10-WIRED-Target Got Hacked

Jan 17, 2014 6:30 AM

Target Got Hacked Hard in 2005. Here's Why They Let It Happen Again *[Anger]*

A gang of shadowy hackers tears through the systems of big-box retailers, making off with millions of credit and debit card numbers in a matter of weeks and generating headlines around the country. Target and Nieman Marcus in 2013? No: This oh-so-familiar attack occurred in 2005 *[Disappointment]*.

To revist this article, visit My Profile, then View saved stories .

Image: Bon Bon/Getty

Save Story

To revist this article, visit My Profile, then View saved stories .

A gang of shadowy hackers tears through the systems of big-box retailers, making off with millions of credit and debit card numbers in a matter of weeks and generating headlines around the country.

Target and Neiman Marcus last week? Nope. This oh-so-familiar attack occurred in 2005.

[Disappointment]

That's when Albert Gonzalez and cohorts – including two Russian accomplices — launched a three-year digital rampage through the networks of Target, TJ Maxx, and about half a dozen other companies, absconding with data for more than 120 million credit and debit card accounts. Gonzalez and other members of his team eventually were caught; he's

serving two concurrent sentences for his role, amounting to 20 years and a day in prison, but the big-box breaches go on.

The latest string of hacks attacking Target, Neiman Marcus, and others raise an obvious question: How is it that nearly a decade after the Gonzalez gang pulled off its heists, little has changed in the protection of bank card data?

[Disappointment]

Target got off easy in the first breach: A spokeswoman told Reuters an "extremely limited" number of payment card numbers were stolen from the company by Gonzalez and his gang. The other companies weren't as lucky: TJX, Hannaford Brothers grocery chain, the Dave & Busters restaurant chain, Office Max, 7-Eleven, BJ's Wholesale Club, Barnes & Noble, JC Penney, and, most severely, Heartland Payment Systems, were hit hard.

This time around, if past is prelude, Target will be forced to pay out millions in fines to the card companies if it's found that the retailer failed to properly secure its network. It also will have to pay reparation to any banks that had to issue new cards to customers. In addition, class-action lawsuits are already being filed against Target by customers, and lawmakers are lining up to make an example of the retailer.

[Legal Action]

But Target's latest misfortune should surprise to no one — least of all Target *[Disappointment]*. The security measures that Target and other companies implement to protect consumer data have long been known to be inadequate *[Disappointment]*. Instead of overhauling a poor system that never worked, however, the card industry and retailers have colluded in perpetuating a myth that they're doing something to protect customer data — all to stave off regulation and expensive fixes *[Disappointment, Anger]*.

"It's a big failure of the whole industry," says Gartner analyst Avivah Litan. "This is going to keep getting worse, and this was totally predictable a few years ago and no one did anything. Everyone got worked up, and no one did anything."

[Disappointment]

What the Target Thieves Got

Not a lot is known about how the latest Target hack occurred. The intruders began the heist November 27, the day before Thanksgiving, and spent two weeks gobbling up unencrypted credit and debit card data for 40 million customers before the company discovered their presence December 15.

In addition to card data, the thieves also swiped PINs for the accounts, though the company says the PINs are worthless because they were encrypted with Triple DES at the card reader, and the key for decrypting them was not stored on Target's system *[Diminish]*. Recently Target revealed that the thieves also absconded with the names, addresses, phone numbers, and email addresses of some 70 million customers – some of whom are the same customers whose card data was stolen. A recent report indicates the hackers got 11 gigabytes of data that was siphoned to an FTP server and from there sent to a system in Russia.

The card data was siphoned from Target's point-of-sale systems, the company says. A report released Thursday by security firm iSight Partners, revealed that the attack involved a RAM scraper , a malicious program that steals data from a computer's memory. It also noted that the operation was "persistent, wide-ranging, and sophisticated."

"This is not just your run-of-the-mill hack," according to iSight, which has been working with law enforcement to investigate the attacks.

But the stolen phone numbers and emails from Target also suggest the attackers accessed a backend database, possibly the Customer Relationship Management system, used to track customer transactions and manage customer service and marketing.

>This is not just your run-of-the-mill hack.

The breach of Neiman Marcus was likely carried out by the same hackers, though the company has not yet revealed how many customers were affected. The New York Times reported that the intrusion began in July and

went undetected for five months until the company discovered the breach this month. At least three other small retailers reportedly were breached as well. They've yet to be identified, and no figure for the number of cards stolen from them has been released.

All of this happened despite the requirement that companies accepting credit and debit cards adhere to a Payment Card Industry standard for security known as PCI-DSS *[Disappointment]*. The standard was developed by Visa and other card companies in part to stave off would-be government regulation, and has been in place since 2001.

It requires, among other things, that companies have firewalls in place, that they have up-to-date antivirus programs installed, and most importantly that card data is encrypted when it's stored or while in transit over a public network. A new version of the standard was released last November, the month Target was breached, that also directs companies to protect credit-card terminals — known as point-of-sale terminals — from physical tampering. This was likely spawned by a wave of hacks in 2012 that involved the physical installation of RAM-scrapers and other malware onto PoS systems by thieves who had access to the devices.

Companies are also required to obtain regular security audits from third-party firms to certify their compliance. The card companies have touted the standards and audits as evidence that customer transactions are secure and trustworthy. Yet nearly every time a breach has occurred since PCI was instituted, the hacked company has in post-breach audits been found to have been out of compliance, even though they had been certified compliant before the breach was discovered.

[Disappointment]

That was the case with at least two of the Gonzalez hacks. Both Heartland Payment Systems and Hannaford Bros. were certified compliant while the hackers were in their system. In August 2006, Wal-Mart was also certified PCI-compliant while unknown attackers were lurking on its network.

