?type=internetNews&storyID=2005-05-02T110846Z_01_MCC240051_RTRIDST_0_OUKIN-TECH-SECURITY.XML