NEWSLETTER

Identity Theft 911®

VOLUME 5
ISSUE 9
SEPTEMBER
2008

AMERICA'S LEADING IDENTITY MANAGEMENT AND EDUCATION SOURCE

THIS MONTH'S TOPIC...

Who's in Your Wallet?
Mapping Out the Data Underground.

Notes from our Chairman, Adam K. Levin

While the marketplace in stolen data has, for years, been on the radar of federal law enforcement officials, the topic is one rarely broached in the popular media. This is not wholly unexpected—after all, cybercriminals are by their nature very secretive in their operations, and comparatively few ever get caught. San Jose-based research and security solutions firm Finjan is trying to change that. In a report released in July, the firm dissected the organizational hierarchy of clandestine cybercriminal syndicates, and explained the dangers they pose to organizations and consumers worldwide.

In this month's article, "Inside the Illegal Data Marketplace," we speak to Finjan CTO Yuval Ben-Itzhak about the ever-evolving world of identity-related cybercrime. The accompanying editorial, "The Invisible Hand," is a call for organizations and consumers to arm themselves against this ever-growing threat.

For a complete newsletter archive, visit: www.identitytheft911.org/newsletters
To learn about the latest scams on identity theft, visit: www.identitytheft911.org
Comments, questions? Contact us: newsletter@identitytheft911.com

INSIDE THE ILLEGAL DATA MARKETPLACE

SECURITY GROUP MAPS OUT BLUEPRINT FOR UNDERGROUND CRIME

The motif is the stuff of a true-crime potboiler: after behind-the-scenes reconnaissance, an undercover agent finally comes face-to-face with the shadowy international criminal syndicate he's been pursuing. Or rather, the agent gets only as close as the cybercriminal will allow. Digital crimes call only for digital communications, and in this particular case, the exchange takes place over an instant messaging platform:

PROSPECT:
I wanna buy fresh dumps – do u have?

CYBERCRIMINAL:
Which country dumps u need

PROSPECT:
US and UK

CYBERCRIMINAL:
Yes I have US and UK

"DUMPS" ARE CREDIT AND DEBIT CARD NUMBERS, STOLEN BY THE HUNDREDS OR THOUSANDS AND RE-SOLD IN THE CRIMINAL MARKETPLACE.

Of course, the cybercriminal hasn't a clue whom he's dealing with; in this case, the "prospect" is not an FBI or Interpol agent but a security researcher with Finjan, a private research and technology company based in San Jose, California. (The company's name is derived from the word used both in Arabic and Hebrew to denote a small metal pot used to make coffee; Finjan began in 1996 to protect "Java" applets.) Having tracked the digital footprints of international cybercriminals like these for years, Finjan's clandestine researchers know what to look for and how to ask for it. "Dumps" are credit and debit card numbers, stolen by the hundreds or thousands and re-sold in the criminal marketplace. For the last several years, Finjan's 10-person security research team has been tracking down stolen data and studying the activities of the hackers who acquire it. To see a real-life contact with a cybercriminal unfold we turn again to Finjan's recent quarterly research report, "Q2 2008 Web Security Trends."

PROSPECT:
are they fresh?

CYBERCRIMINAL:
yes freshly 100% original
US/UK
US/UK Mix (20Gold/20Plats/20Biz&Corp/40MCstandard&Classic) bin of my choice-$30/one in the count you taking 100+
US/UK Classic - $40, Debit Classic - $40
US/UK MC Standard - $40
US/UK Gold - $60
US/UK Platinum - $60
US/UK Business/Corporate - $100
US/UK Purchasing/Signature - $120
US/UK MC World - $120

PROSPECT:
so how did you get the data?

CYBERCRIMINAL:
we are group and our boss hack and we sell

CYBERCRIMINAL:
this is our site www.sca**********ling.com
(Finjan has a policy of not revealing the full names of criminal web sites in case they contain malicious code or stolen data.)

"YOU DON'T HEAR ABOUT ALL OF THE [CYBERCRIME], BUT IF YOU ACCUMULATE IT AND AGGREGATE IT TOGETHER, IT'S A MEGA-STORY THAT NO ONE IS TALKING ABOUT," BEN-ITZHAK SAYS.

