v
e-newsletter
COMDEX Marketplace
Subscribe
Submit Content
Previous Issues
Email this Page
Email this Issue
Contact
current event
COMDEX Chicago 2002
Registration
upcoming events
Spring VON 2001
COMDEX Vancouver 2002
Seybold NY 2002
VoiceCon 2002

Behavior blocking repels new viruses

By Ellen Messmer, 01/28/02

The future of computer viruses seems clear enough: ever more destructive "hybrid worms" that take advantage of software vulnerabilities and destroy files, leave behind holes for hackers to exploit, then scan for new victims at lightning speed.

Viruses such as last year's Code Red and Nimda are overrunning traditional antivirus software and intrusion-detection systems.

Related Links:

- **Learn how to build a powerful vulnerability testing toolkit at the "Hacking Your Own Network: Vulnerability and Penetration Testing" session, part of the High-Velocity Computing Conference at COMDEX Chicago 2002. To register, click here!**
- email this story to a friend
  HELP: set up your email

These products require updated "signatures" to detect and stop most new viruses, possibly leaving a several-hour window when even the best-prepared organizations are at risk.

Although antivirus software vendor Sophos identified 1,000 new viruses last year and such viruses are said to be costing companies billions of dollars on eradication efforts and in lost productivity, the virus writers haven't won this battle yet. Increasingly popular technology - dubbed behavior blocking - is starting to prove itself a worthy adversary.

"It did stop Code Red and Nimda," says Jay Ward, senior network security analyst for First Citizens Bank in Raleigh, N.C., which uses Entercept's behavior-blocking software to protect a Windows NT server running an online banking application.

Behavior-blocking software runs on server and desktop computers, and is instructed through policies that network administrators set to let benign actions take place but to intercede when unauthorized actions occur. Unacceptable behavior can take the form, for example, of a program that attempts to mass mail itself or that rummages around in registries. Behavior-blocking software can set aside suspicious code in a so-called "sandbox," keeping it from causing harm while a network administrator decides whether the code is nefarious.

Behavior-blocking software is available primarily from small companies such as Okena, Entercept and Pelican Security.

ENRON EFFECTS

"Ironically, the most immediate outcome from Enron will likely be the enrichment of the very professions that contributed to the mess."

Source: HBS Working Knowledge, 2002

Inside this edition

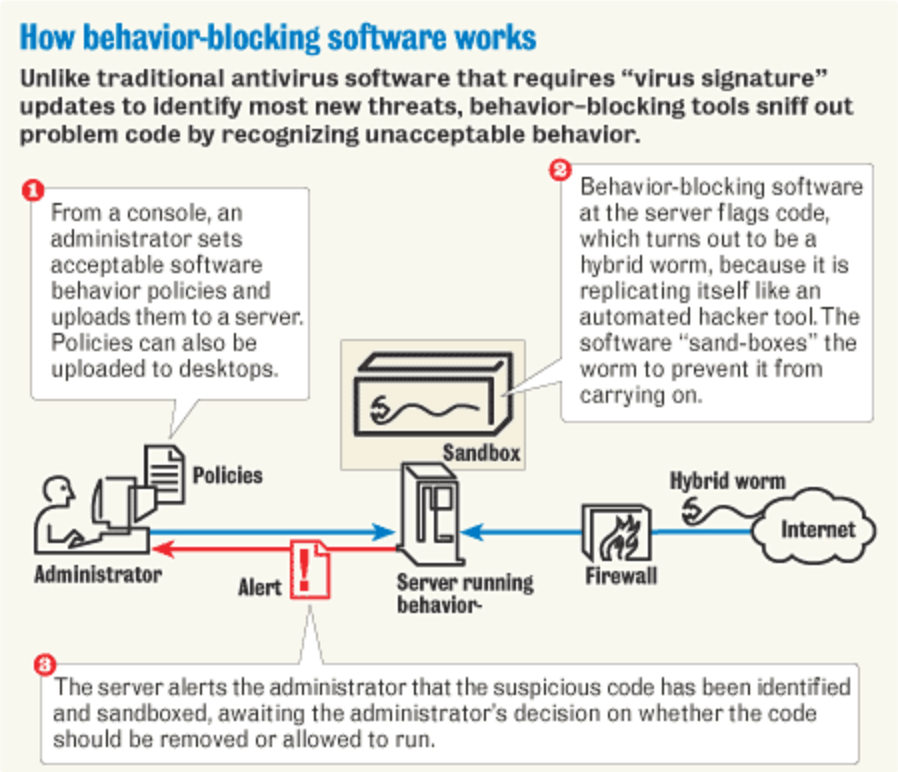
Analysts also mention Aladdin Knowledge Systems, Finjan, Granite Technology, Sandbox Security, Secure4You and even old-timer Harris as companies carving out niches in protection against malicious code.

