Antivirus software often fails to deter hackers

October 3 2013, by Steve Johnson

At a time when millions of computer users face increasingly sophisticated cyberattacks, the antivirus software they rely on to keep their information safe frequently fails to do the job.

Of 45 pieces of malware that lingered on the New York Times computer systems for a third of a year, just one was spotted by its antivirus software, the newspaper disclosed in January. That same month, security company Kaspersky disclosed a global data-stealing scheme had evaded detection by antivirus products for five years.

Such examples are becoming alarmingly common. Recent studies have found much of the malware-fighting software on the market is virtually useless against the growing onslaught of attacks.

"Every couple of months you see there's this major virus outbreak that everybody missed," said Jeremiah Grossman of Santa Clara, Calif.-based WhiteHat Security. "The cards are stacked in the bad guys' favor."

With global spending on antivirus products expected to hit $8.4 billion this year, according to research firm Gartner, he added, "people are paying good money to be less secure."

Campbell, Calif.-based ClickAway's stores repair about 60 infected computers a day, and about two-thirds of them have antivirus software on the machines, said Executive Vice President Oliver Rowen. Jeremy Prader, who sees similar problems at his San Jose, Calif., computer

repair business, The Cheap Squad, added that the crooks "are coming up with something new every day."

Indeed, Kaspersky says it encounters about 200,000 new malware varieties daily compared with only about 25 per day in 1994, 700 in 2006 and 7,000 in 2011.

That's a big problem because antivirus products mostly spot known malware, not new forms. Plus, hackers have gotten more devious, said Wade Williamson of security firm Palo Alto Networks, noting that sophisticated crooks can disable antivirus software while making it appear the software is still working. Other experts say hackers routinely fine-tune their malware against antivirus products to make their code harder to detect.

Although antivirus comparison tests vary widely, some have found grave weaknesses in many of the products.

Of 11 commonly used security programs tested last year by Texas-based NSS Labs, most were found to be "not providing adequate protection," and even updated versions failed to spot malware that had been rampant for years.

When Palo Alto Networks this year scanned about 70,000 malware varieties with a half-dozen antivirus products, it found about 40 percent "were not detected."

A study of 42 antivirus products last year by Imperva of Redwood City, Calif., and the Technion-Israel Institute of Technology determined that the initial detection rate of a newly created virus is less than 5 percent.

Many experts say having the software is better than nothing and that computer users often invite malware by letting their antivirus service

lapse. That's what 25-year-old Jessie Trujillio suspects may have caused his laptop to become infected a few months ago.

"I forgot to renew it, so boom, I guess I got some kind of virus," said the San Jose State University industrial-engineering student, adding that the malicious code fouled up his Web searches by "redirecting me to another site."

Nonetheless, security specialists contend the public needs more help warding off hackers. After all, the experts say, cyberthreats can be complex and confusing. Moreover, while large corporations have IT departments to shore up their computerized networks and often spend heavily on layers of protections, they add, most consumers rely solely on antivirus software to shield them from crooks.

Many antivirus companies are working to improve their products. Instead of just concentrating on detecting known malware, for example, their software scans for unusual behavior and blocks anything not known to be safe.

Still, "when you have a well-funded adversary, they're always going to find chinks in the armor," said Randy Abrams, NSS Labs' research director.

Amichai Shulman, Imperva's chief technology officer, agreed, saying he fears the threat posed by hackers will worsen unless a more comprehensive approach is devised to combat cybercrime.

"Ultimately, it is up to governments and law enforcement to create a more reasonable online environment," he said, adding that what we have now resembles "the legendary Wild West."

—-

TIPS FOR COMBATING HACKERS:

Comparison tests of antivirus products - including some that are free - vary widely. So experts advise anyone looking for a good version to check multiple tests, such as those by AV-Comparatives, AV Test and PC Magazine. More comparisons can be found by doing a Google search for "antivirus reviews" or "antivirus tests."

Be especially careful of antivirus promotions that pop-up on computer screens, experts warn. That's because some of them are bogus and designed to infect computers with malware.

Computer users also are advised to keep their antivirus products and operating systems updated and to never click on links or attachments in emails from unfamiliar sources. If you suspect your computer is infected, experts say, stop using it for online banking, shopping or other activities that require passwords or other personal information.