

From phoenixnewtimes.com  
Originally published by *Phoenix New Times* June 12, 1997  
©2000 New Times, Inc. All rights reserved.

{ <http://www.phoenixnewtimes.com/issues/1997-06-12/feature.html/page1.html> }

Hacker, Cracker, Watchman, Spy

Some old-school Valley hackers grew up to be high-tech cat burglars. Some went to work for the man. Some just never grew up.

By David Holthouse

Like a lot of thieves, Gambit only works at night. It's half past 10 in Phoenix when he boots up his laptop. Darth Vader's voice intones "What is thy bidding, my master?" Gambit double-clicks on a desktop icon shaped like a chess queen and offers no reply. He's about to break into a law firm's office three time zones away. Someone asks how he feels. "Skittish," he says. "Like a cat burglar casing a mansion. Except when a burglar steals a rich man's jewels, it's obvious. When the lawyers come to work tomorrow, they'll never know I was there."

Gambit is a hacker for hire, an electronic spy and saboteur. His fee for hacking into the law firm's office network is \$1,000. His mission: to obtain the firm's case strategy for an upcoming lawsuit over a real estate development deal gone sour. The other side has hired a private-investigations firm that specializes in corporate espionage, who in turn subcontracted Gambit.

The law firm doesn't have a Web page to attack, so Gambit has to find a way in through a direct dial-up modem line--one that allows remote access to the system, so lawyers and legal secretaries can dial into their computers from home. "This is an old-school hack," says Gambit. "WarGames-style."

Normally, a hacker mounting a direct-dial assault would start by using a War Dialer--a program that rapidly dials thousands of phone numbers and keeps track of which ones answer with a modem tone. Since most office networks use the same prefix for modem lines and voice lines, hackers usually program their War Dialers to change-up the last four numbers only. To thwart security alarms that detect sequential dialing, War Dialers randomize their dialing. The whole point is to seek and identify a target network's modem lines.

Gambit's employers, however, have provided him with a little recon: four direct-dial lines that lead into the law firm's network, plus the corresponding user log-in names. But not the passwords. To get those, Gambit splices a chunk of code from a popular War Dialer called Tone Loc into a password cracker program. Once he launches the "script," it speed-dials the four numbers in revolving order, logs on with the corresponding user name, then tries to break the password with educated guessing: First the program attempts various abbreviations and anagrams of the user name. When that fails, it starts to methodically work its way through a database of common passwords.

Gambit sips from a mug of lukewarm Mountain Dew as the program begins its run. "Okay," he says, "let's rattle some doorknobs." The law firm's system lets the program try three passwords per dial-up before it breaks the connection. Then the War Dialer calls the next number and repeats the process with three new passwords. The hacker is gambling--if the program can't unlock a password before morning, phone logs will record the suspicious modem activity in the middle of the night. "Of course, that's only a problem if anyone actually bothers to check the logs," Gambit says. "But I'd rather not have to worry."

Bingo. Gambit gets a hit on the 37th round--user two's password is "sunshine." "At least it wasn't 'password' or 'computer,'" he says. "I've seen a lot of those. That's when you really feel sorry for the stupid people."

Once he's connected to the network, Gambit hacks around until he gains "root" access--the carte blanche "superuser" status of a system's chief administrator. Once he's got root, Gambit erases the incriminating phone logs. Then he weaves a tiny "back door" program into the network's source code--the foundation program that actually runs the system. It's like propping open a basement window from the inside--now Gambit or another hacker he sells or trades the back-door location to can sneak into the firm's system at will.

For his last trick, Gambit installs a "network sniffer" program. Originally designed to help increase system efficiency, sniffer programs basically sit quietly in a corner and record network traffic for later analysis. Gambit has modified his sniffer to flag any e-mail or file exchange containing certain key words--the names of the plaintiffs, defendants and representing attorneys in the case and the property in question--and secretly copy the data into a file hidden in a complex hierarchy of subdirectories within the network. Essentially, Gambit has set an information trap line he can return to check later. Once it's in place, he punches out. The entire hack took just more than five hours.

