

Deploying New Tools To Stop the Hackers

By CHRISTOPHER DREW and VERNE G. KOPYTOFF

Trying to secure a computer network is much like trying to secure a building — the challenge is trying to screen out real threats without impeding the normal traffic that needs to go in and out.

And as the recent hacking attacks against Citigroup, RSA Security and Lockheed Martin show, even sophisticated security systems can be breached.

“We’re seeing an inflection point where the attackers are extremely smart, and they are using completely new techniques,” said Nir Zuk, the chief technology officer at Palo Alto Networks, a firewall company based in Santa Clara, Calif. “Every piece of content that you receive can attack you.”

Historically, the first line of computer defense, the firewall, is like the guard desk at a building. It scrutinizes the traffic going in and out of the system, looking for obviously suspicious characters.

Virtually every company also has antivirus software, which typically keeps an eye out for anything on a “black list” of well-known malware and prevents it from entering the computer system or causing havoc once inside. A more rare type of security grants access only to programs on a “white list” of safe software— the equivalent of allowing employees with ID cards to come and go as they please but preventing anyone else from entering.

But as hackers unleash ever-sneakier attacks, big

Continued on Page 2

As Security Threats Grow, Companies Scramble to Deploy New Tools to Stop the Hackers

From First Business Page

corporations and government agencies are scrambling to deploy new tools and procedures to deal with all the delicate gray areas in between — the cool-looking new smartphone app, the funny Facebook link, the unknown foreign Web site. The flood of malicious software is also prompting renewed debate over how to balance access and protection.

"Right now, if an application is not known, we let it run," said Peter Firstbrook, an analyst at Gartner, a research firm, referring to the prevailing view in most companies. "That's the wrong thing to do."

Companies like Symantec, the giant Internet security firm, are introducing services that assess the "reputation" of software, weighing factors like how old it is and how widely it is used to decide if it is safe. Other vendors are selling enhanced firewalls and products that can sniff out impersonators by detecting unusual file-usage patterns.

Nearly everyone agrees that a mix of defenses is vital, and that even so, some hackers will still slip through. Experts also say that the proliferation of smartphones, the growing workplace use of Facebook and other social media tools, and the shift toward storing more data in a computing cloud are providing new avenues for attackers.

Symantec's chief executive, Enrique Salem, acknowledged at a conference in February that traditional antivirus scans "long ago failed to keep up." As points of entry into corporate and government networks "proliferate on this seemingly insane trajectory," he added, "so do the threats they attract."

The growth in malicious software has been staggering, as criminal organizations seek to

ferret out credit card numbers and other ways to make money and hackers in China and Russia are believed to be seeking national security secrets.

Last year, Symantec discovered 286 million new and unique threats from malicious software, or about nine per second, up from 240 million in 2009. The company said that the amount of harmful software in the world passed the amount of beneficial software in 2007, and as many as one of every 10 downloads from the Web includes harmful programs.

Unlike past blitzes of spam with clunky sales pitches, today's attacks often rely on a familiar face and are extremely difficult

to stop. In a practice known as spear phishing, hackers send e-mails that seem to come from co-workers or friends and include attachments that can release malware to steal passwords and other sensitive data. In other cases, malware can be activated when a Web link is clicked.

Some security experts say companies can better protect themselves against such attacks by expanding the use of "white lists," which are currently in place in only 10 to 20 percent of the computers in large organizations.

Bit9, a Massachusetts company that offers such a white-list service, says it has millions of approved applications in its registry. Federal agencies, retailers, Wall Street firms and technology companies use its real-time mon-

itoring services, which can be set to block unknown software or simply issue alerts about it.

Harry Sverdlow, Bit9's chief technology officer, said its monitoring system stopped an attack on a national defense laboratory in March that was almost identical to the hacking that month at RSA Security, which eventually compromised the electronic security tokens that RSA sells to Lockheed and other corporations around the world.

Mr. Sverdlow said the attack on the lab came via an e-mail attachment with a heading implying that it was from the human resources department. He said a malicious file was embedded in the attachment, but the monitoring system stopped it when it noticed unauthorized activity.

Another strategy used to deflect attacks is to rate software based on its reputation. The technique, championed by Symantec, is supposed to be more flexible than strict white or black lists.

Symantec's strategy is to rate software based on a number of factors including the file's age and source. The company also checks data it collects from users about the kind of software they have on their computers. Software used by 100,000 people is more likely to be good, while a file that no one else has is more likely to be bad.

"You probably don't want to be the guinea pig," said Carey Nachenberg, a fellow with Symantec.

Reputational technology is available in Symantec's consumer products and will be deployed for corporate customers sometime later this year. The software, when used in conjunction with other techniques like black lists and monitoring for unusual activity, is 99 percent effective, Mr. Nachenberg said.

But security vendors like Mr. Zulk of Palo Alto Networks say that in real life, people are being



Symantec security technicians at an operations center in Alexandria, Va. Last year, Symantec discovered 286 million new threats from malicious software, or about nine every second.

bombarded with all kinds of links, and a security threat can be hidden in any one of them. "It's about clicking on a link or a presentation about how to improve your golf play," he said.

New security technology should protect against all sources of malicious files, whether they come in by old-fashioned e-mail, a LinkedIn feed or a Twitter link, Mr. Zulk said.

He said stronger firewalls, which monitor computer networks for suspicious traffic, could also help.

Security experts say companies must also adapt their security systems to protect against attacks through smartphones and tablet computers. Although such mobile devices increase convenience for workers, they essentially create a new door into the network, which then needs its own security watchdogs.

Mr. Firstbrook, the Gartner analyst, said that devices that run Google's Android software, which is open to all applications, were riskier than Apple iPhones and iPads, in which every application is screened by the company before it is allowed into the App Store.

And humans remain a prime weakness in all computer networks that no security system can completely offset, said Mark Hatton, chief executive of Core Security Technologies, a company based in Boston that tests corporate networks for security holes.

"You tell the guy not to click on the link to the free iPad, and he still always clicks on the link to the free iPad," he said.