INSIDE THE ORGANIZATION

According to Finjan, criminal data syndicates operate under a hierarchical structure not unlike that of the Mafia. Its latest report offers side-by-side charts comparing a typical "Mafia Family Tree" to that of a typical cyber-crime organization. The differences between them are few. Each organization begins with a criminal "Boss" who masterminds the operation but doesn't dirty his hands by committing any crimes himself. The "Underboss" is next-in-command, and he serves as the cybercrime organization's Trojan Command and Control center. Beneath the "Underboss" are "campaign managers" who act very much like Mafia capos, each of them leading their own section of the operation and each equipped with the tools they need, Trojan viruses, by their Underboss. Each campaign manager controls his own "affiliate network" that stages attacks and steals data (these are the proverbial Mafia "soldiers" who shoulder the burden of the really dirty work). Finally, the stolen data is sold by "resellers" akin to mob "fences," the intermediaries who trade in stolen wares.

REALITY HASN'T HIT—YET

While the underground data marketplace is well known to the FBI and other law enforcement organizations, everyday consumers may not realize how well organized, widespread and potentially damaging to their welfare this criminal phenomenon can be. Who knew that right now, somewhere in the world, credit and debit card numbers are being sold according to a price schedule not unlike that of a wine club?

According to Finjan, the situation doesn't get the media attention it deserves. "Usually in the media, you hear the mega-stories like TJX and the others," says Finjan Chief Technology Officer Yuval Ben-Itzhak, referring to last year's announcement by the corporate conglomerate (TJ Maxx, Marshalls) that tens of millions of customer debit and credit card numbers had been stolen from its servers (updated estimates put the number close to 100 million). "You don't hear about all of the [cybercrime], but if you accumulate it and aggregate it together, it's a mega-story that no one is talking about," Ben-Itzhak says.

Indeed, the type of activity that led to the TJX breach—the infiltration of corporate or other organizational databases to steal sensitive data—is just one part of the cybercrime problem. A less publicized but no less important aspect involves cybercriminals writing malicious code and attaching it to otherwise benign web sites, Ben-Itzhak says. In the last year, Finjan has found malware on sites ranging from Snapple.com to SFGov.org, the official site of the city and county of San Francisco.

"STARTING AT THE END OF 2007, WE STARTED TO SEE, MORE AND MORE, NOT PROFESSIONAL HACKERS DOING THE CRIME—BUT ACTUALLY, AMATEURS," SAYS BEN-ITZHAK.

When consumers visit infected web pages without the protection of anti-virus software, they risk having their computers infected by "keylogger" programs that record everything typed onto a keyboard and send it to the hackers. This stolen data is stored on servers worldwide, a commodity ready to be exchanged illegally.

"You get infected and you don't even know because nothing changes on your PC," Ben-Itzhak says. "But when you go and shop online or log in to your bank or read your email, someone behind the scenes in the back of your head is kind of watching you, collecting the data and sending it out, and that is the key motivation for hackers today—to get the data because later they can sell it and cash out."

CRIMINAL EVOLUTION

Today's cybercrime landscape has evolved just as surely as the computing systems that hackers seek to manipulate. In the tech-Paleolithic 1990s, malware, or malicious software, was primarily an indulgence of young computer geeks, "script kiddies" motivated by the fame and notoriety achieved by crashing home or corporate computers. Hackers derived their satisfaction simply by shutting down e-mail servers or infecting documents created using Microsoft Office products. The emergence of Windows as a popular computing platform allowed the hackers to proliferate, sharing their tips and experiences in exposing new vulnerabilities.

In 2001, things started to change. A criminal breed of hackers realized there was money to be made exploiting computer security weaknesses, and they began writing scripts to steal personal data or financial information stored or transmitted on computers. Hackers searched for vulnerabilities in popular platforms and sold these to bidders in underground cyber-criminal marketplaces. The crime evolved and soon, cybercriminals began developing and selling software packages to less tech-savvy denizens of the criminal marketplace. These toolkits amounted to a "one-stop crimeware shop," according to Finjan's report. They allowed users to surreptitiously install "keylogging" programs and begin harvesting sensitive data on their own.