An editorial in the Winter 1997 issue of 2600, a hacker quarterly published since 1984, slams mercenary hackers like Gambit. "One thing we must be careful of is the temptation of true crime," it reads. "Once that world is entered, the spirit of adventure and discovery is replaced by the incentive for profit. Not to mention you turn into an utter sleazebag."

Gambit says the spirit of discovery holds no meaning for him anymore, and he has no regrets. Now he wears Tommy Hilfiger cologne.

"When I was a child, I hacked as a child," he says. "Then it was time to make some money."

Tom Jackiewicz, a.k.a. InvalidMedia, could say the same. Jackiewicz, "twentysomething," was the last hacker inducted into the notorious National Security Anarchists (NSA), a Phoenix-based society of elite hackers that was hit with a string of busts from 1992 to 1994. Like Gambit, Jackiewicz says he started hacking as a teenager for the illicit thrill of unauthorized access, fearlessly roaming the electronic wilderness like a rogue samurai. That and he was a geek. "You may be this 5'3", overweight kid who gets beat up in gym class," Jackiewicz says. "But at night, on the computer, you get to be the bully." After three of Jackiewicz's NSA co-conspirators got busted in a row, however, he decided it was time to get a life.

"I could feel I was next, and I just realized one day that, here I was, paranoid all the time, making \$4.45 an hour at some stupid job, living at home, and riding by bike to work. I decided to make money from my skills."

Rather than answer a want ad, Jackiewicz hacked into a local Internet Service Provider--a company that sells Internet access to the public--and stole the system's root password. "Then I called them and said, 'Hi. I'm not going to tell you my name until I see how you react, but here's your root password. I'd like to secure your machines for you.'" The ISP, NetZone, hired Jackiewicz as its security chief. He's since moved up. Last year, Jackiewicz accepted a job as head of systems administration for GoodNet, a major Valley ISP that recently absorbed NetZone. On the side, Jackiewicz does freelance "Tiger Team" work:

For "usually about \$3,000," he'll assemble a team of hackers to attack a client's network using every trick in the book and follow up with a diagnostic report (Robert Redford played the leader of a Tiger Team in the 1992 movie Sneakers).

Gambit and Jackiewicz are both old-school. They learned to hack before the Internet was hip, cheap and easy. Before yuppies put e-mail addresses on their business cards and commercial Web pages exploded like popcorn. Now they represent opposing archetypes for hackers hitting their 20s who've turned their back on the hacker code and gone mercenary in the computer revolution. They are thief and sentry, but Gambit says they're more alike than different.

"I admire the white-hat guys for creating their own job market," he says. "But come on. They're still hackers. They're just taking protection money."

Hacker: someone who enjoys exploring the details of programming systems and how to stretch their capabilities; one who programs enthusiastically, even obsessively.

--the New Hacker's Dictionary, 1994

Jackiewicz slides a security card through a magnetic reader. The electronic lock goes pop, and he pushes open a door. "Well, this is where I work." The monolithic Financial Center building in downtown Phoenix was designed to look like an old mainframe-computer punch card. GoodNet's offices take up the 17th floor.

As soon as he sits down at his desk, Jackiewicz is under siege with demands for his attention from four different media--e-mail, pager, telephone and humans, often with harried looks on their faces that relax once Jackiewicz tells them everything's cool. Underneath his desk is a pillow made from packing foam wrapped in a crinkled, metallic-gray plastic bag. Tacked to one wall of his cubicle is a picture of a badass Mickey Mouse growling a word balloon that says "Buff my dome, G-man." Next to Mick is a postcard of a pinup blonde in a yellow bikini. Two co-workers toss a miniature Earth ball overhead as GoodNet's security chief talks about selling out to the man.

