Cloud Computing with thunder.
The AMD Opteron™ Processor: Essential balanced performance for your cloud.
▸ Buy Now
AMD
The future is fusion

NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/research/2004/0301hackers.html

What are they thinking?

Knowing hackers' favorite attack patterns and motivations can lead to better network security.
By Deborah Radcliff , Network World , 03/01/2004

Hackers, crackers, carders and thieves are putting the squeeze on your network security. But what do you really know about them? What draws them to your network, and why do they do the things they do?

Knowing the motivations of digital intruders helps you understand their behaviors, says Dr. Max Kilger, a social psychologist for the Honeynet Project . And understanding those behaviors can help you better protect your networks.

With this in mind, *Network World* dug into three real cases to analyze the attackers' behaviors and motivations. The incidents include an outsider attack on a financial institution, the rooting of an e-commerce hosting provider to heist credit card numbers and an employee copying a client database from a brokerage firm to take to a new job at a competitor.

Cloud Computing with
thunder.
The AMD Opteron™ Processor:
Essential balanced performance for your cloud.
AMD
▸ Buy Now

Identifying what is common and what is unique about these attacks gives you information you can use to further your own protection, detection and forensics practices.

- Profile 1: The External Attack
- Profile 2: Credit Card Crooks
- Profile 3: Filching Files from Within
- Adrian Lamo: Profiling network administrators
- Meeces to pieces: What motivates the computer criminal
- Profiling defined

NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/research/2004/0301hackersprof1.html

The external attack

By Deborah Radcliff , Network World , 03/01/2004

For the most part, hackers break into corporations for one reason: Status. "The hacking community is a strong meritocracy where status is determined by level of competence," Kilger says.

As such, most attackers go after corporate networks indiscriminately. They're looking for the weakest link. And when they do break in, they share their results with others in their community to prove their prowess.

"These poorly protected victim companies are what I call 'targets of opportunity,'" explains Charles Neal, vice president of security for the managed security services division of Cable & Wireless, which has investigated numerous attacks on customers.

Such was the case when security consultant Greg Gilliss investigated a digital break-in at a large financial institution last year. The mutual funds firm didn't call law enforcement because it conducts business with the government and didn't want them to know about it.

The company suspected foul play when its vice president walked into his office and saw the cursor moving files around on his Windows 2000 workstation.

"This was definitely a target of opportunity," Gilliss says. "The client had weak passwords, no patches, and they were running services they didn't need, all of which were unprotected. Worst of all, they were running pcAnywhere visible to the outside world and with no encryption through their one router firewall."

It was the pcAnywhere application that eventually granted the attacker full access to the 700-node network. All the intruder had to do was install a sniffer and wait for the administrator to log on to the vice president's workstation to do remote administration. Breaking the password was trivial, Gilliss says, because the administrator's username and password were the same three letters.

Using network logs, Gilliss drew a scatter plot of the trespassers' behavior inside the network and gathered this profile:

- They were cautious and knew U.S. calendar holidays, during which they logged on to avoid detection.
- They couldn't be kids because script kiddies aren't so patient.
- They were in a time zone 10 hours away.

PATTERNS OF BEHAVIOUR

Profile 1: EXTERNAL ATTACK

- Select the target using IP lookup tools such as NSLookup, Dig and others.
- Map network for accessible services using tools such as NMAP.
- Identify potentially vulnerable services (in this case, pcAnywhere).
- Brute force (guess) pcAnywhere password.
- Install remote administration tool called DameWare.
- Wait for administrator to log on and capture his password.
- Use that password to access remainder of network.

COUNTER MEASURES

- Restrict remote logons to specific IP addresses and/or use VPN technology.
- Monitor logs daily for anomalous behavior, such as a single user logged on locally and remotely at the same time.

Click to see:

- They never stayed longer than an hour.
- They logged in with a different IP address each time.
- They'd been there for more than a month.

After three weeks, they started logging on during work hours, which meant they didn't care about getting caught anymore.

