

The biggest retail hack in U.S. history wasn't particularly inventive, nor did it appear destined for success. In the days prior to Thanksgiving 2013, someone installed malware in Target's security and payments system designed to steal every credit card used at the company's 1,797 U.S. stores. At the critical moment—when the Christmas gifts had been scanned and bagged and the cashier asked for a swipe—the malware would step in, capture the shopper's credit card number, and store it on a Target server commandeered by the hackers.

It's a measure of how common these crimes have become, and how conventional the hackers' approach in this case, that Target was prepared for such an attack. Six months earlier the company began installing a \$1.6 million malware detection tool made by the computer security firm FireEye, whose customers also include the CIA and the Pentagon. Target had a team of security specialists in Bangalore to monitor its computers around the clock. If Bangalore noticed anything suspicious, Target's security operations center in Minneapolis would be notified.

On Saturday, Nov. 30, the hackers had set their traps and had just one thing to do before starting the attack: plan the data's escape route. As they uploaded exfiltration malware to move stolen credit card numbers—first to staging points spread around the U.S. to cover their tracks, then into their computers in Russia—FireEye spotted them. Bangalore got an alert and flagged the security team in Minneapolis. And then ...

Nothing happened.

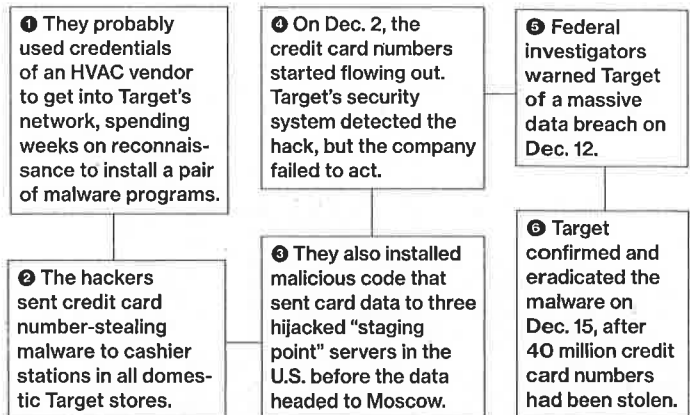
For some reason, Minneapolis didn't react to the sirens. *Bloomberg Businessweek* spoke to more than 10 former Target employees familiar with the company's data security operation, as well as eight people with specific knowledge of the hack and its aftermath, including former employees, security researchers, and law enforcement officials. The story they tell is of an alert system, installed to protect the bond between retailer and customer, that worked beautifully. But then, Target stood by as 40 million credit card numbers—and 70 million addresses, phone numbers, and other pieces of personal information—gushed out of its mainframes.

When asked to respond to a list of specific questions about the incident and the company's lack of an immediate response to it, Target Chairman, President, and Chief Executive Officer Gregg Steinhafel issued an e-mailed statement: "Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach. As a result, we are conducting an end-to-end review of our people, processes and technology to understand our opportunities to improve data security and are committed to learning from this experience. While we are still in the midst of an ongoing investigation, we have already taken significant steps, including beginning the overhaul of our information security structure and the acceleration of our transition to chip-enabled cards. However, as the investigation is not complete, we don't believe it's constructive to engage in speculation without the benefit of the final analysis."

More than 90 lawsuits have been filed against Target by customers and banks for negligence and compensatory damages. That's on top of other costs, which analysts estimate could run into the billions. Target spent \$61 million through Feb. 1 responding to the breach, according to its fourth-quarter report to investors. It set up a customer response operation, and in an effort to regain lost trust, Steinhafel promised that consumers won't have to pay any fraudulent charges stemming from the breach. Target's profit for the holiday shopping period fell 46 percent from the same quarter the year before; the number of transactions suffered its biggest decline since the retailer began reporting the statistic in 2008.

In testimony before Congress, Target has said that it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that company investigators went back to figure out what happened. What it hasn't publicly revealed: Poring over computer logs, Target found FireEye's alerts from Nov. 30 and

How the Hackers Broke In



more from Dec. 2, when hackers installed yet another version of the malware. Not only should those alarms have been impossible to miss, they went off early enough that the hackers hadn't begun transmitting the stolen card data out of Target's network. Had the company's security team responded when it was supposed to, the theft that has since engulfed Target, touched as many as one in three American consumers, and led to an international manhunt for the hackers never would have happened at all.