"I even wear a suit now sometimes," he says. "I used to think that if I was good enough at what I did, I could have long hair and wear whatever I wanted." Jackiewicz says he used to have a multicolored ponytail and show up for meetings at NetZone in thrift-store wear. "Then I reached a level where I was like, 'You know what? I want to advance, I want to impress my managers, but if I keep showing up to meetings in a powder-blue Naugahyde leisure suit, they may not be able to get past the clothes.' They should, but they may not be able to. So I tried to look more normal."

Now Jackiewicz's office wear looks like it came off the casual-Fridays rack at L.L. Bean, except for a pair of truly crisp, vintage two-tone leather shoes. Two months ago, Jackiewicz was the guest speaker at an interagency law enforcement conference on computer crime organized by Maricopa County prosecutor Gail Thackeray, a computer-crime specialist who helped bust several of Jackiewicz's NSA friends in the past.

"The first thing she said when I walked in was, 'Well, Tom, I see you're not wearing black fingernail polish anymore.'"

Seven years ago, Thackeray spearheaded an interagency hacker bust called Operation Sun Devil. On

May 8, 1990, 150 federal agents and hundreds of state and local police took part in raids in 14 cities across the U.S. Forty computers and 23,000 discs were seized. Most of the charges resulting from the sweep were quietly dropped, however, and in the end, Sun Devil only netted three hackers who took plea-bargain deals. Still, Thackeray is one of the most prominent anti-hacker law enforcement agents in the country. In 1995, she was the featured guest speaker at DefCon, an annual hacker convention in Las Vegas.

Thackeray refers to the National Security Anarchist hackers as "our alumni." Besides Jackiewicz, she says, there are two other NSA hackers who claim to have gone straight and now work in computer jobs with access to sophisticated hardware and high-speed Internet connections. One, who went by Dark Druid, works at Northern Arizona University. The other, Merc, does research and security consulting for Genuity, another Valley ISP.

"I'm very concerned that places hire these guys and then absolutely do not monitor them appropriately," Thackeray says. "Hackers have a higher recidivism rate than alcoholics. I don't think any of these guys ever retire totally." Thackeray says she once asked a manager at Genuity what early-warning devices were in place to monitor its ex-hacker employee. The answer was none. "It was basically the same response I got from GoodNet about Tom [Jackiewicz]: They said, 'Well, we've given them a lot of responsibility, and some of the best tools in the world, and we're counting on them to see it's to their advantage to go straight.' They're calling it a position of trust. I take a more cynical view. I think they're being incredibly naive."

Although Jackiewicz says he stopped hacking as soon as he took his first security job, he still operates Unphamiliar Territories ([www.upt.org](http://www.upt.org)), one of the most revered hacker bulletin boards on the Internet. Jackiewicz prefers to call UPT a "computer security Web site" now. It's all semantics, really, since there's so much overlap between the technology of hacking and defending against hacking. For example, a network scanner program originally designed by a security expert to analyze a network and expose weaknesses--sort of an automated Tiger Team--is useful to hackers for obvious reasons. Likewise, ISP administrators can use a password guesser program written for hackers to find out which of their clients have stupid passwords and give them a wake-up call.

UPT boasts an extensive library of hacking/security programs, from classic to cutting-edge, which are free to download. It also carries a summary of the latest security bulletins--holes in certain systems discovered by hackers, patches to those holes quickly written by white-hats. Jackiewicz says that, as a chief of security, overseeing the site is an invaluable asset. "It's a constant seesaw between security holes and patches," he says. "You have to keep up on the latest, because the hackers do."

Another feature of UPT is a public access account titled "Hack UPT." It's an open challenge set up by Jackiewicz and his former partner in crime, Merc. The account lets you onto the network server--UPT nerve center--housed in Jackiewicz's bedroom. The challenge is to get root access once you're in. So far, no one's succeeded. If he had, he would have talked smack about it far and wide, because going up against Merc is going up against a top gun.

