

Tales of Cyber-Crime Running Rampant

When Donna Getgen opened a letter from her credit union in March, the message within was anything but routine. Getgen was informed that she had been the victim of a cyber-theft. Getgen's account number, the letter read, was stolen from a database at BJ's Wholesale Club Inc., where she shopped from time to time.

Stunned, Getgen, a business operations specialist for a high-tech company from Owings, Md., would later learn that she was one of tens of thousands of victims of one of the largest cyber-thefts in recent history.

As the number and scope of cyber-crimes proliferate, local, state and federal authorities are scrambling for resources to combat the threat. In many cases, the authorities are directing resources away from cyber-crime cases.

"Most Americans would be surprised to know that thousands of credit card numbers are sold online every day, and very little is done to stop it," said Jim Melnick, director of threat intelligence at iDefense Inc., in Reston, Va., and a former Defense Intelligence Agency officer.

The number of phishing attacks alone has grown by 1,200 percent in the past year, according to MessageLabs Inc., in New York. Phishing is the practice of sending fraudulent e-mail purporting to come from a bank, credit-card issuer or other trusted source to solicit account numbers, Social Security numbers and other sensitive data.

Despite the mounting research, bank officials contacted for this story said they, along with credit card issuers, are doing most of the education and prevention regarding cyber-crime without much help from law enforcement or government regulators. "Identity theft is escalating, and it's moving offline. We see people coming in here with stolen numbers trying to open accounts. It's happening."

In fact, of the 500 companies that responded to a recent FBI survey, 90 percent said they'd had a computer security breach, and 80 percent of those said they'd suffered financial loss as a result.

Today, online criminals use stolen credit card numbers as illicit currency. The information is traded for other commodities, such as Social Security numbers or access to networks of compromised PCs that can be used in distributed-denial-of-service (DDoS) attacks.

But as the cyber-crime rate climbs, security experts, consumers and even former government officials are questioning why federal lawmakers and administration officials have devoted so few resources to combating the menace. Many attribute the resource issue to the war on terrorism.

Indeed, in the months following the terrorist attacks of Sept. 11, 2001, counterterrorism became the highest priority for the FBI as well as the Secret Service, the two federal agencies responsible for the bulk of the government's cyber-crime investigations.

"Cyber-crime was put on the back burner. Pure investigations into cyber-crime have diminished at the FBI and the Secret Service."

That shift took its toll on the computer crime units at both agencies, and nearly 20 Secret Service agents who were working on cyber-crime at the time of the attacks were transferred to terrorism investigations.

"There's a broken spirit in the government as far as cyber-crime," the former agent said. "It's one of the most daunting tasks that law enforcement has ever had to deal with."

For those investigators at the FBI and Secret Service still responsible for handling cyber-crime—about 300 and 100, respectively—many are often pulled away from their regular duties to work on special details, which can lead to long delays in completing investigations.

"There just aren't enough agents to do what's required," the former agent said. "The response from the government hasn't been commensurate with the problem. The big investigations that you see on TV with the press conferences were the exception, not the rule."

According to government and law enforcement officials, the lack of interest in fighting cyber-crime comes from the top down and is traced to the current and past presidential administrations.

Ingram Micro Discloses Hacker Attack

Hacker attacks on businesses are on the rise, and these days generally are launched by more sophisticated and motivated perpetrators. The sophistication is making it more difficult for companies to secure sensitive employee and customer information, according to research firm Gartner. Even companies that distribute software and systems aren't immune. Ingram Micro Inc. last week disclosed in a letter to former and current employees that the company detected unauthorized access to its computer systems containing names and personal identification such as Social Security numbers, national identification numbers, and passport numbers for U.S. employees and their beneficiaries of health care, life insurance, and 401(k) benefits. The letter dated May 17 reveals that the computer distributor has no evidence of entry into specific personal-information databases, but wanted to alert employees whose stored information may have been compromised.

Taking precautionary measures, company officials recommended placing a fraud alert on credit files, and provided telephone numbers to Equifax, Experian, and Trans Union credit-reporting agencies.

But Ingram Micro isn't alone. Companies typically store employee and customer information in archived databases for seven or more years to accommodate Internal Revenue Service tax audits. As a result, companies need to do more to protect sensitive information, Gartner urged in a recently released study. The research firm suggested putting in place intrusion-prevention systems to block malicious actions. These intrusion-prevention systems need multiple algorithms to successfully keep out unauthorized access.

