Securities Industry News
www.securitiesindustry.com
OCTOBER 1, 2007

# Hackers Up the Ante, Network Protectors Respond

*Security specialists use unified, intelligent systems to thwart attacks*

By Maria Trombly

Once a hobby popular with teenagers, hacking has evolved into a multinational, multibillion-dollar industry that utilizes ever-more sophisticated techniques to penetrate companies' information technology security systems. Targeted cyberattacks can now inflict substantial damage on a financial services firm.

"The hackers aren't doing it for fun anymore," says Gene Manyak, product marketing manager at Redwood City, Calif.-based Check Point Software Technologies. Ten years ago, Manyak notes, a company could settle for an "M&M" security model: "a hard shell on the outside, and the inside was soft and chewy." That form of defense is no longer sufficient. "Today, everything is connected," he says. "Laptops get plugged in, go home, then plug in again the next day."

There are threats in such mobility. In August, a Merrill Lynch & Co. laptop holding sensitive data—including Social Security numbers of 33,000 employees—was stolen. According to a study conducted by Traverse City, Mich.-based research firm Ponemon Institute, 73 percent of corporations experienced the loss or theft of a data-bearing asset during the last 24 months. The survey of 735 senior IT security professionals, released in June, also reported that 70 percent of data breaches result from the loss of off-network equipment.

Employees, suppliers and partners connect to networks through virtual private networks, smart phones and instant messaging. And even as the perimeter grows increasingly vulnerable, the network and applications that allow those off-network connections are facing new challenges.

Inno Eroraha

## New Openings

"We have financial services clients that worry about Web 2.0 applications that run in their network," says Tom Turner, VP of marketing at Waltham, Mass.-based security firm Q1 Labs. "We have hedge fund clients, for example, that worry about the use of tools like Plaxo"—an online address book—"that allow the exchange of personal information. We have a hedge fund that outright denies its employees the use of Plaxo in the network because it doesn't want the database of the hedge fund's partners and investors to float away over the network." It's not easy to catch the leakage of information, he says. "You need to understand the nature of applications on the network."

Wireless technology is also a common source of access for hackers. Large brokerages have hundreds of offices around the world, and it's easy for an employee or group to set up an unapproved wireless network in a remote office. "Employees think that if they put in a request to IT, it will take months," says Greg Murphy, COO of AirWave Wireless in San Mateo, Calif. "So they just take things into their own hands. If an employee has a wireless network in his house and wants the same kind of access at the office, he goes down to an office supply store, gets a device, and plugs it in." A wireless network installed by an amateur is likely not to have the security functionality that a brokerage would require.

Many devices such as laptops come with preinstalled wireless capabilities. Though a company may have a no-wireless policy, an employee can accidentally—or deliberately—turn on the broadcast functionality of a computer and create an "ad hoc" wireless network. At a consulting group with five people, "one of those users might connect to the wired port and have the other four connect through the ad-hoc network," Murphy says. "That is potentially a very dangerous thing for organizations."

Firms can monitor for rogue wireless access points by scanning a network for devices that look like access points, or wandering the hallways with a "sniffer" to detect unauthorized networks. Neither of these techniques is likely to find an ad-hoc network that is only up for a short time, so many firms have begun to remove the temptation by setting up their own, secure wireless networks. Such networks can also be used as around-the-clock sniffers to monitor the airwaves for unencrypted, unsecured traffic.

Gene Manyak

AirWave manages wireless networks for about 500 customers, 25 of which are in financial services. It says that its client have anywhere between 25 and 40,000 wireless access points.

## Standbys Get Updated

While hackers are continually looking for new paths into corporate networks, they've also been busy enhanced old methods. "Trojans have become very sophisticated and take advantage of vulnerabilities of Web client browsers," says Inno Eroraha, founder and chief security strategist of Sterling, Va.-based NetSecurity Corp., which has three financial customers, including a mutual fund and one of the country's three largest banks. Seventy percent of the company's business comes from U.S. government agencies such as the Department of Defense.

"My experience tells me that brokerages have filtering technologies in place at the application level that prevent attacks such as rootkit applications, which hide in the operating system and give hackers deep access into systems," says Eroraha. "The brokerage firms I work with have measures in place to harden the host systems so that they are not a target for Trojans, and are patched as well."

But brokerage firms can be vulnerable to internal threats, he says, especially in newly deployed systems that are installed with default configurations. "In an assessment we did recently, we were able to compromise a lot of systems because they had weak configuration settings," he says.

If a firm's security operations are not adequately staffed, personnel may wait until the next update cycle to install a new patch—or miss an old one. "Some Trojans are successful because a ten-year-old patch or a five-year-old patch hasn't been applied," Eroraha says.

Another traditional hacking tool, spyware, has become ubiquitous on computers, though a majority of it is harmless software that tracks Internet usage to better target advertising. Spyware detection has not be a high priority for enterprises, due largely to the perception that it is relatively benign.