Merc's handle is short for Mercury, messenger of the Roman gods. A fashion maven might charitably describe Merc's look as "rumped." During one recent dinner, he spilled food on his shirt, looked at it, and just left it there. But Jackiewicz and other former NSA hackers say what Merc lacks in social graces, he makes up for doubly in computer skills. As they say on late-night Kung-Fu Theater, his technique is strong. "Merc's a god hacker," says MindRape, an NSA hacker who got busted in 1992. "He's so

freaking good." Thackeray is more reserved with her assessment. "There's basically two kinds of hackers. The ones who are looking to get something from it, and the ones who just have to take everything apart, to examine everything and learn what it does and mess with it. There's no profit motive there, no benefit other than bragging rights and knowledge. Merc is in that category." Thackeray also allows that, as a programmer, "he's certainly several leagues above most of the people we deal with."

Admittedly paranoid, Merc wouldn't let his voice be recorded, and agreed to an on-line interview for this article on the condition that New Times not use his legal name, even though it's attached to his "handle" in numerous public-record court documents.

The last NSA hacker to get popped, Merc was raided in 1994. When he heard the early-morning pounding on his door and looked out the window to see federal agents with drawn guns, Merc says, his first thought was, "Well, I guess this is the day." Thackeray says that compiling a list of all the hacks they had Merc nailed for took reports from the Secret Service, Air Force intelligence, the IRS, and state and local police. "Given what we had on him, the best he was looking at was probation with some jail time. The worst was prison." Instead, the government made what Thackeray calls "an unusually favorable offer": If he agreed to explain some of his methods to the Secret Service and Air Force OSI (office of special investigations), the government would let him plead out to one charge--breaking into a Salt River Project computer--with a guarantee of probation; no fine, and no time.

Merc took the deal, but it has yet to be finalized before a judge. He's due to be arraigned June 17, at which time he'll receive a new court-appointed attorney, who will review the deal and, presumably, accept it in short order. Until then, he still has charges pending. If the government decides he hasn't been a good boy, it could yank the deal at the last minute. Merc says he hasn't done any illegal hacking since his bust. But other hackers say he's been wreaking havoc on SPAM (junk e-mail) marketers across the country. Also, when Merc applied for his current job, local hackers say, the systems administrator at Genuity reportedly laid down a challenge: "If you're such a god hacker," he told Merc, "then do this: I've got a private Internet account on an ISP in Cincinnati. That's all I'm going to tell you. I want you to find the ISP, get into my account and leave me a message that proves you were there."

The story goes that when the Genuity administrator checked his Cincinnati account the next morning, not only was there a message from Merc, but it contained several of Genuity's most critical system passwords, which Merc had somehow pried out of the Phoenix ISP.

Merc's job at Genuity is less formal than Jackiewicz's at GoodNet. He doesn't have to dress well or come in on time. The two are still good friends, but Jackiewicz says he'd never hire Merc because the guy can't keep a schedule. On the flip side, when Merc calls his friend a sellout and makes fun of him for having a girlfriend, you can tell he's only half joking. Back in the day, they were Merc and InvalidMedia. Now they're Merc and Tom from GoodNet.

The NSA disbanded after Merc's bust. The group had originally formed in 1989 as the first 2600 group--a local hacker club--in the Valley. 2600 groups got their name from the hacker magazine, which took its name from the frequency of a certain long-distance carrier tone that a legendary '70s "phone phreak" named Captain Crunch discovered he could emulate with a toy whistle from a cereal box. By tradition, 2600 groups held meetings on the first Friday of every month. In Phoenix, the hackers met inside a pizza restaurant at Metrocenter.

Jackiewicz says 2600 meetings in Phoenix started after he met two NSA members, MindRape and Dark Druid (Druid's the one who now works at NAU), on a German hacker chat room called Lutzifer. "We found out we were local to each other and got together in person one night."

All the NSA hackers were usually at the meetings, along with other local hackers who hung around and tried to impress the big boys like aspiring hip-hop MCs circling a table of famous rappers at a club, looking to "get on." Except there was one difference--the elite hackers didn't have any girls sitting with them. Jackiewicz says there aren't a lot of female hackers because ". . . most girls can get a date on a Friday night no matter how geeky they are."