They also must provide blocking capabilities that include signature-based blocking of known attacks by moving beyond simple signature-based approaches, such as those used by antivirus and intrusion-detection systems, to at least support policy, behavior, and anomaly-based detection algorithms, Gartner suggested. These algorithms should operate at the application level in addition to standard, network-level firewall processing.

As intrusion-prevention systems mature, they will positively identify and block higher percentages of attacks than today's first-generation intrusion-prevention systems, Gartner said. However, the system will never be perfect, and it's always necessary to flag suspicious activity for further investigation by humans.

Many Wireless Networks Lack Security

While Wi-Fi Is Hot, Security Is Not

SAN JOSE, Calif. (AP)—With a laptop perched in the passenger seat of his Toyota 4Runner and a special antenna on the roof, Mike Outmesguine ventured off to sniff out wireless networks between Los Angeles and San Francisco. He got a big whiff of insecurity.

While his 800-mile drive confirmed that the number of wireless networks is growing explosively, he also found that only a third used basic encryption—a key security measure. In fact, in nearly 40 percent of the networks not a single change had been made to the gear's wide-open default settings.

"They took it out of the box, powered it up, and it worked. And they left it alone," said Outmesguine, who owns a technical services company. He frequently goes out on such "wardrives" in search of insecure networks. And while Outmesguine says he doesn't try to break in, others aren't so benign.

Even the makers of Wi-Fi routers, access points and other gadgets privately say that as many as 80 percent of home users don't bother to enable basic encryption or other protections against connection theft, eavesdropping and network invasion.

Experts say that while Wi-Fi hardware makers have made initial setup easy, the enabling of security is anything but. Meanwhile, average users are no longer tech savvy. The gadgets are mainstream, appearing on the shelves of Wal-Mart and other mass retailers.

continues on page 2

contents

Ingram Micro Discloses Hacker Attack.....1
 Many Wireless Network Lack Security.....1,2
 Six Reasons Linux has Enterprise Appeal.....3
 Tales of Cyber-Crime Running Rampant.....4

During his wardrive, Outmesguine counted 3,600 hot spots, compared with 100 on the same route in 2000. Worldwide, makers of Wi-Fi gear for homes and small offices posted sales of more than \$1.3 billion in 2003, a 43 percent jump over 2002, according to Synergy Research Group.

The result? A lot of wide-open networks that offer anyone within range of the Wi-Fi signal free access to a high-speed Internet connection. Any hacking is unlikely to be noticed, while illegal activity would be traceable only to the name on the Internet account.

"What we probably really have here is a whole bunch of very vulnerable systems exposed to attack or infection over a network that has no access control," said Al Potter, manager of technical services at the security firm TruSecure's ICSA Labs.

Companies that sell Wi-Fi products want their hardware to be simple and interoperable, especially as more than just computers—wireless TV monitors, digital music receivers, DVD players and game consoles, for example—are wirelessly connecting to home networks.

At the same time, they want to keep support calls and returns low, so they turn off security by default.

"We've been putting friendly front ends in front of technology for a long time," said Peter Evans, vice president of business development at AirDefense Inc., a wireless security firm. "I'm not sure why the industry has not yet made those tools much easier to use."

Yet even knowledgeable consumers find it frustrating to set up security. It can involve punching in dozens of characters as the passphrase for each connected device, and navigating screens filled with a dizzying set of acronyms for encryption and authentication.

Problems grow when consumers try to mix a laptop wireless card from one vendor with a Wi-Fi access point from another. With security turned off, everything works fine. With basic encryption turn on, the headaches begin.

Because his Linksys access point and Gateway notebook used different techniques for generating the "key" to scramble and unscramble the data, Victor Miller of Princeton Junction, N.J., learned he had to twice punch in dozens of characters using the hexadecimal numbering system.

That process is prone to typing errors, which aren't apparent since Windows XP doesn't display the characters as they're entered. Also, Miller said, the user guides did not say that the computer would require a restart.

Some manufacturers are beginning to tout security features as a selling point, just as they market faster speeds and greater signal range. Microsoft Corp., for instance, made the transfer of keys fairly easy by copying the key and other settings to a floppy disk that could then be used to configure wireless laptops. The company, though, announced in May that it was getting out of the Wi-Fi hardware business.

Users who don't secure their networks are often the very people who don't keep their computers up to date with the latest security patches and antivirus software.

