

CIO DECISIONS

UNDER FIRE

DESPITE THE SAME OLD BUDGETS AND RESOURCES, MIDSIZED COMPANIES HAVE TO CONTEND WITH NEW AND MORE COMPLEX SECURITY ATTACKS. HERE'S HOW A FEW ARE RISING TO THE CHALLENGE. BY JAMES CONNOLLY

MICROSOFT DISCOVERS a vulnerability in its domain name server but says it may take weeks to deliver a patch, and the W32/Delbot-AI worm promptly launches attacks using that flaw. Two research houses predict that pinpointed attacks on select companies will soon replace broadly targeted worms as the greatest threat to corporate computer security. At a Usenix conference, experts warn that botnets—which use a collection of compromised computers to steal financial data or send spam—are getting increasingly complex and more capable of taking over more computers and accessing important data.

That was just some of the bad security news that came out in a single week this spring. While information security teams still struggle to plug new holes in technology and avoid broadly targeted viruses, they have to keep an eye on the threat of a carefully architected and targeted multi-vector attack.

Information security managers know that teams of hackers are working around the clock to craft multi-vector attacks, pairing the best and brightest of the bad guys. These attacks probe a company's network simultaneously in several ways—leveraging spam, searching for gaps in firewall coverage—thus giving hackers a better chance to find a hole in a company's security. Multi-vector attacks clearly raise new challenges for midmarket companies strapped with the same limited resources. Yet smart CIOs are turning the tables and adopting a multifaceted approach to defense that employs several security technologies as well as tools from outside the security realm.

Just how prevalent are multi-vector attacks? “The sense of people

deliberately banding together to put some multi-vector threats together is relatively new,” says Stephen Fried, vice president for information security and privacy at Milwaukee-based Metavante Corp. “When you take a look at the history of attacks that we've been seeing in the past few years, there has been a lot more talk about multi-vector than we've actually seen in the wild, but I think its day will come.”

AFTER WEIGHING THE PROS AND CONS OF FOUR VENDORS, HE CHOSE TRIGEO NETWORK SECURITY INC.'S SIM SOLUTION. “IT WAS ALMOST A LIVE-BY-LUNCH SOLUTION THAT REQUIRED VERY MINIMAL SETUP,” HE SAYS. “IT WAS PRICED VERY COMPETITIVELY AND MET ALL REQUIREMENTS THAT I HAD, INCLUDING MINIMAL MANAGEMENT AND TOTAL COST OF OWNERSHIP.”

Multi-vector attacks can take many forms. For instance, an attacker who uses social engineering to gain personal information from users might join forces with someone who uses distributed attacks or distributed spam networks, says Scott Crawford, senior analyst at Enterprise Management Associates (EMA) in Boulder, Colo. “The ability to work to-

LIKE WILLFORD, BRISCOE CHOSE TRIGEO. SHE SAYS IT NOT ONLY OFFERS FUNCTIONALITY THAT BEATS OUT COMPETITORS, SUCH AS DESKTOP AGENTS AND USB LOCKDOWN, BUT IT ALSO FOCUSES ON THE MIDMARKET, SO THE PRICE WAS RIGHT. THE BANK WAS PAYING ABOUT \$120,000 A YEAR FOR LIMITED COVERAGE OF ITS SYSTEMS; FOR A LITTLE LESS THAN THAT ON A ONETIME PAYMENT, BRISCOE GETS ADDED FUNCTIONALITY AND NETWORK-WIDE COVERAGE.

gether in order to achieve common goals is getting to be a much more serious concern, which raises the bar even further on the ability of IT to be able to cooperate with security and leverage integration across IT to achieve their own common goals.”

Several factors set a multi-vector attack apart from the general release of, say, a virus or worm. First, a multi-vector attack targets a specific company, often with the intent to do harm or steal information. It also uses several avenues to gain entrance, with one or more of those attempts often acting as a decoy to divert the security team’s attention from the real attack.

“Midmarket companies are exposed to the same types of threats as larger companies, although they probably are more at risk from multi-vector attacks,” says Jerry Murphy, vice president and service director at Robert Frances Group. “It used to be that security threats were like high-school kids coming by and toilet-papering a house. It was obvious that it happened, and it looked really nasty, but at the end of the day nothing was really damaged. Today, the threats are much more like spies watching from behind the bushes at all the entrances to your house to see where you hide the key so when you’re gone they can sneak in and steal stuff.”