The heart of Target's antihacking operation is cloistered in a corner room on the sixth floor of a building in downtown Minneapolis. There are no internal-facing windows, just a locked door. Visitors ring a bell, then wait for a visual scan before being buzzed in.

If you've seen one security operations center, or SOC, you've essentially seen them all. Inside, analysts sit in front of rows of screens that monitor Target's billion-dollar IT infrastructure. Government agencies often build their own SOCs, as do big banks, defense contractors, tech companies, wireless carriers, and other corporations with centralized stockpiles of high-value information. Retailers, however, tend not to. Most still focus on their primary mission, selling stuff—in part because their sprawling networks of stores and e-tailing entry points are difficult to lock down against incursions. A three-year study by Verizon Enterprise Solutions found that companies discover breaches through their own monitoring in only 31 percent of cases. For retailers, it's 5 percent. They're the wildebeests of the digital savannah.

Target was striving to be different. Company officials say its information security staff now numbers more than 300 people—a tenfold increase since 2006, says one of the chain's former information security managers. Less than a year before the Thanksgiving attack, Target brought in FireEye, a security software company in Milpitas, Calif., that was initially funded by the CIA and is used by intelligence agencies around the world.

The system works by creating a parallel computer network on virtual machines. Before data from the Internet reach Target, they pass through FireEye's technology, where the hackers' tools, fooled into thinking they're in real computers, go to work. The technology spots the attack before it happens, then warns the customer. Unlike antivirus systems, which flag malware from past breaches, FireEye's isn't as easily tricked when hackers use novel tools or customize their attack, customers say. "It's a very smart approach," says Robert Bigman, the CIA's former chief information security officer. "When we first started working with them several years ago, no one ever thought of doing it that way."

On Nov. 30, according to a person who has consulted on Target's investigation but is not authorized to speak on the record, the hackers deployed their custom-made code, triggering a FireEye alert that indicated unfamiliar malware: "malware.binary." Details soon followed, including addresses for the servers where the hackers wanted their stolen data to be sent. As the hackers

inserted more versions of the same malware (they may have used as many as five, security researchers say), the security system sent out more alerts, each the most urgent on FireEye's graded scale, says the person who has consulted on Target's probe.

The breach could have been stopped there without human intervention. The system has an option to automatically delete malware as it's detected. But according to two people who audited FireEye's performance after the breach, Target's security team turned that function off. Edward Kiledjian, chief information security officer for Bombardier Aerospace, an aircraft maker that has used FireEye for more than a year, says that's not unusual. "Typically, as a security team, you want to have that last decision point of 'what do I do,'" he says. But, he warns, that puts pressure on a team to quickly find and neutralize the infected computers.

Target had done a months-long test of FireEye that ended in May and was rolling out the technology throughout the company's massive IT system. It's possible that FireEye was still viewed with some skepticism by its minders at the time of the hack, say two people familiar with Target's security operations. And the SOC manager, Brian Bobo, departed the company in October, according to his LinkedIn page, leaving a crucial post vacant. (Bobo declined to comment.) Yet it was clear Target was getting warnings of a serious compromise. Even the company's antivirus system, Symantec Endpoint Protection, identified suspicious behavior over several days around Thanksgiving—pointing to the same server identified by the FireEye alerts. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee. If Target had had a firm grasp on its network security environment, he adds, "they absolutely would have observed this behavior occurring on its network."