Buffalo Technology Inc. has introduced a one-touch security system that exchanges keys between wireless devices and the wireless access point within a two-minute window after a button is pressed. Critics point out, however, that the system requires the manual entry of keys on non-Buffalo devices. And not all of Buffalo's products support the technology, called AOSS.

Meanwhile, Broadcom Corp., the leading supplier of Wi-Fi chips, has announced a software feature called SecureEZSetup that generates the encryption key based on answers to simple, easy-to-remember questions. Still, any device that's not supported must be manually set up, and only one vendor—Belkin Corp.—has so far publicly committed to using the technology.

The Wi-Fi Alliance, an industry group that certifies Wi-Fi-labeled gear, has posted educational videos on its Web site and recommends that vendors use automated setup tools in their products. But it has stopped short of mandating specific interfaces, said Frank Hanzlik, the group's managing director.

"Key to our strategy is consumer education," said Darek Connoles, media relations manager at D-Link Systems Inc.



Six Reasons Linux Has Enterprise Appeal

First and foremost, it has gathered momentum and a critical mass of developers, hardware vendors and software tools that enable the most complex of corporate applications to be created. It has become a standard part of the enterprise bag of tricks.

Jim Stallings is general manager for IBM's Linux business and oversees more than 6,300 engagements for IBM that are Linux-related. "Those are the ones that I know about, and that is more than double what we did last year," he says.

Second, Linux has appeal because it isn't Windows and doesn't carry with it heavy usage fees, disk footprints, and consumption of memory and other resources that typical Windows applications carry. Linux is also a lower-cost alternative to SPARC/ Solaris and HP-UX Unix-based computing: Put a collection of Intel rack-mounted servers together under Linux and you have lots more CPU horsepower-per-dollar. In some cases, enterprises are funding their Linux developments out of their saved annual maintenance contracts when they turn off their larger Unix mainframes.

Some of the motivation for being the anti-Windows OS comes from foreign governments, which are looking to standardize on a cheaper desktop alternative and don't want to continue to pay the Microsoft desktop support and licensing fees.

Third, Linux has important backers in the form of IBM, Novell, Oracle, Sun and others. These companies aren't doing it for the altruism of supporting open source or because they want an alternative to Microsoft, but because it makes good business sense, and because their enterprise customers are now demanding Linux in their server rooms and for their applications. And the latest versions of Linux are enterprise-ready, Oracle's Dargo says.

There is high-performance computing, selling the advantages of running Linux on clusters of IBM's Power CPUs. Some of these high-powered applications have to do with high-density processing, using server blade enclosures that can marry dozens or even hundreds of processors together to work. According to VARBusiness' State of the Enterprise survey, a robust 40 percent of respondents with 10,000 or more employees report they are likely to deploy blade

servers this year. And most of these servers will be running Linux.

Fourth, the differences between Windows and Linux are rapidly disappearing. The desktops have similar looks and feels, the browsers and Web servers pretty much act and do the same things, and the development tools can create the same Java applications and run the same database structures.

Fifth, Linux is the embodiment of choice; the trick going forward is to keep the choices down to a small number and not repeat the mistakes of Unix past when every vendor offered its own flavor and distribution. Fortunately, the market has brought two Linux distributions to general acceptance: Red Hat and SuSE, the latter now owned by Novell. Hardware vendors such as Dell, HP and IBM are excited that these two versions are strong competitors and that the number isn't greater than two. That gives their customers—and yours—a nice, bounded problem and keeps enough competition to make Linux interesting, but not overwhelming.

"IBM has to remain agnostic when it comes to Linux, and they are happy to see us compete with Red Hat," says John Dragoon, vice president of marketing for Novell.

Sixth, Linux is a lot like Unix, and once enterprise IT support staff knows Unix, making the leap to Linux isn't all that difficult. Oracle's Dargo compares Linux today to where Unix was in the early '90s.

"Back then, Unix wasn't proven in the marketplace, the skill sets weren't there in the enterprise, and we didn't have any critical mass with regard to running Unix on RISC machines from Sun and HP," he says. "Now it is just an accepted fact that anyone can run Unix, and the skill sets are easily transferred from Unix to Linux."

The same ease between Unix and Linux holds for the vendor community, too. Oracle, which last year began selling what it calls "unbreakable Linux" as part of its partner offerings, has widened its support to both Red Hat and SuSE Linux distributions, and has expanded its line to include the various IBM hardware incarnations of Linux, including Power CPUs.

"This isn't hard work," Dargo says. "It takes one person very little to port our apps to new platforms."