With this information and a little investigation, Gilliss ascertained that the attackers used different compromised DSL lines each time they returned, and all of these lines tracked back to a single ISP in Europe. His recommendation to his client was to fire its IT consultant, run a penetration test against the network, patch its systems, close vulnerabilities and restrict remote access.

Main | Next: Profile 2: Credit Card Crooks

NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/research/2004/0301hackersprof2.html

Credit card crooks

By Deborah Radcliff , Network World , 03/01/2004

What identity thieves are seeking is money, of course. But those who broker in stolen credit cards also are strongly motivated by status, says Dan Clements, CEO of CardCops.com , a credit card protection service agency that scours the Internet for compromised credit card and personal data and reports it to victims and banks.

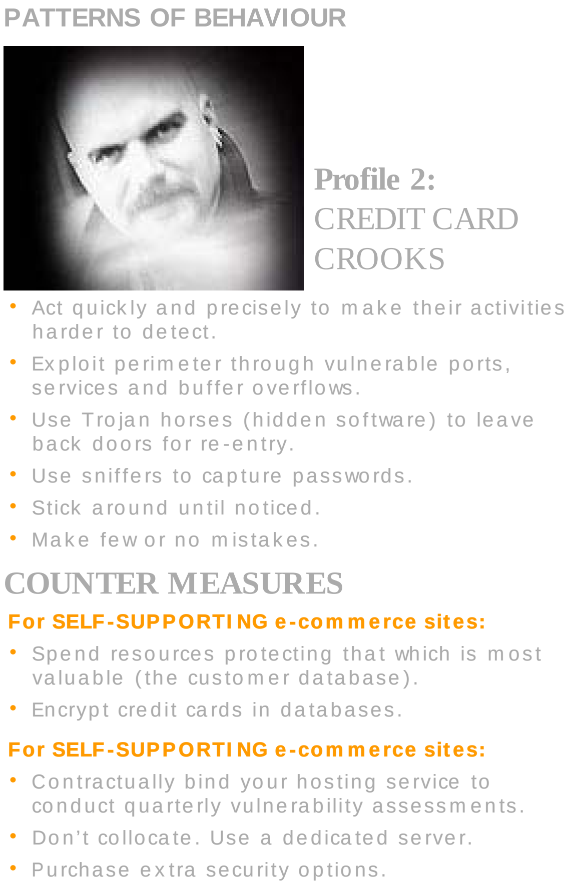
"Carders would love to root servers at e-commerce sites and own them, especially when credit cards are sitting there unencrypted," Clements says. "Then they post them to carder Web sites and say, 'Hey, rate me.' The better your rating, the better your trading privileges."

Increasingly, carders are part of organized crime rings mostly from former Soviet Union states, Kilger says. In these cases, after the cards are used to purchase expensive items, they're posted at carder sites to obscure their usage patterns and therefore confuse investigators.

Attackers going after e-commerce sites also indiscriminately look for the weakest security . "I call these 'targeted victim attacks.' They gain root with the specific intent to steal something," C&W's Neal says. "I would expect the pattern of intrusion activity to be similar to a 'target of opportunity' attack."

Such an opportunity presented itself in January 2002 to a carder who had rooted at least one server at an e-commerce hosting provider. The case began to unfold in September, when CardCops investigators culled some 60 invoices (complete with purchaser's names, addresses and phone numbers) off Carderplanet.com, a carder Web site since removed.

"We noticed that the invoice numbers had the same long-digit formats. So we started calling the consumers whose card numbers, phone numbers and addresses were on the invoices. We asked them where they shopped. We were able to trace them all back to several merchants at a single hosting provider called Serve.com (since renamed as Datarealm).



PATTERNS OF BEHAVIOUR

Profile 2:
CREDIT CARD
CROOKS

- Act quickly and precisely to make their activities harder to detect.
- Exploit perimeter through vulnerable ports, services and buffer overflows.
- Use Trojan horses (hidden software) to leave back doors for re-entry.
- Use sniffers to capture passwords.
- Stick around until noticed.
- Make few or no mistakes.

COUNTER MEASURES

For SELF-SUPPORTING e-commerce sites:

- Spend resources protecting that which is most valuable (the customer database).
- Encrypt credit cards in databases.