As the crime spread, Finjan says, it was no longer limited to experts. "Starting at the end of 2007, we started to see, more and more, not professional hackers doing the crime—but actually, amateurs," says Ben-Itzhak. "By amateurs, I mean people who do not have a security background or computer science background." But, as is often the case, inexperienced users made rookie mistakes when they set up their new software: They didn't secure their servers. That meant the data they

THE DATA WAS UNPROTECTED, MEANING IT WAS FREELY ACCESSIBLE TO ANYONE, AND CONTAINED 1.4 GB OF STOLEN DATA—THE DIGITAL STORAGE EQUIVALENT OF ABOUT 1,000 NOVELS.

stored was open to being cached on Google and subject to retrieval via a simple Google search. Earlier this summer, a Colorado woman got a call from a reporter for the San Francisco Chronicle, who asked her whether she was aware that her frequent flier numbers and passwords, home address, phone number and even a conversation she was having with some friends had come up on a Google search for her name. The data had been stored on a server in Malaysia. Of course she had no idea, and Finjan warns there are many more like her. In May, Finjan reported that it had discovered a domain name that was being used as a repository for data harvested through crimeware. The data was unprotected, meaning it was freely accessible to anyone, and contained 1.4 GB of stolen data—the digital storage equivalent of about 1,000 novels.

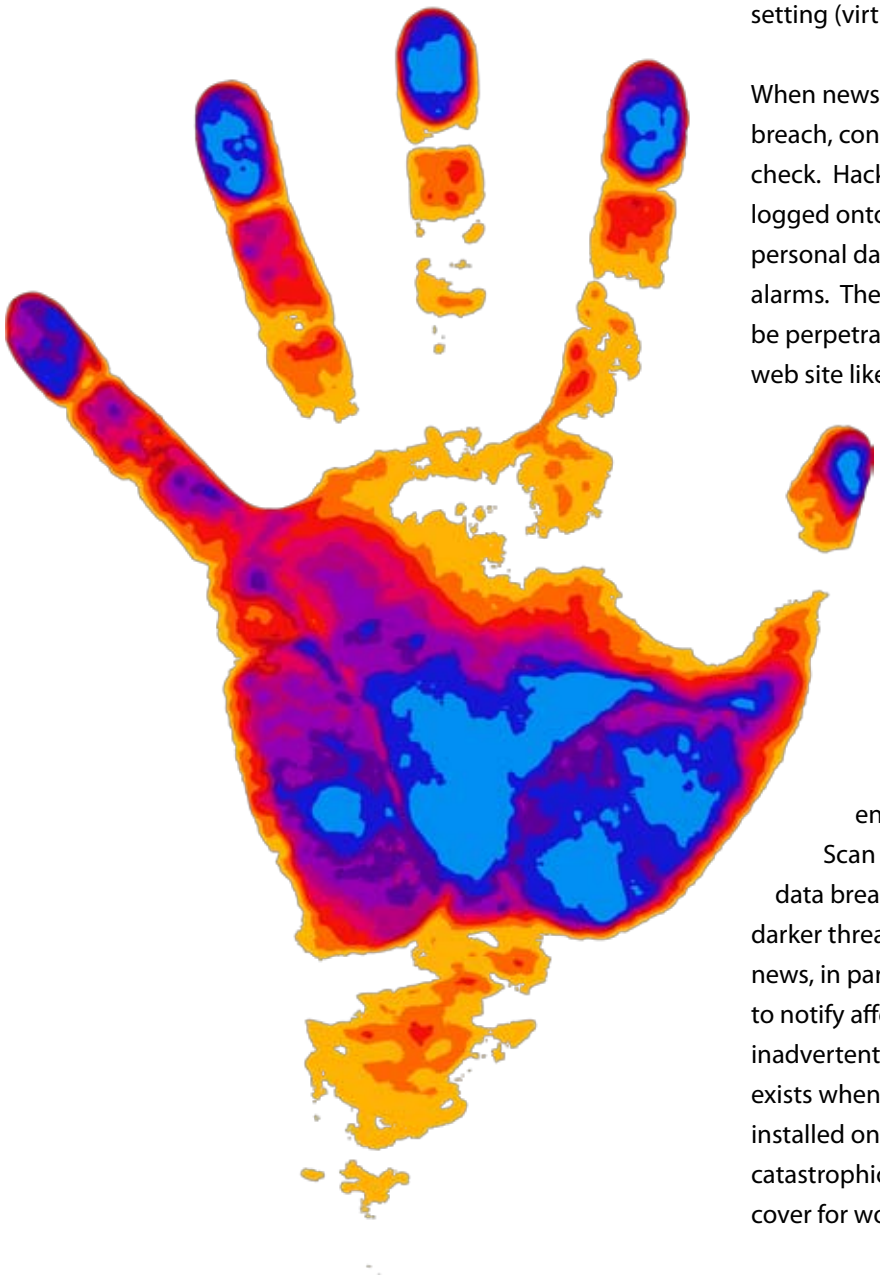
THE SCOPE—UNKNOWN, BUT DEFINITELY GROWING

