Reprinted from Ziff Davis ***Smart Business*** Magazine (formerly PC Computing)
July 2000

How to Hire a Hacker
By Christopher Null

Jack Stevens knew his company was being hacked. Someone was snooping around in sensitive information on the company network. So Stevens (not his real name) called John Klein's Rent-A-Hacker (**http://www.rent-a-hacker.com**), a security consulting firm. Klein leapt into action. Klein logged onto the client company's network and quickly sized up the situation. The intruder had exploited a common Solaris server bug. Klein immediately found what had gone on. "The trick was not just blocking them out, but finding out who they were," Klein says. "But it's delicate. It's like a chess game: First mistake loses."

Klein employs some 300 freelance computer security experts-better known as hackers- throughout the world. He handpicks a specialist to fit each call he gets. In this case, he tapped Kelvin Wong, a top operative who also happens to be his company's chief operating officer. Wong back-traced the intruder's connection to a Canadian @Home network, which tracked him to his cable modem. To confuse his pursuers, the offender launched several denial-of-service attacks. But eventually the intruder lost the chess game and was handed over to the Royal Canadian Mounted Police. By acting quickly and returning the attack against its intruder, the victimized company foiled the hacker and prevented any real damage. In the dot-corn era more than ever, the best defense is a good offense.

Hired Guns

In the wake of recent security fiascoes like the theft of 350,000 credit card numbers from CD Universe and the rampant distributed denial-of-service attacks on top Web sites this spring, hacker-for-hire services are thriving. Andersen Consulting, IBM, Pinkertons, and even software developers like Internet Security Systems are offering what they call security auditing and other ethical hacking services.

So who needs a security consultant? Everybody.

"Ninety percent of all systems are insecure and hackable," according to Wong. "It's not a question of whether they can be hacked or not, it's a matter of when and how"

Wong's estimate looks spot-on. In March, the Computer Security Institute (wwwgocsi.com) took its fifth annual survey of large corporations and government agencies. Ninety percent said that computer security breaches had occurred within the last 12 months, and 70 percent classified those incidents as serious-constituting theft of proprietary information, financial fraud, and sabotage. The total bill? More than $265 million in losses.

The numbers are sobering, and they make Rent-A-Hacker's $175-and-up hourly rate look like chicken scratch.

Big Boys Hack Too

More traditional security companies like Internet Security Systems (www.iss.net) tend to offer a wider range of security services. Mark Sims, ISS's vice president of managed security services, leads the company's outsourced firewall, virtual private network, and antivirus management services in addition to its ethical hacking services (also known as penetration testing). ISS's ePatrol Internet scanning service scans company systems starting at $10,000 per year; subscription cost varies with network size.

ISS uses internal staff for security jobs, eschewing the consultants Rent-A-Hacker uses. The reason, Sims says, is because it's crucial to build trust between ISS and its clients. ISS does background checks, Sims says, but "finding out if someone was a [malicious] hacker or not is virtually impossible. We're performing the same actions a hacker would; we're just not exploiting them. We hire people and educate them on hacker techniques.

John Spain, president and CEO of Pinkertons' Information Risk Group (www.pinkertons.com), says his company provides a full range of information security and risk management services, including penetration testing. Pinkertons employs its own specialists and uses partners to cover specific areas of expertise, thought the company policy is to "never employ someone with a history of [malicious] hacking." Spain declined to discuss pricing, saying fees are always negotiated with customers individually.

For top-of-the-line security consulting, IBM's Ethical Hacking Service offers all kinds of security assistance, from design and implementation to maintenance. Al Decker, managing principal of security and privacy services for IBM's Global Services division (www.ibm.com/security/services), says that penetration testing is just a small part of his company's offerings. On average, clients pay from $25,000 to $50,000 for a typical contract.

Rent-A-Hacker's Klein says his boutique service is better, pointing to the big guys' higher fees and saying they lack the kind of experience his contractors have.

"We differ from most in the fact that we cater to small businesses and individuals," he says. "We see things more from a real-world perspective. We know there are 14-year-old kids out there who can hack and do things well beyond what someone with a computer science degree sitting in an office would ever even dream of. We know the tools those kids use, and their methods are beyond conventional thinking."

To get beyond that conventional thinking, Klein says he calls on his 300-plus contractors in the hacker community each with a specialty-a particular operating system or a well-known firewall.

"I match up the skills of my hackers with the particulars of the job," he says. "It's impossible for any one person, firm, or software program to cover all the bases, so almost invariably [the hackers] are successful."