Target's security blunders don't end there. Its spokeswoman, Molly Snyder, says the intruders had gained access to the system by using stolen credentials from a third-party vendor. Brian Krebs, a security blogger whose site krebsonsecurity.com first broke the news of the Target hack, has reported that the vendor was a refrigeration and heating company near Pittsburgh called Fazio Mechanical Services. A statement on Fazio's website says its IT systems and security measures are in compliance with industry practices, and its data connection to Target was purely for billing, contract submission, and project management. Target's system, like any standard corporate network, is segmented so that the most

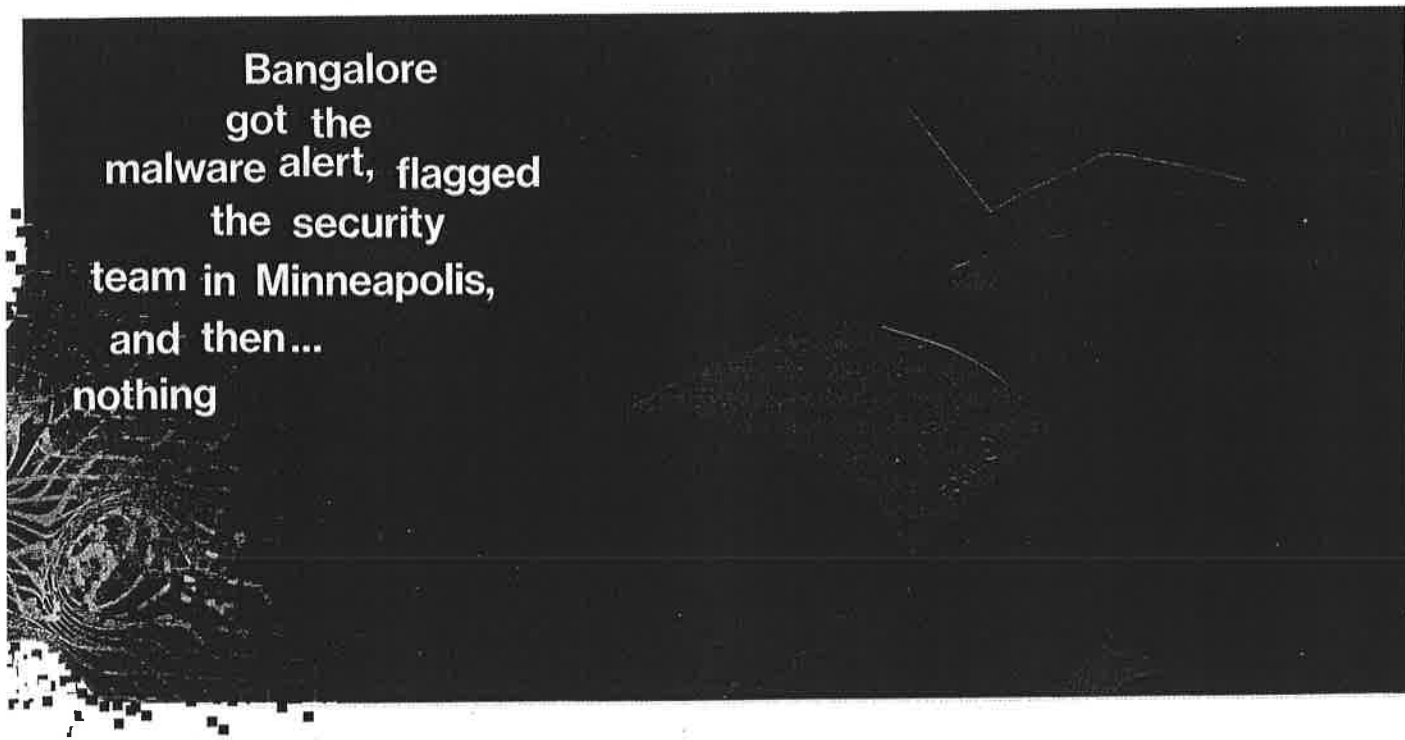
sensitive parts—including customer payments and personal data—are walled off from other parts of the network and, especially, the open Internet. Target's walls obviously had holes. The hackers' malware disguised itself with the name BladeLogic, probably to mimic a component in a data center management product, according to a report by Dell SecureWorks. (SecureWorks is one of many cybersecurity firms that got their hands on the Target malware, which was made public on various websites used by researchers to help other companies fend off similar attacks.) In other words, the hackers cloaked their bad code with the name of legitimate software used by companies to protect cardholder and payment data.