The 2600 meetings were essentially in-person versions of the hacker chat rooms on the Internet. The boasting and banter were the same, and the hackers traded programs and tips. But after the meetings, they would go "trashing," hacker slang for stealing trash hoping to score technical manuals, company phone lists, security procedures, interoffice memos or other corporate detritus that can be used to hack their network or social engineer (con, sweet-talk, bullshit) someone inside a company into giving out useful information over the phone.

Two favorite trashing spots for Valley hackers were the US West building at 32nd Street and Shea, and the AT&T offices at 35th Avenue and Indian School. The AT&T building downtown has a "secure Dumpster," meaning it's lighted, within a fence, and surrounded by security cameras. "Which means you wear a mask, jump over the fence, grab the trash, jump back over the fence, and run like hell," says MindRape, a.k.a. Donald Moore, 24. The NSA's best trashing discovery, Jackiewicz says, came from an impromptu raid on the Dumpsters of a company called NORSTAN, located just across the street from an NSA member's house. "We came up with a big Rolm CBX phone and hundreds of manuals," he says. NSA members eventually wrote several how-to articles for various hacker journals based on the hardware and manuals they obtained that night.

Another memorable run, Jackiewicz says, was the time they hit a Sprint building that was next door to a medical testing facility. "We grabbed two bags and took off running. Turned out we had a bag each of dirty diapers and medical waste." Jackiewicz says the last time he went trashing was right before his job interview at GoodNet. He raided the ISP's Dumpster to read up on what was going on inside the company.

There are still 2600 meetings in Phoenix, the first Friday of every month, but they're in a large chain bookstore at Metrocenter now, not the pizza joint. And the NSA guys don't go anymore. "The scene here now isn't one I would be proud of," says MindRape, whose 1991 bust for infiltrating credit-bureau computers was widely publicized in hacker magazines. "It's too full of lamers [hackers without the skills to back up their boasts] and warez kiddies [software pirates with negligible programming knowledge]. They enter the scene expecting to be given all the answers. They take no pride in figuring it out for themselves. Most of them think hacking is just breaking into systems, bent on destruction."

Jim Lippard, director of Internet security operations for the Valley-based ISP GlobalCenter (formerly Primenet), says the hackers he deals with are ". . . mostly the dumb ones. The good ones you don't really see, because they don't screw up. And usually, they don't do anything very malicious. As long as that's the case, it's easier to just ignore them."

Hackers target ISPs for several reasons--to get free Internet access, or to go up against a particular security expert, or because they want to disguise themselves during illegal hacking. Gambit says he goes

through at least four ISPs around the nation before attacking a target. Since all the users connecting to the Net via a certain ISP at any one time all appear under one umbrella "shell" account, if a hacker hopscoches through several ISPs before making a run, it's difficult for someone who detects a break-in to "backward hack" and track you down. Gambit favors ISPs that are known to purge their system logs every week--a common protocol.

Both Lippard and Jackiewicz say hackers have broken into their systems. "I would say that's true of any major commercial ISP in the country," Lippard says. "The best hackers collect access like mountain climbers collect summits."

Luckily, Jackiewicz says, the best hackers are the least likely to do damage. "My primary goal is keep out the 14-year-old kids who want to get in and nuke all the files." Such vandals get no respect from Jackiewicz. "They have no elegance," he says. "Look at it this way--if you come home and someone has broken into your house and stolen all your furniture and there's a big urine spot on your carpet, it's just boring. But if you come home to find all of your furniture hanging by strings from the ceiling, with a polite note advising you to lock a certain window the next time you leave, well, that's a little more interesting."

Often mythologized as folk heroes by the mass media, these self-styled cyberpunks possess an equal abundance of nerve and naivete, espousing a quasi-utopic science-fiction vision that scoffs at convention. In cyberspace, they argue, the rules of society should not apply.