So far, traditional antivirus software companies have shown little interest in behavior-blocking, which observers say may be a mistake.

"Based on signatures, antivirus software on the desktop is dying," says John Pescatore, an analyst with Gartner. "We need behavior-based interception."

Behave yourselves

While custom say they aren't necessa abando their signatu -based antiviru softwar they are starting to comple it with behavio -blocking products.



First Citizens Bank's Ward gave Version 2.0 of Entercept's behavior-blocking software a whirl after learning he couldn't patch known holes in the company's Microsoft servers without messing up an online banking application.

In mid-July, the Entercept software blocked and sandboxed unknown code it identified simply as a "Microsoft Directory Transversal Attack." By the next day, the world had identified the same code string as Code Red, Ward says.

Still, First Citizens Bank isn't about to dispense with its traditional antivirus software, which Ward says is effective at removing known viruses and in cleanup when viruses make a successful strike. However, he pointed to at least one case in

which running both behavior-blocking and antivirus software slowed down an NT server, which meant the antivirus software had to be turned off.

Hosted-service provider Corio is also sold on behavior-blocking software, which it used to stop Code Red and Nimda.

"We use the software as a layer of prevention," says Mark Milatovich, Corio's director of security. "The current model of the world - the antivirus model at the gateway, server, mail exchange and desktop - is a cat-and-mouse scenario. Antivirus software is only as good as those signatures. There's a window of exposure even with due diligence. We need prevention because these worms will get nastier."

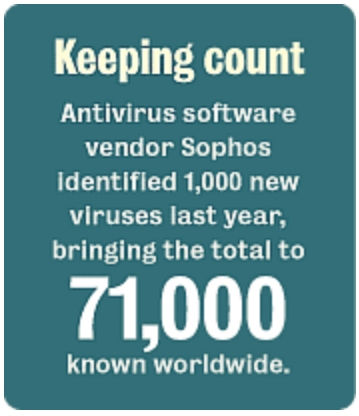
Staying the course

In spite of such evidence that behavior-based software works, traditional antivirus vendors are largely ignoring the technology. Computer Associates, Network Associates, Sophos and Symantec say their tools will remain signature-based for the foreseeable future. Among other things, they point out that behavior-blocking software isn't geared toward eradicating viruses.

"For the foreseeable future, it's a matter of how up to date are you with signatures," says Sam Curry, McAfee.com's security architect.

While some vendors give behavior-blocking tools a modicum of respect, others are more critical.

"It brings a higher degree of false positives," says Vincent Werf, Symantec's senior director of security response. Symantec touts the "heuristics" capabilities in its Norton Antivirus products as able to detect some unknown viruses without signature, but Werf admits that heuristics didn't detect or stop Code Red or Nimda.



Challenges acknowledged

Even behavior-blocking product vendors say using their wares can be challenging. For one thing, it can be tricky to devise policies that ensure the software can distinguish between good and bad behavior.

"It's difficult to write generic rules that screen valid requests

for data from invalid attacks," says Chad Harrington, product director at Entercept.

Behavior-based software also asks a company's IT administrators to be arbiters of whether suspect code, once it is flagged, is actually bad. Not only does this put an administrator on the spot, it could create a delay in action being taken.

But some customers are eager to give the software a chance.

"Behavior-blocking technologies could be easier to manage" because they don't require signature updating, says David Yaacobi, manager of information services at El Al Airlines. The company just deployed Sanctum's AppShield software to keep hackers from getting into its network through a public Web server and is investigating software from Pelican to help guard the airline's desktops.

Interestingly, although behavior-blocking software can stop harmful worms, most vendors that make it are reluctant to press their wares as a substitute for traditional antivirus code. "We don't protect against viruses, such as disk viruses not introduced from the Internet," says Gilad Golan, Pelican's president.

"We don't replace an antivirus product," Entercept's Harrington says. "The best way to stop intrusions is through both, because not all attacks can be detected through behavorial rules."

Ultimately, network executives have to decide whether they are willing to pay for behavior-blocking software, especially where it is seen as being merely complementary to traditional signature-based antivirus or intrusion-detection software that companies may already be spending $25 or more on per desktop. Behavior-blocking software costs roughly $50 or $60 per desktop and between $1,000 and $1,600 per server.

email this story to a friend
HELP: set up your email
Back to Top Stories
Top of this page