One indicator that the data black market is increasing is the prices that credit cards fetch. Ben-Itzhak says prices on credit card numbers dropped sharply last year from around $100 to $15 a pop. "The hackers are now moving toward a different type of data that can still charge a premium price," he says. The new frontier? Health care data. Ben-Itzhak says he worries about the trend toward putting personal health information online. His researchers often Google username and password information on crimeware servers. "If your medical history will be behind this username and password, you're done," he says.

Nobody can say for sure exactly how much stolen data is being trafficked via this underground economy. Industry security vendors report that the use of malware by cybercriminals has risen unequivocally since 2007. In April, the Russian computer security company Kapersky Lab predicted that by year-end 2008, malware will have increased ten-fold. If the tools used to steal data are more abundant than ever before—and most law enforcement agencies are reporting increases in identity theft and credit-related fraud—the assertion that Social Security numbers and credit and debit card numbers are in greater supply on the black market is not difficult to accept. Ben-Itzhak says that his team finds new, stolen data online nearly every day, and that his researchers have already detected several hundred servers hosting stolen sensitive data. But the Finjan CTO warns that this is a fraction of what is likely out there. "Most likely, there are thousands or tens of thousands. We are just limited in our resources to find them." ■

The Invisible Hand

Businesses and Consumers Must Brace for the Worst—and Protect Themselves



Gone are the days when you knew you could reasonably avoid peril by staying away from the dodgier realms of the Internet. Now, by simply visiting a legitimate website that hasn't been secured—a city government's, for example—you may actually be setting (virtual) foot into a hacker's den and never even know it.

When news broke last summer of the watershed Monster.com breach, consumers everywhere were socked with a terrifying reality check. Hackers had used stolen job recruiter names and passwords, logged onto Monster.com and stole 1.3 million pieces of sensitive personal data from job seekers—all without tripping Monster's alarms. The collective fear was palpable: If something like this could be perpetrated through a trusted (and therefore supposedly safe) web site like Monster.com, who's to say it couldn't happen with other mainstream, trusted web sites?

Since then, it has happened—and numerous times.

