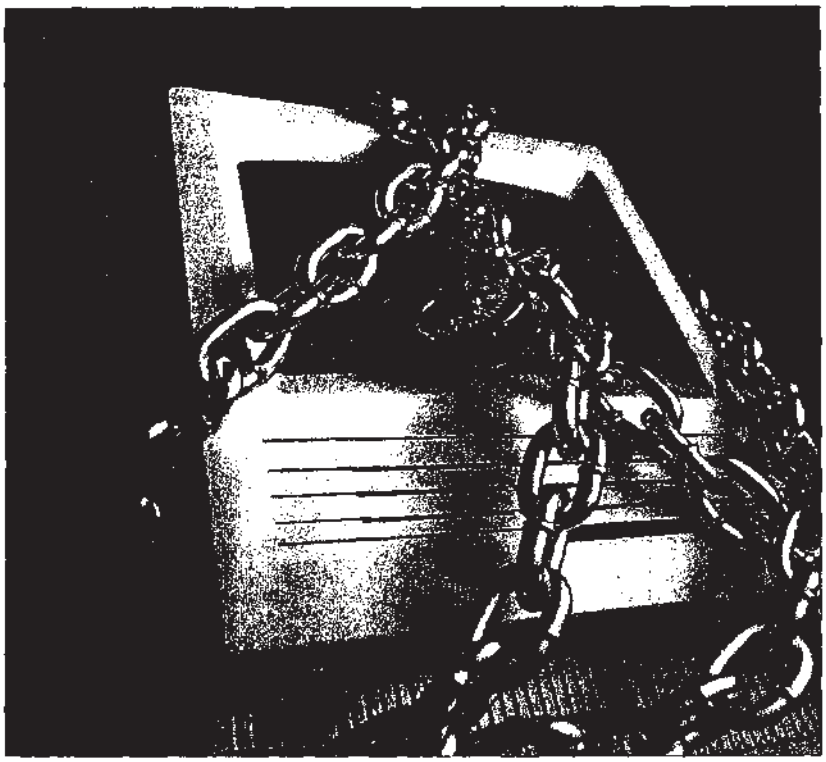
Inside Business
May 2000

Top Hats

With online security becoming increasingly important, a new breed of consultant has come of age. Call them white hat hackers, ethical hackers or security consultants, but don't call them too late.



BY **BOB BATCHELOR**

Like millions of Americans, 39-year-old Mark Loveless works from home. Surrounded by 15 computers, Loveless is taping discussions between two high-speed Ethernet-connected computers.

With the trained ear of a Wild West safecracker, he's searching for a digital hole in the latest release of a commercial software package. He's also writing code. Over the whirring din of competing hard-drives, Loveless is attempting to duplicate what the computers are saying to each other.

If he's successful, he gains entry into a corporate network's infrastructure, leaving bare invaluable intellectual property, trade secrets and confidential information. Welcome to the hacker's delight.

Observing Loveless at work would "bore you to death," he says. Yet, Loveless, who is better known by his Internet handle, "Simple Nomad," possesses a talent that scares the bejesus out of corporate America and law-enforcement agencies. Loveless thwarts computer security systems, climbs over fire walls and exploits little cracks that inevitably pop up in the millions of lines of computer code that make up software programs. Simple Nomad can crack a corporate network, access company secrets and then create a hidden back door that enables him to return without notice. "Once I'm inside a network, that's it," he says. "If I find one way to poke through ... game over."

Lucky for us, Loveless is one of the good guys.

In fact, many of today's best computer

security consultants at one time cut their teeth illegally breaking into networks. Like the characters out of a classic black-and-white Western, the good guys in the hacker culture — like Loveless — wear the white hats, while those bent on mischief and bad deeds don the black hats. For corporations that depend on internal computer networks as a part of daily business, these white hats use their digital talents for good, keeping out the black-hatted "script kiddies" and "cyber terrorists" that threaten security.

