COMPUTERWORLD
Development



# NY Times warns of rogue antivirus on Web site

**Robert McMillan**

**September 14, 2009** (IDG News Service) Online scammers have apparently found a new way to reach their marks: They've started running ads on the Web site of The New York Times.

The newspaper warned readers Sunday that so-called rogue antivirus sellers had been spotted on its Web site, NYTimes.com. Their products, often promoted by Eastern European criminal organizations, are either ineffective or actually end up infecting the computers of people who purchase them.

"Some NYTimes.com readers have seen a pop-up box warning them about a virus and directing them to a site that claims to offer antivirus software," the Times said in a "Note to Readers," posted to its Web site Sunday. "We believe this was generated by an unauthorized advertisement and are working to prevent the problem from recurring." The newspaper did not respond to a request for more information on the issue.

Because online advertisements are usually sold through networks, sites like NYTimes.com often have to rely on other companies to make sure that the ads they carry are appropriate.

Blogger Troy Davis was hit with the ad Saturday night. After taking a closer look, he discovered that JavaScript code in a New York Times ad redirected him to a Web site that popped up a browser Window designed to look like it is conducting a scan of the system. The window warns, "Your computer is infected."

"It's a fake page for a nonexistent antivirus app, which is actually malware," Davis wrote in his analysis of the issue.

The rogue antivirus problem got a lot of attention one year ago, when Microsoft and the Washington State Attorney General's office sued a pair of Texas companies for allegedly pushing the software.

Since then, things have only gotten worse.

In the past three months, rogue antivirus software has emerged as a major online problem, according to Paul Ferguson, a researcher with antivirus vendor Trend Micro. "Its pervasive," he said in an instant message interview. "Right now, they are going full-tilt."

Criminals use a variety of tricks to get people to shell out for the bogus products: They use search engine optimization techniques to get search engines like Google to list Web sites that display the pop-up ads, or they'll flog them through social media sites like Twitter or Facebook. They even use malicious Trojan horse programs to pop up error messages in hopes that people will buy.

"It's a multimillion dollar business," Ferguson said.