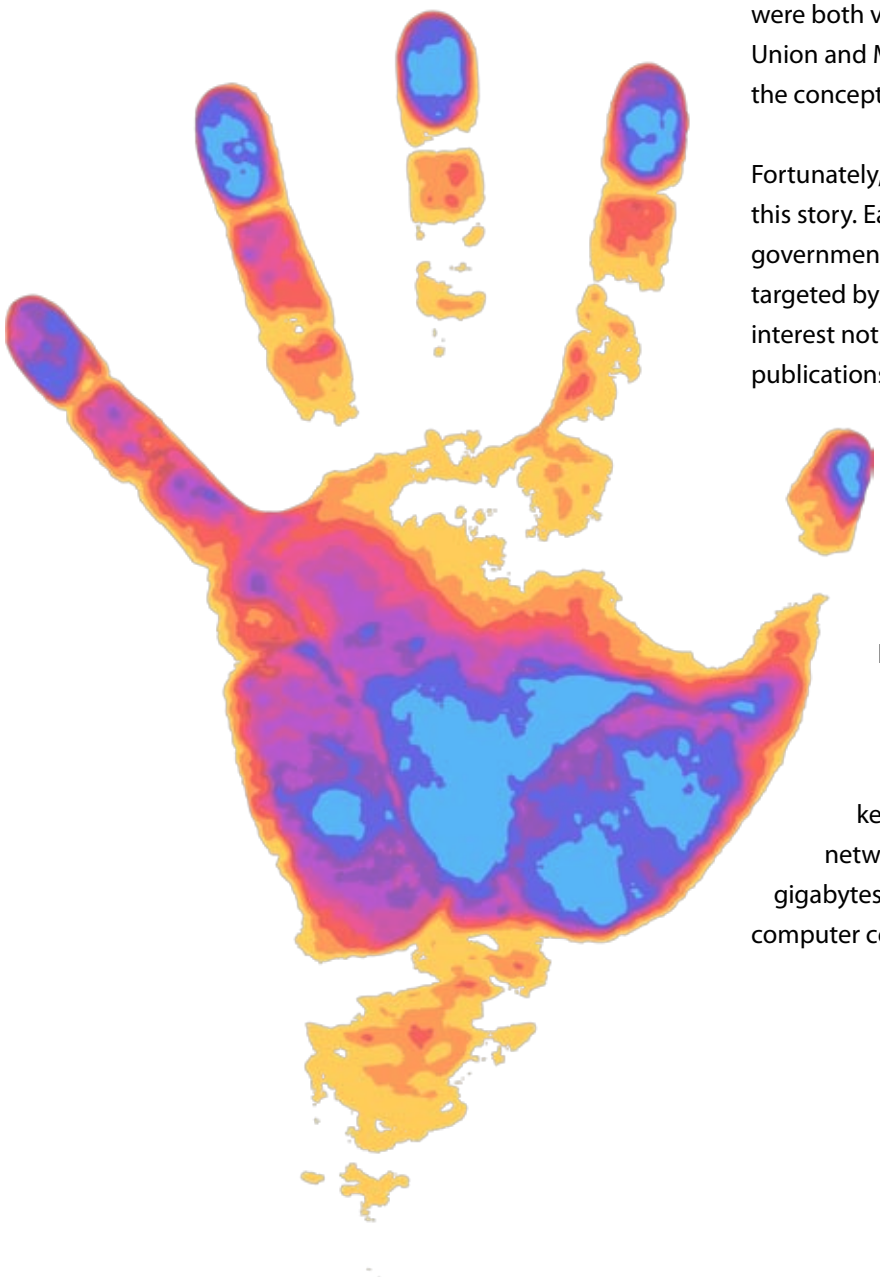
What's even more terrifying? That technology has democratized the hacker playing field.

Not necessarily in the news

If you look to the news for a definitive picture of the enemy we now face, for the most part, you won't find it. Scan the headlines, and you might develop a healthy fear of data breaches—as well you should—but you might overlook a darker threat. Data breaches like last year's colossal TJX fiasco make news, in part, because laws in many states require organizations to notify affected consumers when data is either snatched or inadvertently released into the ether. However, no such mechanism exists when data is compromised through a keylogger program installed on a computer by a stealthy hacker. So many of these catastrophic events go unnoticed, under the radar. It's the perfect cover for would-be identity thieves.