Once their malware was successfully in place on Nov. 30—the data didn't actually start moving out of Target's network until Dec. 2—the hackers had almost two weeks to pillage credit card numbers unmolested. According to SecureWorks, the malware was designed to send data automatically to three different U.S. staging points, working only between the hours of 10 a.m. and 6 p.m. Central Standard Time. That was presumably to make sure the outbound data would be submerged in regular working-hours traffic. From there the card information went to Moscow. Seculert, an Israeli security firm, was able to analyze the hackers' activity on one of the U.S.-based staging points, which showed them eventually taking 11 gigabytes of data stored there to a Moscow-based hosting service called vpsville.ru. Alexander Kiva, spokesman for vpsville.ru, says the company has too many clients to monitor them effectively, and that it hadn't been contacted by U.S. investigators as of February.

If Target's security team had followed up on the earliest FireEye alerts, it could have been right behind the hackers on their escape path. The malware had user names and passwords for the thieves' staging servers embedded in the code, according to Jaime Blasco, a researcher for the security firm AlienVault Labs. Target security could have signed in to the servers themselves—located in Ashburn, Va., Provo, Utah, and Los Angeles—and seen the stolen data sitting there waiting for the hackers' daily pickup. But by the time company investigators figured that out, the data were long gone.

Federal law enforcement officials contacted Target about the breach on Dec. 12, according to congressional testimony. CEO Steinhafel has said that it took his company three days to confirm it. The authorities had more than just reports of fraudulent charges to go on, however: They had obtained the actual stolen data, which the hackers had carelessly left on their dump servers, →

**Bangalore
got the
malware alert, flagged
the security
team in Minneapolis,
and then...
nothing**



according to a person familiar with the federal investigation.

The guts of the malware code provided some intriguing leads. One of the passwords was Crisis1089. That happens to be the nickname of an Xbox gamer. (His rank on the Xbox Live global leaderboard as of March 10: 11,450,001.) It also appears to be a reference to the October 1989 date of mass protests that preceded Ukrainian independence and the dissolution of the Soviet Union.



There was another name embedded in the exfiltration code: Rescator. The alias, a reference to a pirate in the 1967 French film *Indomptable Angélique*, belongs to a prolific Ukrainian trafficker in stolen credit card numbers. Rescator operates several online card number sites—cheapdumps.org and Lampeduza.la, to name two—that use the country domains of Laos, Somalia, and the former Soviet Union, among others. Rescator isn't the only reseller pushing the stolen Target data, but according to Krebs and several other security investigators, he's the most active, apparently operating with impunity out of the Black Sea port of Odessa.

Odessa is the Tortuga of the Russian-speaking world, notorious since czarist times as a gathering spot for gangsters, swindlers, and pirates. Today it's a haven for "carders." In a milestone for credit card theft, a group of Russian-speaking hackers in May 2001 set up a digital crime syndicate called Carderplanet that for the next few years held annual conventions in Odessa, according to the U.S. Secret Service. Carderplanet grew to become the world's biggest online marketplace for stolen card data, with more than 6,000 members, many of them recruited through an online ad campaign that promised, "Dumps—credit cards—will make you rich!"

The U.S. Justice Department worked with European law enforcement agencies to shut down Carderplanet in the mid-2000s. All that did was move Odessa's carder scene underground. The ringleaders of today's carding operations "never meet, they never know each other's names," says Ilya Zadorozhko, one of the deans of Odessa's hacker community, who currently makes his living aboveboard, as a network specialist for a Dutch IT group. "There are only private messages, strictly anonymous."

And there are assumed names, such as Rescator. In posts to vor.cc, an online forum for Russian hackers, Rescator said he had also gone by the nickname Helkern. Photos, e-mail addresses, and other details that Helkern posted online show a 22-year-old from Odessa named Andrey Khodyrevskiy. An in-house blog at Netpeak, an Odessa marketing company where Khodyrevskiy once worked, confirms that he went by the nickname Helkern. A photo of a Helkern, posted on a website called Darklife that was co-founded by a person using the nickname, was identified by Netpeak's CEO as Khodyrevskiy.