The recent denial-of-service (DOS) attacks on eBay, Amazon.com and Yahoo! are only recent examples of new-age security problems. In response, companies hope to retaliate with a new type of consultant, one who now wears the white — or shade of gray — and has an interesting title such as penetration analyst, digital detective or computer-forensics expert.

Unfortunately, these professional hackers can't talk in great detail about their clients or work because of strict nondisclosure contracts. Company execs don't want to broach the subject, because the hint of network vulnerability could lead to plummeting stock prices for large corporations or breed feelings of fear and violation at small and midsize companies.

"You have to think like a hacker to really secure a site from a hacker," says Ken Stasiak, senior security consultant at marchFIRST.

Northeast Ohio business leaders who don't see computer security as a major concern are making a huge mistake, according to Ken Stasiak, senior security consultant at marchFIRST (formerly Whittman-Hart). Not only is computer crime a national problem, accounting for losses of hundreds of millions of dollars annually, but Northeast Ohio companies are woefully behind their counterparts in other regions. "Our blue-collar past has made Cleveland a little slow in getting the necessary security awareness," says Stasiak, who has worked in the IS field for seven years, 3 ½ as an ethical hacker.

However, signs indicate that many firms have taken this potentially unseen threat very seriously. Northeast Ohio, through its InfraGard program, has been a leader in business-law-enforcement partnerships (see "FBI Cyber Unit Born in Cleveland," page 79).

Similarly, more security consultants are moving into the area, and the Big Five consulting firms are beefing up their security staffs. "That alone speaks to the size of the market here [for high-tech systems security]," says Stasiak, who estimates that the size of the greater Lake Erie market exceeds $200 million. "It hasn't been tapped in Northeast Ohio."

Stasiak caught the security bug by working on the AS 400 platform main-

frame system. While looking at the operating system, he began seeing its holes. He informed his bosses and tried to lock down the security gaps. The experience opened up more security-related work, until he evolved into a full-fledged white hat.

However, like much in the hacking world, even "white hat" is a misnomer. Most outsiders would consider even the whitest of hats somewhat gray. Ethical hackers commonly interact with black hats to gain insight into their interloping mind-set. "You have to think like a hacker to really secure a site from a hacker," says Stasiak. However, E. Kelly Hansen, president and CEO of Milwaukee-based Sun Tzu Security, puts it differently, "I wouldn't hire [black hats], but they are friends of mine."

Some within corporate America question the use of self-professed white-hat hackers, who in a former life may have skirted legal boundaries in their exploits, regardless of their expertise. Stasiak explains that the demand for experts in the field further blurs this line. "A survey released by the FBI asked corporations if they would hire a documented hacker," he says. "Seven percent of them said they would, which is an amazing figure."

Stasiak takes a hard line on this issue with one exception. "I would not hire a hacker with a felony background," he says. "You have an obligation to your clients; hiring a hacker would be introducing a risk to the organization that is not acceptable."

Loveless isn't on an FBI most-wanted list. Luckily, for corporations around the world, Simple Nomad is an ethical hacker. For his part, Loveless views himself as a "technological explorer," and for most of his life he has tried to make computers "bypass limits and make them do something beyond what they were designed for."

Today, Loveless is a member of BindView Corp.'s RAZOR team, a computer security group that identifies network vulnerabilities and helps BindView develop risk-management solutions. BindView, headquartered in Houston, is a public company whose client list includes 75

Cybercrime Stats

The "1999 Computer Crime and Security Survey" is based on responses from 521 security practitioners in U.S. corporations, government agencies, financial institutions and universities. "The findings confirm trends established over the last three annual surveys," the report states. "It is clear that computer crime and other information-security breaches pose a growing threat to U.S. economic competitiveness and the rule of law in cyberspace. It is also clear that the financial cost is tangible and alarming."