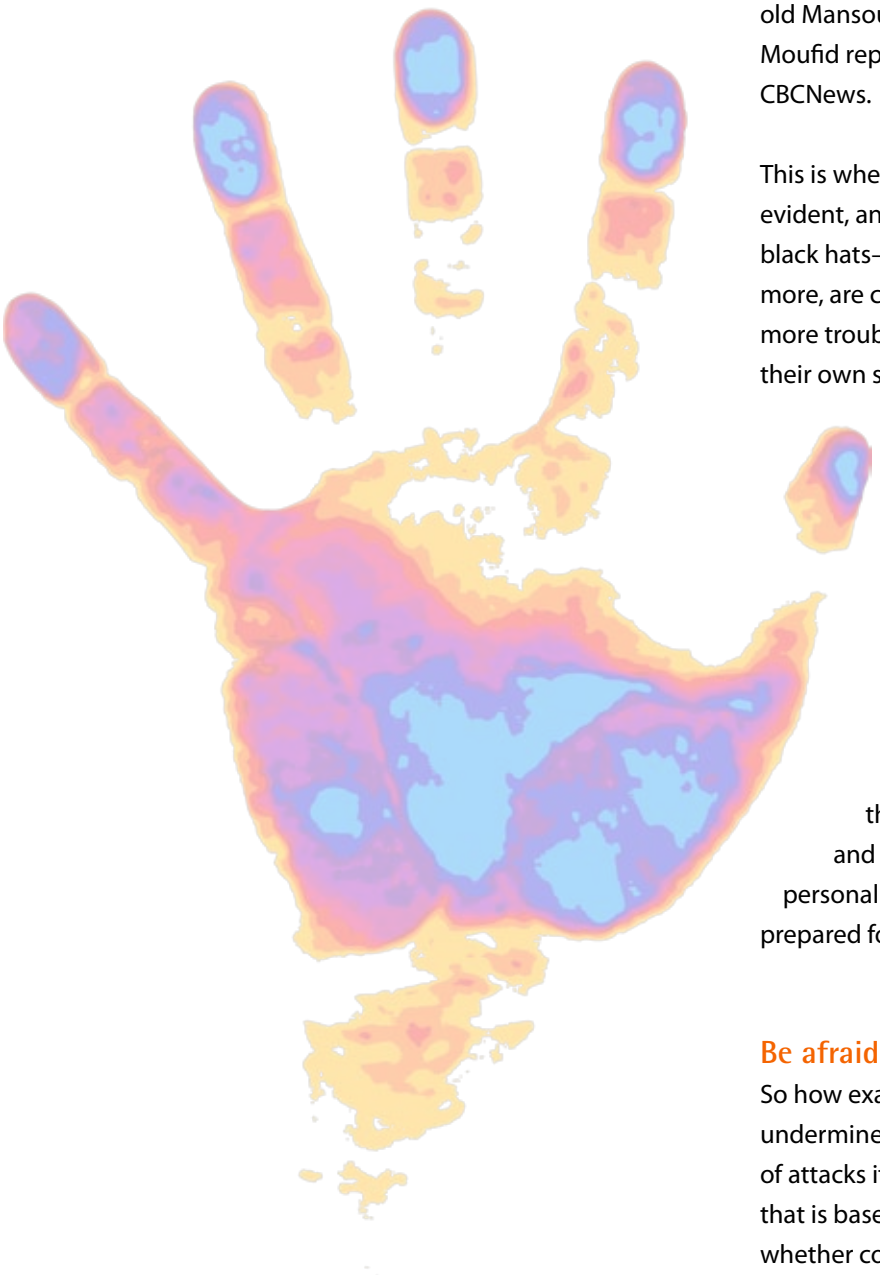
Thus, we're left to rely upon the tactical research of law enforcement organizations, non-profit groups and private security vendors (like Finjan) to keep us abreast of criminal cyber-activity. Through its blog and quarterly reports, Finjan's Malicious Code Resource Center offers insight on how hackers organize and execute attacks on consumers. It's prime reading material for anyone whose personal data has ever been transmitted over the Internet or entered onto a computer connected to the Internet.

And how truly eye-opening something like Finjan's blog is. For example, did you ever wonder how cyber-criminals pay for your stolen data? According to Finjan's report, e-Gold and WebMoney were both viable options for one criminal group, as were Western Union and MoneyGram (evidently, cybercriminals don't subscribe to the concept "never leave home without" their credit cards).



Fortunately, more and more media outlets are catching on to this story. Earlier this summer, when Finjan reported that 1,000 governmental, retail, health care and advertising web sites were targeted by sophisticated SQL injection attacks, it generated interest not just in the high-tech press but in blogs affiliated with publications including the San Francisco Chronicle and The Guardian in the UK.

