



Web threats to surpass e-mail pests

By Joris Evers

http://news.com.com/Web+threats+to+surpass+e-mail+pests/2100-7349_3-6178930.html

Story last modified Wed Apr 25 06:17:12 PDT 2007

SAN FRANCISCO--By next year, Internet users can expect more cyberattacks to originate from the Web than via e-mail, security firm Trend Micro predicts.

E-mail has traditionally been the top means of attack, with [messages laden with Trojan horses](#) and other malicious programs hitting inboxes. But the balance is about to tip as cybercrooks increasingly turn to the Web to attack PCs.

"By 2008, most of the threats you are facing will be Web placed. Today most of it is still e-mail," Raimund Genes, Trend Micro's chief researcher, said in a presentation at the Gartner Symposium and ITxpo here on Monday.

The reason for the flip is simple. Security tools for e-mail have become commonplace, but the same isn't true for Web traffic. Security firms have found it tough to secure what comes into a network and computers over port 80, the network port used to browse the Web using the hypertext transfer protocol, or HTTP.

"You can't block port 80," Eva Chen, Trend Micro's chief executive, said in an interview. "It is different than e-mail. E-mail is store and forward. HTTP is real time and you need to be able to deal with the latency in the user experience."

In a recent example of Web threats, miscreants broke in to the Dolphin Stadium Web site and [rigged it to load malicious software onto Windows PCs](#). The incident happened just before the Super Bowl was to be held at the stadium.

It is part of the classic rat race between security firms and cybercrooks. This has spawned an underground market for security vulnerabilities. Many of the bugs offered will [let an attacker silently commandeer a PC through the Web](#) when the unsuspecting user hits a site that packs an exploit, so-called "drive-by" installations.

"Malware for profit is definitely driving these Web threats," Genes said. "The last real virus we had was in 1999, Melissa. Since then it has been mostly worms and Web threats."

Criminals are offering up to \$75,000 for a Windows XP vulnerability and \$50,000 for a Windows Vista vulnerability, Genes said. Security firms such as VeriSign's iDefense and 3Com's TippingPoint pay around \$12,000, he said. "The good guys are paying, but the bad guys are paying more," Genes said.

The security firms will report a bug to the software maker so it can be fixed and add protection to their products while a patch is in the works.

The Web threat hasn't gone unnoticed by the security industry, but securing Web traffic for corporate users has primarily been the [terrain of specialized companies](#) such as Websense, Surf Control and ScanSafe. All these companies offer products or services to block known malicious sites or scan Web traffic.

"The big guys, including ourselves, have not been able to keep up with the hackers. The threat landscape changes so fast," Chen said. Trend Micro is the third-biggest antivirus company in the world, after Symantec and McAfee.

But Trend Micro is getting ready to launch an updated version of its security product for corporate desktops that includes a new Web security feature. The new technology sends every Web query to a Trend Micro data center and will block access to known malicious sites. If Trend Micro doesn't know the site, the company will scan it.

[Copyright](#) ©1995-2007 CNET Networks, Inc. All rights reserved.