Some specific findings:

- System penetration by outsiders increased for the third consecutive year; 30 percent reported intrusions.
- 55 percent reported incidents of unauthorized access by insiders.
- 26 percent reported theft of proprietary information.
- 32 percent reported serious incidents to law-enforcement agencies.
- Financial losses to security breaches totaled more than $100 million; of 51 percent who acknowledged losses, only 31 percent were able to quantify them.
- Financial loss is primarily through theft of proprietary information and financial fraud.
- 38 percent reported two to five incidents of unauthorized access or misuse; 26 percent reported 10 or more.
- 90 percent reported virus contamination.
- 69 percent reported laptop theft.
- 97 percent reported insider abuse of Internet privileges (downloading porn or pirated software).
- Companies spent $4.2 billion on computer security software in 1999; International Data Corp. predicts the number will rise to $7.4 billion by 2002.

members of the Fortune 100 and 22 of the largest U.S. banks. Confidentiality agreements prevent BindView from publicly naming these companies.

Contrary to the media's portrayal of hackers, they are not all shifty-eyed, pasty, 18- to 25-year-old white males with a desire to bring down "the man." Yet hackers do have an intense desire to surpass limitations and treat computers and networks as a puzzle. Loveless describes much of what he does as "connecting the dots and finding holes."

Gray hats exude a certain air of virtue. "There are people [black hats] who get this information, and eventually they'll take advantage of it," explains Loveless. "If I know something about a particular software, then sitting on it doesn't make a lot of sense."

In fact, gray-hat hackers have established a rough set of guidelines on disclosing problems to software vendors. If a minor problem is found, a hacker will contact the vendor and give it a week to fix it. A more problematic discovery warrants a month's leeway. If the error isn't fixed, then gray hats go public with the information.

Simple Nomad's Web site, www.nmrc.org

"You can't let companies like Microsoft and Novell police their own software," says Loveless. "You have to tell them you're going public with the information, or they'll just ignore it. What we provide is an external audit of software, since there is no formal equivalent of Underwriters Laboratories for computer software."

For example, three years ago, white- and gray-hat hackers began reporting problems with Microsoft's NT product, Loveless says. Microsoft ignored them, even though thousands of people were using the software. It wasn't until people made the flaws public that the company took it seriously.

Stasiak acknowledges the role the grays play in pointing out problems. "Those guys make security better by finding [programming] holes," he says. "The vendors are not reacting fast enough to security issues. An awareness of security in some ways is as important as security itself."

Loveless says vendors have sent him advanced copies of software programs for his scrutiny. "Novell realizes that hackers are improving their product," he explains. "They're getting free R&D from me."

However, Loveless also acknowledges that, as in every aspect of society, those few bad apples in the hacker society will spoil the whole bunch. "If you take any large cut of the population, you're going to have mostly good people," he says. "But you'll have some bad people in it, too."

Long before he became Simple Nomad, Loveless became interested in computers as a teen-ager in the late 1970s, when his dad brought home an Apple II. In the early days, he says, it wasn't illegal to take over a phone line, and no laws existed to prohibit hacking. As his skills developed, Loveless admits there was some glamour involved. "It was fun to break in and fun to figure out something no one else has."

In the 1980s, he would find flaws in networks and "go in, exploring and playing around." Rather pragmatically, Loveless explains, "What changed it for me was when hacking became illegal. I just thought that I'm not going to go to prison over this." Even though he's now an ethical hacker from 9 to 5 at BindView, he still gets a great deal of satisfaction from his gray-hat work.

Many white hats establish their own Internet sites to provide analysis and anonymity for members. Loveless set up the Nomad Mobile Research Centre (www.nmrc.org) to continue doing his gray-hat work. Stasiak has his own site (www.6ft-under.com), but it caters to corporate America and provides a place for business-information-systems employees to test and learn about the hacker community. Hundreds of other Web sites provide information on the hacker community, as well as magazines such as

2600: The Hacker Quarterly and even a daily news site, Hacker News Network (www.hackernews.com).

The many hacker-related Web sites and discussion lists spawned a new generation of "script kiddies," who Loveless scorns. The new breed of cybercriminals uses the information derived from the work of old-school hackers to hurt companies.