Still, there's no definitive proof that Rescator and Khodyrevskiy are the same person. Krebs, the security blogger who first disclosed the Target hack, reported that when he sent an instant message to one of Rescator's addresses, asking to speak with "Rescator a/k/a Andrey," he got a reply from someone asking why he wanted to contact that person. Later he got a message from Rescator's address offering him \$10,000 not to publish his article, which identified Rescator as Khodyrevskiy. U.S. Secret Service Special Agent Brian Leary, spokesman for the cybercrime unit, says the agency could not comment on whether it was investigating the identity of Rescator or had linked the carder site to a particular individual.

There is proof that Khodyrevskiy is a hacker, if not an accomplished one. One morning in February 2011, users of Odesskiy Forum, a popular Odessa Web portal, awoke to find the site

riddled with error messages. Administrators swiftly determined that a hacker had planted malware on the site and stolen the e-mail addresses of 190,000 users. Breaking in was easy, because an administrator's password had been left visible in a rarely used part of the portal—"an awful mistake," owner Dmitriy Kozin says. Still, it was hard to understand why anyone would want to hack a site that offers a blend of local news, Craigslist-type advertising, and discussion groups on everything from philosophy to pet grooming—and doesn't store any financial data or other sensitive information.

The Odesskiy Forum hacker screwed up: He streamed the stolen e-mail addresses to a proxy server that didn't have enough capacity to absorb them all. Some data spilled over into the hacker's own computer, exposing his IP address. Kozin alerted Ukrainian security police, and within days they'd made an arrest: Khodyrevskiy. He was convicted and received a three-year suspended sentence. Kozin, for one, finds it hard to believe that this inept small-time hacker could have masterminded one of the biggest credit card heists ever. "He was lame, really unprofessional," he says.

Before his arrest, Khodyrevskiy worked as a programmer at Netpeak. Founder and CEO Artyom Borodatyuk recalls Khodyrevskiy as "a talented programmer with discipline problems," unreliable and frequently late for work. When police stormed the premises in early 2011 and said they were looking for a hacker, he says, "I thought of Andrey at once." Borodatyuk fired Khodyrevskiy after the police took him away and says he's had no further contact with his former employee.

Bloomberg Businessweek was unable to reach Khodyrevskiy. E-mail and instant messages sent to addresses he's used bounced back or went unanswered. A cell phone he used previously has been disconnected. There was no trace of him at the downtown Odessa address for Ghost.ua, a Web hosting company he ran for a time.