Likewise, a finding from the Atlanta-based malware research firm SecureWorks earned a mention in an article appearing in the Technology section of The New York Times. SecureWorks's director, Joe Stewart, had determined that a Russian gang was controlling as many as 100,000 infected computers across the Internet. According to the Times, the system relied on botnets (networks of afflicted computers) to infect PCs with a keystroke-recording program known as "Coreflood." The network of infected computers collected as much as 500 gigabytes of data and sent it to a commercial Internet hosting computer center located in Wisconsin, according to the Times.



"Average Joe" hackers on the rise

How else are hackers using keyloggers? At Canada's Carleton University, one student hacktivist accessed 32 electronic accounts equipped to buy food, books and other school supplies by installing a keylogging program on a campus computer. With the information he obtained, the student was able to hack into fellow students' emails and had full access to their accounts. He said he wasn't out to commit financial fraud. In fact, he shared with university administrators a 16-page document detailing exactly how he did it—a gesture some observers took to be consistent with "white hat" hacking, motivated by a desire to point out security holes. Though the student hacker tried to remain pseudonymous, authorities identified him as 20-year-old Mansour Moufid. He now faces criminal charges. As a sidenote—Moufid reportedly wrote the software in "two hours," according to CBCNews.

This is where the democratizing effects of technology are becoming evident, and frighteningly so. While many hackers—white hats and black hats—are certified pros, the idea that rank amateurs, more and more, are commandeering crimeware kits stands among Finjan's more troubling findings. But it doesn't stop there. By failing to secure their own sites, the amateurs then wind up releasing personal data into the great morass of information identifiable through Google web searches. It's a sad day when hack identity thieves can do potentially more damage than old pros—but don't blame Google for archiving their handiwork. The popular search engine is merely doing its job by cataloguing web information and making it searchable by keywords. It's up to consumers and businesses to protect themselves, to make sure two-bit hackers don't find ways to take their information and run with it—to Eastern Europe, Asia, or anywhere else that hackers operate remotely. Anyone with the ill intent and an Internet connection can now find a way to extract your personal data, largely without detection, especially if you're not prepared for the threat.

Be afraid...be very afraid

So how exactly were so many mainstream, "trusted" web sites undermined by hackers in this latest wave? Finjan says that the types of attacks it is detecting are intended to thwart security technology that is based on "signatures"—that is, technology that determines whether content is safe based on its origin. In the cases Finjan

has studied, hackers have been able to insert malicious code into otherwise legitimate web sites, rendering signature-based security measures unable to detect the attacks. A number of companies, including Finjan, offer solutions intended to protect businesses and end-users (in Finjan's case, a secure browser intended to protect consumers from malware is free).

Legislative strides

Senators Patrick Leahy and Arlen Specter have emerged as advocates in the fight against cybercrime. Late this month, the senators' Identity Theft Enforcement and Restitution Act passed the Senate and House and was awaiting signature into law by President Bush. Notably among other provisions, victims of identity theft and other cybercrimes are allowed to seek restitution in federal court, in the proposed bill, not only for any monies stolen from them directly, but also from the loss of time and money they incurred while trying to undo the damage done to their lives by identity thieves. The legislation also addresses emerging technological threats to our identities, making it a felony to infect computers with spyware or keyloggers. Under this law, according to a statement by Specter, "the most egregious identity thieves will not escape with a minimal, or no, sentence." We're fervent advocates for strong penalties and deeply appreciate our lawmakers' unwavering efforts to combat these crimes—the legislation is a considerable step in the right direction, to be sure. But the ugly reality is that for every hacker who does get caught, there are countless others who escape detection—which unfortunately means that consumers and organizations still must remain on red alert.

Bottom line, consumers and businesses must look to good technology to fight the bad, to research commercially available products and choose the solutions that work for them. As Finjan has ascertained through its findings, organizations are caught off-guard when malicious code is inserted in their sites. It's important, then, for organizations to not only employ strategies to ward off attackers, but to also employ technologies that keep tabs on attempted network intrusions. Hackers know a good offense responds to defensive strategies, and it's important to adjust defenses accordingly. The stakes are simply too high to do otherwise. ■