> **"A true hacker is more interested in writing a virus that will impress his friends than unleashing it on people, which doesn't take much skill at all,"**
>
> **says E. Kelly Hansen, president and CEO of Milwaukee-based Sun Tzu Security.**

"Script kiddies are using hoodlum techniques, and it's very easy for them to do," says Sun Tzu's Hansen. "It doesn't take much of a brain." The technical tools, she explains, are out there for those who want to commit crimes. In fact, anyone with some computer knowledge can find sites on the Internet to download viruses or programs that will probe for network weaknesses.

The only other stereotype that holds true in the hacker world is that a college education isn't a prerequisite. Most hackers got hooked on computers at an early age and then found college unnecessary, especially considering that not long ago, higher-education curriculums didn't offer much in the way of pro-

Stay Secure

The FBI provides some tips to help you minimize your potential vulnerability.

- Maintain backups of all original operating-system software.
- Maintain backups of all important data.
- Maintain a solid, well-thought-out corporate security plan accepted and practiced by all employees involving all necessary levels of your organization.
- Install sufficient software to recognize attacks and track/audit defensive steps.
- Ensure audit trails are turned on.
- Consider placing a warning banner on your system to notify unauthorized users they may be subject to monitoring, and data residing on the system is subject to review.
- Routinely test network for vulnerabilities.
- Change logins/passwords frequently, especially when employees change jobs.
- Require use of passwords containing alphanumeric character combinations and/or one-time tokens.
- Cancel logins/passwords when employees leave the organization.
- Minimize the number of modems on the system.

If you become a victim, the following steps may help reduce the negative effects of such an incident.

- Respond quickly. This will greatly reduce potential damage and monetary losses.
- Consider activating Caller ID on inbound lines.
- Have pre-established points of contact for the general counsel, emergency response personnel, law enforcement, etc.
- Appoint one person to handle potential evidence. Establish a chain of custody.
- Do not "duel" with the hacker. This typically invites more attacks.
- Do not use your network's email functions to discuss the incident. The mail server may have been compromised.

gramming or high-level computer skills. Many of today's younger computer explorers also find a degree unnecessary. They can find jobs based on the skills they've developed.

Loveless took a few courses at a local community college and never earned a degree, but he cautions his children not to follow his example. He readily admits that he would have attained the level he's achieved at BindView earlier if he had earned a degree. And he laughs that he's repeatedly told his kids, "If I had a college degree, you would have had a lot more toys when you were growing up."

Though Loveless jokes about it, skill sets reign supreme in the hacker world, even if someone uses his or her knowledge for illegal activities. "If someone is a criminal," he says, "I will still have a level of respect for the technological end of what they're doing." Perhaps this goes to the heart of the hacker community — it's a subculture that places ultimate emphasis on what one can achieve through the creative use of his own or shared information. Hackers eliminate the political atmosphere that runs rampant through the business world and revere knowledge.

MARCHFIRST SENIOR SECURITY CONSULTANT KEN STASIAK'S WEB SITE, WWW.6FT-UNDER.COM

"Hackers have a unique sense of humor and are either wickedly smart or wickedly funny — some both," says Hansen. She explains that the real hacker leaders, such as Simple Nomad, L0pht's Dr. Mudge and Secure Computing's Jeff Moss, are not dangerous and have most likely gained their fame through writing about network security. "A true hacker is more interested in writing a virus that will impress his friends than unleashing it on people, which doesn't take much skill at all," Hansen says.

With the proliferation of media outlets and online news agencies, many hackers are finding themselves deluged with media opportunities. In the quest for sensational stories, and in the wake of DOS attacks, anything related to computer security is hot news.

Simple Nomad often speaks at national conventions, like Moss' Def Con and Black Hat. He even has groupies. "I've found myself invited to a lot of parties at conventions just because somebody wants to go around telling his friends that Simple Nomad was at his party," he says. "That's when I'm like, later, dude."

Although these pockets of adoration exist within the hacker community, for the most part it is similar to groups of academics who specialize in a particular subject.

Instead of labor history or constitutional law, hackers study software and network systems. It's sort of like the older professors guiding the newly anointed. We have each other, Loveless explains. "We all read each other's papers that get published — that's how I've made most of my really good friends." ■