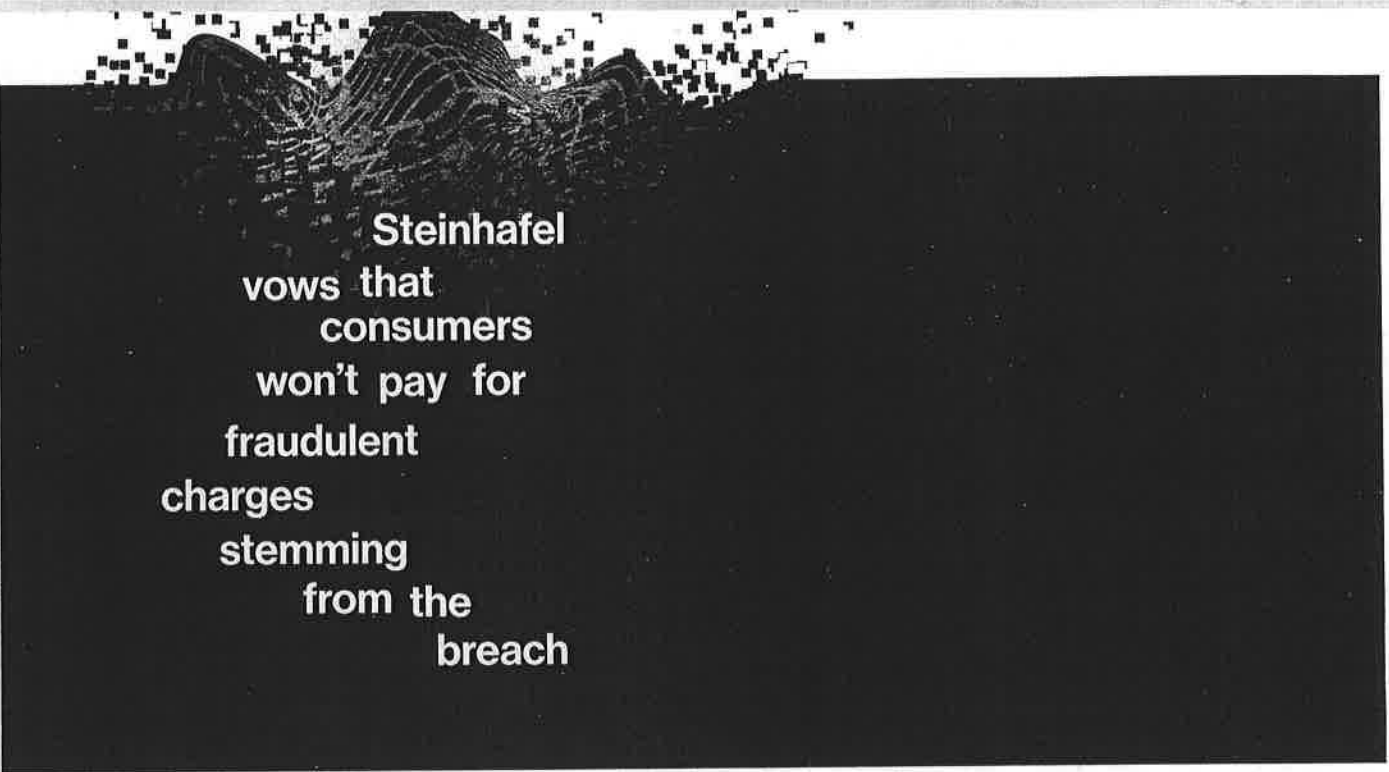
Four consultants familiar with the Target probe say it's likely that Rescator wrote the Target malware. The word "Rescator" ended up in the Target code by mistake: It's the name of the home directory of the computer on which the code was compiled. For Zadorozhko, the reformed hacker, the fact that an alias showed up in the Target malware suggests that Rescator was, at best, a low-level "monkey" in the operation who was merely given blocks of the stolen cards to sell. "Nobody who is serious would do such a stupid thing as to put his name there," he says.

All this means is that it's unlikely someone with Rescator's skill set would have acted alone. Modern computer crime is often a group affair, committed by gangs whose members bring different capabilities to the caper. In recent congressional testimony, William Noonan, deputy special agent in charge of the Secret Service's cybercrime investigations division, likened it to the movie *Ocean's Eleven*. To apply the comparison to the Target hack, Rescator may have been George Clooney—the ringleader who recruited other criminals with the real skills. Rescator wrote the code, investigators suggest, then worked with a group of more expert hackers who breached the network and removed the data. The group he worked with are relative newcomers, and the network of servers they used, along with other clues, connect them to at least six other data thefts over the last two years, investigators say.

Top 10 Biggest Data Breaches* By Number of Records Stolen

200,000,000	Experian (2013)
152,000,000	Adobe Systems (2013)
130,000,000	Heartland Payment Systems (2008)
110,000,000	Target (2013) ←
104,000,000	Korea Credit Bureau (2014)
94,000,000	TJX (2007)
90,000,000	TRW** (1984)
77,000,000	Sony (2011)
50,000,000	LivingSocial (2013)
42,000,000	Cupid Media (2013)

*EXCLUDES THE 2013 THEFT OF 140 MILLION ACCOUNTS IN SOUTH KOREA INVOLVING MULTIPLE RETAILERS, E-COMMERCE SITES, AND GAS STATIONS
 **TRW CREDIT REPORTING SERVICE, NOW EXPERIAN
 DATA: OPEN SECURITY FOUNDATION



Steinhafel vows that consumers won't pay for fraudulent charges stemming from the breach

Rescator's flagship site for selling illicit credit card numbers, Rescator.so, is unadorned—no logos, no background images, all business, and extremely user-friendly. Shoppers can buy individual card numbers or load up by the thousands and get a bulk discount. Drop-down menus filter by geographic region, as well as by bank and type of card (ATM, American Express Blue, Visa, etc.). You can also filter by expiration date, last four digits, and city. That last feature is particularly impressive, says Mark Lanterman, a former member of the Secret Service Electronic Crimes Task Force who now runs his own digital forensics company, Computer Forensic Services, in Minnetonka, Minn. "Fraudsters want to buy credit cards for areas where they live," he says, to foil banks' fraud monitoring. If a card number attached to a billing address in New Jersey suddenly shows up in Stockholm, that's a red flag.