For SELF-SUPPORTING e-commerce sites:

- Contractually bind your hosting service to conduct quarterly vulnerability assessments.
- Don't collocate. Use a dedicated server.
- Purchase extra security options.

Click to see:

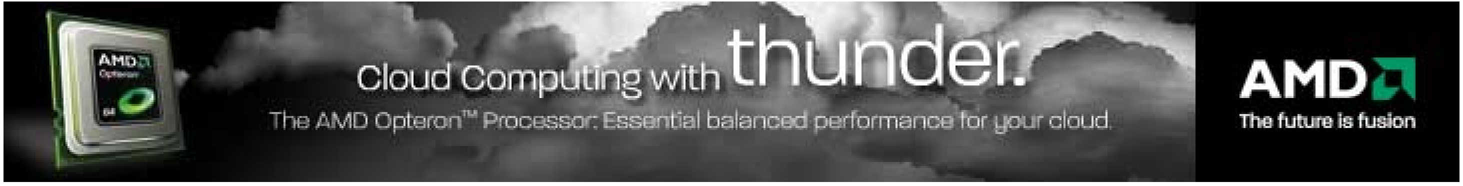
When he called the merchants whose invoices were heisted, they complained that they'd suspected problems for months because cards were approved at the time of purchase, but then declined two weeks later when they rechecked the cards before shipping backorders.

Clements e-mailed Serve.com's system administrator, who attributed the problem to a flaw in the shopping cart software that affected only 24 of Serve.com's 4,000 e-commerce clients. Then in November, a skin care merchant hosted at Serve.com found an alteration to her directory - a page added on Jan. 23, 2003, titled "index.old." She clicked on the page that read, "MuShrooM said That No RedeFace (sic) ! ! nitr0x Ownz serve.com ...lol."

Clients of Serve.com, along with its CEO and systems administrator, didn't return *Network World's* calls about the incident, so details are not forthcoming as to how the carder gained root.

However, Neal surmises that once the perimeter is exploited, carders act more professionally because they don't want to be caught (see graphic, above.)

Main | Next: Profile 3: Filching Files from Within



NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/research/2004/0301hackersprof3.html

Filching files from within

By Deborah Radcliff , Network World , 03/01/2004

Revenge is one reason employees misuse and abuse systems, as was the case when Kenneth Patterson, former data communications manager for American Eagle Outfitters, disabled his company's ability to process credit card purchases for the first five days of the holiday shopping season in 2002. But the most common motivator behind the inside job is a sense of entitlement, experts say.

"The threat from inside is not just disgruntled employees wanting to get even," C&W's Neal says. "Businesses have always had what you could call shrinkage. Employees rationalize stealing pencils, paper clips and bottles of Coke. But with digital assets stored in computers, this process becomes more impersonal, repeatable - and scalable. Now you can steal a case of pencils instead of a box of pencils, metaphorically speaking."

So strong is this feeling of entitlement that employee theft of data makes up about 75% of the cases investigated by Anton Litchfield, director of forensics consulting services for NTI, an electronic evidence discovery firm.

For example, last summer a vice president of sales for a stock analysis firm quit to go to a competitor. But before she left, she copied the customer database to take with her.

Suspicions were raised when one of her co-workers told his network manager that he'd seen a Windows dialog box copying large files to a folder on her home computer the week before she left - while nobody was at her desk. She'd accessed her office computer from her home computer using GoToMyPC.

PATTERNS OF BEHAVIOUR

Profile 3: INTERNAL ATTACK

- Create network accounts for themselves and their friends.
- Access accounts and applications they wouldn't normally use for their daily jobs.
- E-mail former and prospective employers.
- Conduct furtive instant-messaging chats.
- Visit Web sites that cater to disgruntled employees, such as f'dcompany.com.
- Perform large downloads and file copying.
- Access the network during off-hours.

COUNTER MEASURES

- Enforce least privilege, only allowing access to the resources employees need to do their job.
- Set logs to see what users access and what commands they're putting in.
- Protect those resources that are most important with strong authentication.
- If you see someone accessing something they shouldn't, have that person's manager discuss it with the employee to deter future bad behavior.
- Upon termination, delete all computer and network access.
- When employees leave the company, make a mirror image of their hard drive before reissuing it. That evidence might be needed if your company information turns up at a competitor.