Klein says that the prepackaged security scanners (like Webtrends Security Analyzer or Network Associates CyberCop) simply don't do the job because they focus only on common security holes and can't invent creative attacks like real hackers can.

"Most of the time, what trips up system administrators is that they think like system administrators and not like hackers," Klein says. "We spend a lot of time teaching our clients to think like hackers."

Put on Your Hacker Shoes

Thinking like a hacker means knowing what a hacker wants. Some want data, says Klein, but "the real hacker challenge comes from inventing a new way in. That's what we find: new and creative ways to exploit a system."

What common holes do hackers find in systems? There's no standard answer, according to Klein, though "some of the most egregious holes we have found were the simplest things." Wong adds that hackers come up with *zero-day* (that is, brand-new) tactics all the time. Occasionally he finds systems that have been backdoored-hackers create secret entryways by modifying the software installed on a server.

Klein and Wong say that the biggest Internet security holes today are not found on Windows. Sun Solaris and Linux power a huge portion of servers connected to the Web, and security on these systems is typically spotty. However, ISS's Sims says that the most common hole his company finds involves Microsoft Windows NT running Internet Information Server.

"The Web server that comes out of the box has many security problems," says Sims, adding that no one bothers to apply the patches.

IBM's Decker points to a more pedestrian security issue as the most widespread. "Unfortunately, the most common security holes are default passwords and out-of-the-box settings," he says, followed by failure to do basic maintenance or upgrade to new, more secure software packages.

So what about the question of hiring a supposedly reformed hacker to muck around on your network as an invited guest? Would you trust a criminal, even a rehabilitated one, with your most precious company secrets?

Former hackers and their employers universally insist that potential clients have nothing to worry about.

"I have taken great pains to allow my clients to trust my company as well as my contractors," says Klein. "I sign an all-encompassing nondisclosure agreement with each client, as well as provide them with copies of the nondisclosure agreement I have pre-executed with each contractor." Every company we talked to also stressed the importance of thorough background checks.

But while Klein says his insistence is genuine, his NDA recognizes that even he can't guarantee the identity of his contractors: "Rent-A-Hacker hereby warrants that it has made its best-faith effort to verify the legal identity of its subcontractors, however, Rent-A-Hacker makes no warranties concerning the validity, accuracy, quality, or completeness of any of the representations made by any subcontractors."

But Wong pooh-poohs any notion that hired guns have a hidden agenda. The ex-hacker is pragmatic about the idea of going beyond the scope of his assignment, saying simply, "I could be sued."

Beyond Mere Hackers-for-Hire

Security analysis services like Rent-A-Hacker are just the beginning. Companies are learning that they need more comprehensive protection.

Chief among the outsourced security companies is Counterpane Internet Security (wwwcounterpane.com), founded by noted cryptographer Bruce Schneier (see "Hot Seat," April 2000, page 42). Counterpane installs hardware on its customers' premises that patrols the network for security violations. At one base of operations, Counterpane keeps tabs on clients' networks 24 hours a day, and the company can act the moment something suspicious arises.

Schneier remains skeptical about his competition: "What hire-a-hacker services do is run a tiger team against your system, which is good for finding out what the vulnerabilities are. What we do is alarm monitoring…24 - 7, real-time."

To better illustrate the difference, Schneier offers a physical analogy: "You might want to hire someone to break into your warehouse to see if you're vulnerable, but that doesn't mean you're going to fire your burglar alarm company. Both are valuable, but certainly a burglar alarm is more valuable. Experts are expensive, and they don't tell you if you're safe or not. They tell you whether that particular expert was able to break in on that particular day using that particular set of tools."

Hack this

Want to find out what you're up against? Here's where the bad boys of the Net hang. Check out these hacker-related Web sites. But don't let your guard down.

AntiOnline www.antionline.com
Nothing but news on the ins and outs of hacker activity. An added twist: reports of hack attempts against AntiOnline itself.

Computer Security Institute www.gosci.com
Current security research and tips on how to keep your company's systems bulletproof .

Hackers.com www.hackers.com
This snazzy site is heavy on archives of underground text files and indispensable hacker shareware.

Lopht Heavy Industries www.lOpht.com
Web Headquarters for the self-absorbed and outspoken hacker group that released products like LophtCrack and other cracking tools.

SecurityFocus.com www.securityforces.com
An invaluable security portal with news, downloads, and advance word about the latest attacks.