Lanterman says that 10 years ago, during the era of Carderplanet, websites like Rescator's were public. Now you have to apply for credentials. Lanterman got his after lurking on black market forums, building a presence and a persona as a player in the carder underground. "You just hang out," he says. "Eventually they just think you're the same kind of scumbag they are and say, 'Yep, here's your login.'"

Sitting in his conference room, Lanterman pulls up Rescator.so on his laptop's browser and shows a drop-down menu of cards for sale. He enters towns and cities. For Minnetonka, about 12 miles from Target's headquarters with a population of 51,000, there are 7,000 cards for sale. For another Minneapolis suburb, Plymouth, population 73,000, there are 5,335 cards available. Fayetteville, Ark.: 3,685. Torrington, Conn.: 5,115. The cards run from \$6 apiece for a prepaid gift card to almost \$200 for an American Express Platinum, and Rescator accepts payment in Bitcoin and Western Union. The return period—just in case some of the cards don't work—is six hours, according to the site's Replace Policy page, which is printed in Russian and English for better customer service. Long before six hours elapse, thieves can have the stash of stolen numbers printed on counterfeit cards and charge up a storm of purchases at stores or online, often in the form of gift cards that are easily transformed into cash. Eventually a bank catches wind of the fraud and freezes the card. For the thief, it's on to the next one.

Target first publicly confirmed the breach in a press release at 6 a.m. on Dec. 19. Kelly Warpechowski, a 23-year-old IT recruiter

in Milwaukee, already knew something was wrong. Her bank notified her that someone in Russia had spent \$900 at "an oil company" using her card. Target had been Warpechowski's go-to store, but she says she's visited only twice since.

That night, Jamie Doyle, who's in the Navy and lives in Chesapeake, Va., got a fraud alert from the Navy Federal Credit Union while he was on overnight shipboard duty. His wife, Tracy, a school speech pathologist, checked the next morning and found their debit card had been drained, with more than \$600 in pending charges. "We were literally going in to buy our Christmas dinner, and we had no money," she says. Jamie, who almost never shopped at Target, had used his debit card to grab \$5 worth of groceries from a Chesapeake store on Black Friday. The card number was then used by thieves at an Ellicott City (Md.) Target store, Tracy says. She blames the retailer for the breach and for not checking more closely when the fraudulent user rang up the charges. Why didn't the cashier ask for ID to verify the cardholder, she wonders. The bank credited the Doyles' account in two days, Tracy says. She no longer shops at Target.

The anger has spilled into Congress, where company officials, including Chief Financial Officer John Mulligan, were called to testify in February. On March 10, the House Committee on Oversight and Government Reform received from Target documents related to what executives knew and when they knew it, according to a committee aide who declined to be named. Major banks and store chains are pointing fingers at each other over years of delay in adopting a more secure technology that uses cards with embedded chips. Such cards, now common throughout Europe, are harder to counterfeit than those with magnetic strips. Target executives—Chief Information Officer Beth Jacob resigned on March 5—promise that their company will help lead that transition; they announced in February that they'll spend \$100 million for registers and other technology that read the new cards. Its stock is trading near \$61, almost unchanged since the day it disclosed the hack. FireEye shares have more than doubled, to around \$80.

Sometime in early March someone broke into Rescator.so and stole the logins, passwords, and payment information of carders, then posted the data online. Krebs says it's unclear who was behind the hack, but it appears to be someone who wanted to shut the operation down, possibly vigilantes or competitors. **B**

—With reporting by Dawn Kopecki and Derek Wallbank