Click to see:

That's when the network manager contacted NTI.

"Through forensics analysis of her home computer, her office computer and the network logs, we were able to prove that she'd accessed those files from home and copied them onto her home computer just before she quit," Litchfield says. "But if that employee hadn't seen her computer copying those files, nobody would have been the wiser."

In cases of both a disgruntled employee causing damage or one who feels entitled to steal, you won't see much digital evidence of a crime, Neal says. That's because they already have the access and the insider knowledge. For example, in the American Outfitters case, for which Patterson was sentenced to 18 months in prison in December 2003, he used his own password to access the system and cause the damage. The female vice president also used her own remote logon program to get to the files she downloaded.

Main | Next: Adrian Lamo: Profiling network administrators

AMD Opteron
Cloud Computing with thunder.
The AMD Opteron™ Processor: Essential balanced performance for your cloud.
▶ Buy Now
AMD
The future is fusion

NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/research/2004/0301hackerslamo.html

Profiling network administrators

By Adrian Lamo , Network World , 03/01/2004

Editor's note: Adrian Lamo, a white hat hacker who pled guilty to accessing The New York Times computers without permission, agreed to share what he knows about some of the common IT security slips network administrators make. Lamo studies journalism at American River College in Sacramento, Calif, as he awaits sentencing next month.

One well-ranked Fortune 500 company was recently hiring a network security professional. The interview process required applicants to wait in the HR lobby, where they could use public workstations to browse job listings.

Cloud Computing with
thunder.
The AMD Opteron™ Processor:
Essential balanced performance for your cloud.
AMD
▶ Buy Now

Although the company had spent a hefty sum on a Cisco PIX firewall installation, it made the mistake of placing these visitor workstations on the internal network where files could be accessed. Rather than invest less than $100 per month to equip the public workstations with their own broadband connection, the firm left a fine trophy for anyone with an interest in competitive intelligence.

Knowledge about potential security threats is generally required for the defense of any complex system. But intruder intelligence is only useful as long as it's not running the show. Otherwise, you'll be predictable by the same schemas you use to predict the actions of others.

For instance, many would-be intruders know that administrators configure their intrusion-detection systems in very linear ways, assuming that intrusions will come in the form of scans, buffer overflows and predefined attack patterns.

One way around this is to simply push random requests through the Web browser, a legitimate point of access. At one company, the Web mail system let users forward their mail to any address with only their Social Security number and last name. However, a quick search revealed a corporate directory that included Social Security numbers of all employees and contractors, including the CEO.

Some companies even put in extra layers of security such as token authentication devices. But again, they perceive the problem incorrectly by forgetting that attacks can't be counted on to originate at the edge of the network.

In the late 1990s, intruders remotely bypassed AOL's SecurID authentication system by developing software that would let them redirect their Internet connections through AOL employee workstations, masked as innocent Web connections. Suddenly AOL's network was riddled with private gateways. AOL's logon servers saw their connections as originating from inside the network, and didn't bother to ask them for a SecurID code. As a result, hundreds of high-profile AOL accounts were compromised.

The belief that attacks will inherently come from the outside sets networks up to fall. Security is not always a linear process. If you're going to profile intruders, profile defenders too - be they good examples, or terrible warnings.

Main | Next: Meeces to pieces: What motivates the computer criminal

NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/research/2004/0301hackersdef.html

Profiling defined

By Deborah Radcliff , Network World , 03/01/2004

Cyber crime profiling is defined as the investigation, analysis, assessment and reconstruction of data from a behavioral/psychological perspective extracted from computer systems, networks and the humans committing the crimes, according to William Tafoya, professor in the national security graduate program at the University of New Haven in West Haven, Conn.

Tafoya contends that serial computer crackers' M.O.s are the same as that of serial murderers and rapists, meaning:

- They're creatures of habit.
- They repeat what works.
- They repeat what feels good.
- They operate up to their abilities.

Back to main feature