CardSystems Solutions, a card-processing company that was hacked in 2004 in one of the largest credit card data breaches at the time, was

breached three months after CardSystems' auditor, Savvis Inc, gave the company a clean bill of health .

Inherent Flaws In the System

All of these companies had different vulnerabilities and were hacked in different ways, but their cases highlight inherent flaws in both the standards and the auditing process that are supposed to keep customer card data secure.

Audits take only a snapshot of a company's security at the time of the audit, which can change quickly if anything on the system changes, introducing new and undetected vulnerabilities. What's more, the auditors rely in part on the companies providing complete and accurate information about their systems — information that isn't always complete or accurate. But the biggest problem is the standard itself.

"This PCI standard just ain't working," says Litan, the Gartner analyst. "I wouldn't say it's completely pointless. Because you can't say security is a bad thing. But they're trying to patch a really weak [and] insecure payment system [with it]."

[Disappointment]

The problem goes right to the heart of the system for processing card payments. With small restaurants, retailers, and others that accept card payments, the transactions go through a processor, a third-party company that reads the card data to determine where to send it for authorization. Large retailers and grocery chains, in contrast, act as their own processor: Card transactions are sent from the company's individual stores to a central point on the corporate network, where the data is aggregated and routed to the proper destination to be authorized.

But both scenarios have a major flaw in that the PCI standards don't require companies to encrypt card data while in transit either on the company's internal network or on its way to a processor, as long as the transmission is over a private network. (If it crosses the public internet it must be encrypted.) Some companies, however, secure the processing channel

through which the data travels — similar to the SSL encryption used to protect website traffic — to prevent someone from sniffing the unencrypted data inside the channel as it moves.

>The problem goes right to the heart of the system.

Target was likely using such a secure channel within its network to transmit unencrypted card data. But that wasn't good enough. The attackers simply adapted by employing a RAM scraper to grab the data in the point-of-sale device's memory, where it was not secured.

A security researcher who has extensive knowledge of card processing systems but asked not to be identified says he first began seeing RAM scrapers used against merchants in late 2007 after another set of PCI standards, known as the Payment Application Data Security Standard was implemented for card readers. Those standards prohibited a widespread practice of storing credit card numbers on point-of-sale terminals long after a transaction was completed, which allowed hackers to copy them at their leisure. The newer standard, along with the practice of sending data through a secure channel, forced hackers to switch their tactics and grab card data during the split-second that it's unsecured in the memory of POS systems while the transaction is in progress.

"Criminals learned that if they used a RAM scraper, there will be a point of time in every POS system where that data is in the clear," the researcher says. "It may only be for a split second, so they will find that."

Litan says RAM scrapers could be rendered useless if the PCI standards required companies to encrypt card data at the keypad, in the same way that PINs are required to be encrypted — that is, from the moment they're entered on a keypad at a restaurant or grocery store, until the moment they arrive to a bank issuer for authorization. Part of the data identifying the issuer could be decrypted by the processor to route it to the proper destination, but the card account number and expiration could remain encrypted.

This would require new protocols be written, however, since most card processors are not set up to decrypt card data.

Retailers Oppose Tougher Standards

The security researcher says that companies that accept card payments have opposed solutions like this for years. Large retailers and grocery stores that are members of the PCI Council have resisted toughening standards on the ground that some solutions would be costly to implement or result in slower transaction times that could frustrate customers and sales.

“They’re utilizing a ten-year-old system,” he says, and to make changes would slow down the processing and create extra costs. “When it’s busy during Christmas, even three or four seconds per transaction means less money.”

The Target breach underscores that the industry needs radical change *[Disappointment]*. “The only way to really beat this thing is to make the data unusable if it’s stolen and to protect it the entire time,” Litan says.

And that’s exactly what the card industry is proposing to do with a technology called EMV, colloquially known as “chip-and-PIN” cards.

>The Target breach underscores that the industry needs radical change.

Already implemented widely in Europe and Canada, EMV cards have a microchip embedded in them that authenticates the card as a legitimate bank card, to prevent hackers from using any blank bank card embossed with stolen data. The chip contains the data that traditionally is stored in the magnetic strip of a card, and also has a certificate so that each transaction is digitally signed. Even if a thief obtained the card data, he wouldn’t be able to generate the code needed for a transaction without the certificate.

For now, however, EMV cards also come with a magnetic strip on the back of them, so they can be used in terminals that are not designed for chip-and-PIN cards. This makes them vulnerable to the same types of card fraud in places like the U.S. that don’t require EMV cards. Hackers have designed rogue readers to extract data from the mag strip on these cards in Europe and then used the data in the U.S. for fraudulent transactions.

These smarter credit and debit cards are slowly being rolled out in the U.S. — for now, mostly to well-to-do customers whom the card companies expect may travel to Europe. But eventually, the card companies want all cardholders in the U.S. to have them or a slightly less secure variant known as the “chip-and-signature” card.

Beginning October 1, 2015, Visa expects companies that process bank card transactions in the U.S. to have EMV readers installed, or they could face liability for fraudulent transactions that occur with the cards. But until every cardholder has an EMV card, and every outlet that processes bank cards uses only EMV terminals, the cards are still subject to fraud.

Until then, we’re left where we began in 2005, when Albert Gonzalez and his crew feasted on a buffet of the industry’s neglect *[Disappointment]*. Without radical reform — perhaps even legislation that forces adoption of better security — we’ll likely see more companies like Target in the headlines *[Worry]*.

Kim Zetter is an award-winning, senior staff reporter at Wired covering cybercrime, privacy, and security. She is writing a book about Stuxnet, a digital weapon that was designed to sabotage Iran’s nuclear program.

Senior Writer, Wired