SIMPLY SECURE

Some CIOs draw on multiple security technologies to defend against multi-vector attacks. Security information management (SIM) systems, for instance, monitor and analyze huge volumes of data in the logs of firewalls, intrusion detection systems and other tools to spot attacks, thus taking the burden off human eyes.

“The challenge I have from the SMB perspective is having the staff and cost-effective tools to monitor all of our systems,” says Mark Willford, manager of IT at DirecTV Castle Rock Broadcast Center in Castle Rock, Colo. “We don’t have the luxury of having a dedicated security department. I have a staff of 19 people that is responsible for everything from toner replacement to managing a very large ATM backhaul network. So my staff wears a lot of hats, and part of our responsibility is making sure that our data is secure.”

Willford wanted a system that could correlate log files from various servers, firewalls and other components and offer real-time alerts about suspicious activity. He also wanted to be able to audit those log files. After weighing the pros and cons of four vendors, he chose TriGeo Network Security Inc.’s SIM solution. “It was almost a live-by-lunch solution that required very minimal setup,” he says. “It was priced very competitively and met all requirements that I had, including minimal management and total cost of ownership.”

The SIM system correlates most of the security device log files and provides real-time alerting by tracking event data from multiple firewalls, switches, routers and intrusion detection systems. Willford notes that his company may be an exception in the midmarket; rather than looking back after a problem occurs, he proactively audits logs. “We’re able to catch things a lot earlier in the process, especially with virus activity that isn’t necessarily recognized by one device but is

recognized when correlated between two devices,” he says. Previously, virus activity or a denial-of-service attack may not have been spotted until users complained.

Another midsized organization turned to SIM because it was a cost-effective way to extend the reach of its alerting capabilities. For about a year, Stillwater National Bank in Stillwater, Okla., had outsourced key monitoring functions such as alerting. While the monitoring service worked fine, it covered only one-fifth of the bank’s 100 servers. It also didn’t provide crucial log monitoring and reporting functions, including those required by various regulations such as the Sarbanes-Oxley Act, the Health Insurance Portability and Accountabil-

“WE’RE ABLE TO CATCH THINGS A LOT EARLIER IN THE PROCESS, ESPECIALLY WITH VIRUS ACTIVITY THAT ISN’T NECESSARILY RECOGNIZED BY ONE DEVICE.”

—MARK WILLFORD, DIRECTV CASTLE ROCK BROADCAST CENTER

ity Act, and the Gramm-Leach-Bliley Act, says Laura Briscoe, vice president for information security at the bank.

“We already had the need for this type of monitoring. Your auditors and the laws all require that you have this type of monitoring and reporting in place, that you know who’s accessing what kind of data on which box,” says Briscoe.

Rather than extend its commitment—and annual payments—to the service provider, the bank looked at in-house SIM technology. Like Willford, Briscoe chose TriGeo. She says it not only offers functionality that beats out competitors, such as desktop agents and USB lockdown, but it also focuses on the midmarket, so the price was right. The bank was paying about \$120,000 a year for limited coverage of its systems; for a little less than that on a onetime payment, Briscoe gets added functionality and network-wide coverage.

But it’s important to note that SIM technology is still evolving. One IT manager says that SIM’s data monitoring rules, which vendors often define, allow SIM to catch some kinds of attacks but not all. Murphy says that SIM also presents a resource challenge for midsized companies, which are less likely to have a dedicated analyst who can make the most of such a system through heuristic analysis. “There are some tools starting to put this stuff together,” Murphy says. “But usually some human being has to put the rules in there to say what all this information coming from different locations means.”

Research labs are developing technology to help midmarket companies better utilize SIM, creating tools that use histogram analysis to spot anomalies in SIM reports. The histogram would help map the mean behavior for traffic associated with specific applications. So if there is an increase in traffic on part of the network—a sign of a possible problem—an administrator could investigate. There may be a legitimate business reason, such as a special promotion, that creates additional activity surrounding that specific application, or it may be caused by malware.

Excerpted with permission from CIO Decisions, June 2007.

© 2007 TechTarget. All Rights Reserved. FosteReprints: 1-866-879-9144