"We've seen a 60 percent spyware infection rate" in large companies, says Michael Irwin, COO of Webroot Software in Boulder, Colo. Over time, spyware can build up and crash computers, he says, overwhelming help desks with employee calls. Spyware also tends not to be securely written and can be easily accessed by hackers. "Something else can come in and attach to that [spyware] and start directing traffic on your computer," he says.

Hackers can combine several of the tools at their disposal to create customized attacks aimed at high-profile institutions—and financial firms like brokerages are near the top of the list, since that's where the money is.

In a "spearphishing" attack, an e-mail is sent out to a select group of people, or even a single person, to obtain information or entice the recipient to download malware. Spearphishing is hard to detect, says Steve Booth, director of security operations for VeriSign's managed security services unit. While ordinary phishing attempts are comprised of thousands—or millions—of e-mails and show up on the radar screens of security companies, spearphishing is more tightly focused. The e-mails are meant to appeal to a specific individual or group and sometimes appear to come from a trusted person. They don't look like spam and often include up-to-date company news.

Greg Murphy

It can be worth a lot to a hacker if a CFO clicks on a bad link. "If they can get the high-value target to click the link or accidentally install the malware, then they're going to have a much higher payload," Booth says.

On the other extreme are targeted attacks that use every tool in a hacker's arsenal. Multi-prong attacks may try to install as many as 3,000 different files on a single computer, according to Booth. By hitting their target with every piece of malicious software available, "the bad guys have a much higher likelihood of owning that box," he says.

## Unified Systems

To fortify their networks, firms increasingly rely on intrusion protection systems and unified threat management to bring security solutions together. Technology company Unisys, says that it has clients that use over 15 different security solutions for protection. "Each individual product centralizes, but how do you tie this information together?" says Tim Kelleher, VP and general manager of enterprise security at Unisys Federal Systems. "By combining the data, organizations are able to better see the bigger picture. Without consolidating all these disparate security solutions, it is extremely challenging to stay on top of any kind of threat."

Check Point's Manyak says that the ultimate goal is to unify various aspects of network security into a single threat management system with one interface. "It's really hard to do," he says. "But that's something that's really [become] top-of-mind in the last year and a half or so."

Michael Irwin

A consolidated defense system must keep up with log data from the various security devices and appliances, and use that information to block malicious traffic and identify multi-prong attacks. When attacks do come, the system needs to be able to react instantly.

Sealing off access points is an effective way to block attacks, but can hurt business. There are, however, other ways to defend a network, such as making communication channels secure. Companies can rank incoming traffic by its perceived trustworthiness. "Normally, I would block something I considered to be an attack if the confidence level, was, say, under 95 percent," Manyak says. "If I see evidence of a coordinated attack, I might drop that confidence level to 80 percent. I might be blocking more traffic, but it might be a worthwhile tradeoff."

Even internal traffic can be ranked, with less mission-critical messages delayed or scrutinized more closely. Internal encryption is becoming an increasingly viable alternative, notes Manyak. Encryption can also help protect data stored on laptops and other mobile devices, he adds.

Checkpoint offers both encryption tools and a unified threat management product. "That M&M model of security doesn't work anymore," says Manyak. "You need a candy that's hard and crunchy all the way through." ■

netSecurity™

## Corporate Overview

NetSecurity is a digital forensics, security consulting and training company. We work with you to understand the unique goals and requirements of your business. Then we provide tailored, high quality, customer-focused, and cost-effective solutions.

- Our hands-on security solutions protect you against emerging security threats and help you manage your enterprise security risk proactively
- **NetSecurity Forensic Labs** delivers solutions that help you acquire, preserve, analyze, and produce digital evidence promptly
- Our proprietary **Hands-On How-To**® training program provides you with the knowledge of real-world security issues through simulated and "how-to" exercises that enable you to do your job successfully

## Solutions Overview

| NetSecurity Forensic Labs | Hands-on Security Solutions | Hands-On How-To® Training |
|---|---|---|
| ∞ Electronic Discovery | ∞ Security Assessments and Audits | ∞ Web-based Applications |
| ∞ Computer Forensics | ∞ Technology Implementation and Integration | ∞ Database Systems |
| ∞ Cybercrime Response | ∞ Infrastructure Security | ∞ Network Systems |
| ∞ Forensics Training | ∞ Regulatory Compliance (SOX, PCI, HIPAA, ISO, FISMA, etc.) | ∞ Operating Systems |
| | | CISSP® Certification Training |

## Contact Information

NetSecurity Corporation
21010 Southbank Street
Suite 210
Sterling, Virginia 20165

**Phone:** (703) 444-9009
**Fax:** (703) 444-6899
**Toll Free:** 1 (866) 664-6986
**Email:** Info@NetSecurity.com
**Web:** http://NetSecurity.com