--the Washington Times, May 8, 1995

Gambit says the first job he got hacking for money was with a small private-investigations firm on the East Coast. "I helped track down people who'd skipped bail and did background checks. If you know the right numbers to dial, you can track someone from their birth certificate to their death certificate, with all their criminal offenses, name changes, car purchases, speeding tickets, marriages, divorces, pet licenses, business licenses, inheritances and bankruptcies in between. It was all public records and newspaper library stuff. It was all legal."

Then one day the PI firm asked if it could refer Gambit to a larger investigations company that specialized in corporate espionage. "They told me the money was good, but it might involve going into--as it was phrased to me--some 'legal gray areas.' I said it was okay for someone to ring me up."

The next day, Gambit says, a man from the new firm called. "I asked him if he was a PI, and he said no, he was a security consultant," says Gambit. "I asked him what that meant and he ignored me." The man wanted to know if Gambit could access the current month's payroll records from a well-known West Coast graphic-design firm. Gambit said maybe, why? The man replied that some people wanted to target underpaid designers and lure them away. "I told him I might have to break a few laws, but he said he didn't want to hear about it, to just get him the records and he would give me the money. And that was it."

The graphic-design firm had a Web page, back when they were still a novelty. Open to the public by design, the Web server--the computer system that runs a Web page--was connected to the firm's office network with no "firewall" security measure in place to police traffic between the two. "It was pathetic," Gambit says. "An eeny-weeny baby hack." He got paid \$400 for stealing the data. "The guy who called me probably got five times that."

Gambit says he has taken almost a hundred jobs since then, each paying between \$300 and \$3,000. He says he made more than \$60,000 last year. And he paid taxes on it. "I'm on their payroll." His job title? Gambit has to laugh. "Security consultant."

In hacker culture, Gambit is a "Cracker," a knight who has sold his sword, who hacks for money instead of knowledge and freedom.

In his 1984 book *Hackers: Heroes of the Computer Revolution*, author Steven Levy summarized the six basic tenets of the hacker code:

- 1) Access to computers should be unlimited and total.
- 2) All information should be free.
- 3) Mistrust authority--promote decentralization.
- 4) Hackers shall be judged by their hacking, not bogus criteria such as degrees, age, race or position.
- 5) You can create art and beauty on a computer.
- 6) Computers can change your life for the better.

That was the old-school manifesto. Now it's a new world. The Internet has gone supernova, and in the 1997 hacker underground, the way of the masters is an obscure art. Back in the day, you had to be a programmer before you could be a hacker. One navigated the Net with arcane UNIX text commands, not a point-and-click Web browser with graphic interface. Also, target systems were fewer and more worthy. Five years ago, the Net was still primarily the domain of the military and academia, whose networks had been hammered on for years and understood the concept of security. You had to be good to get in. Now, commercial companies are flocking to the Net like lemmings, clueless to the risks of the plunge they're taking. Cyberspace is riddled with insecure systems, and bulletin boards where 25 years of hacker techniques and programs are free for the taking.

"There are now many more hackers than there used to be," says Merc. "Everyone on the Internet these days seems to consider themselves a hacker of some sorts." You can practically see the "god hacker" sniffing in the air, but he has a point. Fourteen-year-old kids who would have been throwing eggs at the schoolbus five years ago are now hacking just for the malicious thrill, using tools they don't understand. Most of them have no respect for the how of hacking, and care little for the why. The golden days of the NSA and groups like it are gone forever, their members scattered, either gone straight or walking the underground alone.

"Think of the days when you were a kid and you owned a dirt bike," Merc says of hacking in the heyday. "Think of a Saturday morning and you are up early and on a trail with some of your friends. You have no idea where you're going, and all you know is that you are on an adventure. Nobody is there to tell you where to go, and the road ahead is unknown. If you can recall these feelings, or perhaps you have your own version of them, then you will understand what hacking was for me.

"Maybe today my motivation is to try to find those feelings again.

{ <http://www.phoenixnewtimes.com/issues/1997-06-12/feature.html/page1.html> }