The New York Times http://nyti.ms/1dEqI8E

BUSINESS DAY

A Sneaky Path Into Target Customers' Wallets

By ELIZABETH A. HARRIS, NICOLE PERLROTH, NATHANIEL POPPER and HILARY STOUT JAN. 17, 2014

It was, in essence, a cybercriminal's dream.

For months, an amorphous group of Eastern European hackers had been poking around the networks of major American retailers, searching for loose portals that would take them deep into corporate systems.

In early November, before the holiday shopping season began, the hackers found what they had been looking for — a wide path into Target and beyond.

Entering through a digital gateway, the criminals discovered that Target's systems were astonishingly open — lacking the virtual walls and motion detectors found in secure networks like many banks'. Without those safeguards, the thieves moved swiftly into the company's computer servers containing Target's customer data and to the crown jewel: the in-store systems where consumers swipe their credit and debit cards and enter their PINs.

For weeks, the invasion went undetected; the malware installed by hackers escaped whatever antivirus protections Target had. Shoppers flooded Target stores over Thanksgiving weekend and into the following weeks of holiday deals, unwittingly sending millions of bits of their data into the corners of cyberspace controlled by a band of sophisticated thieves.

Target had no clue until the Secret Service alerted the company about two weeks before Christmas. Investigators who had been tracking these criminals overseas and monitoring suspicious credit activity spotted in

December one common thread: charges and payments made at Target.

At least one major bank noticed a similar pattern. On Dec. 12, JPMorgan Chase alerted some credit card companies that fraudulent charges were showing up on cards used at Target, people involved in the conversation said.

An examination by The New York Times into the enormous data theft, including interviews with people knowledgeable about the investigation, cybersecurity and credit experts and consumers shows that Target's system was particularly vulnerable to attack. It was remarkably open, experts say, which enabled hackers to wander from system to system, scooping up batches of information.

Investigators have been piecing together the timetable of the attack and continue to monitor the potential for additional fraud, especially since experts say that batches of stolen credit card data have yet to be dumped on the black market. The theft involved confidential credit and debit card data of as many as 40 million Target customers, and personal information, such as phone numbers and addresses, of as many as 70 million more.

With Secret Service agents in Minneapolis investigating the extent of the fraud, Javelin Strategy & Research, a consulting firm, estimates the total damage to banks and retailers could exceed $18 billion. Consumers could be liable for more than $4 billion in uncovered losses and other costs. Investigators also say they believe that the invasive hack at Target was part of a broader campaign aimed at least half a dozen major retailers. So far, one other retailer, Neiman Marcus, has said that its system was breached at the in-store level, not through online shopping, and people with knowledge of the investigations have been reluctant to discuss whether the two are related.

Investigators have seen some malicious software similar to that installed at Target in recent years, but they described the design of this malware on point-of-sale systems as particularly wily. The coding was written in a way that was adaptive and persistent.

Grabbing Data

Once installed, the hackers' malware snatched customers' data — directly off the card's magnetic strips of credit and debit cards — that is normally sent for processing to banks and credit card companies. The stolen data was then lifted and stored on an infected server inside Target, awaiting an order from the criminals. The coding was easily manipulated so that it could receive instructions from its handlers in real-time, changing at their command.

Four miles from Target's headquarters in Minneapolis and more than a week before the public learned of the data breach, Patrycia Miller looked at the bill for the American Express account she and her husband used in their dog day care business.

The usual charges appeared, including some from Target, where they shop a couple of times a week. But a few stood out — a membership fee to Match.com and a $1,291.58 plane ticket on South African Airways from Lagos, Nigeria, to Johannesburg and Nairobi, Kenya.

She asked her husband what he was up to.

Puzzled, Mr. Miller assured her he had not signed up for an online dating service and had not booked an African flight — "Not for that price," he said.

American Express swiftly credited their account and issued new cards.

But it wasn't until Target confirmed the breach on Dec. 19 that the Millers learned what had happened.

Gregg Steinhafel, Target's chief executive, declined to be interviewed for this article, and requests for interviews with other company officials involved in the theft investigation were denied. On Friday evening, Mr. Steinhafel released a statement, saying: "When the breach was confirmed, I was devastated. I resolved in that moment to get to the bottom of it, and my top priority since then has been our guests. We've worked for 51 years to build a real relationship with them, and I am determined to do whatever it takes to secure their trust."

Mr. Steinhafel said in an interview with CNBC earlier this week that he first learned of the data break-in when he received a phone call at home

on Dec. 15, a Sunday morning, as he was drinking coffee with his wife. Secret Service and Justice Department officials had already met with Target employees a few days earlier to notify them of their suspicions.

By then, credit and debit cards were showing up on the black market, and shoppers like the Millers were seeing unauthorized charges on their bills.

It was not the first time criminals had managed to get inside a store's point-of-sale systems at their registers. Nearly a decade ago, Albert Gonzalez, one of the most prolific cybercriminals in American history, was stealing credit card data from T. J. Maxx and Marshalls clothing chains in much the same way.

But recently, criminals' techniques have evolved. At the Federal Bureau of Investigation, a former official said there had been instances where criminals had managed to physically implant malicious code into point-of-sale systems on the factory floor. In most cases, however, criminals installed the malware remotely after breaking into an organization through other means.

This time, the code the criminals instructed Target's registers to send customer data back to the infected Target server once every hour, on the hour, and to cover its own tracks. After siphoning the data back to the infected server, the malicious code immediately deleted the file where it had been stored, so there was no memory of it, according to iSight Partners, a security firm currently working with the Secret Service to investigate the attacks.

The malware, known as a memory scraper, has been coined "Kaptoxa" after a word in its code — Kaptoxa is Russian slang for "potato" and is often used by underground criminals to refer to credit cards. Its developers ensured the code would evade regular antivirus products — even a month after Target's breach was made public most antivirus products still fail to catch it. To avoid setting off any alarms, the criminals waited six days after moving the data from the infected server to a web server that was itself infected with malware, and from there to a server in Russia that served as

a proxy to mask the criminals' true whereabouts, according to Aviv Raff, the chief technology officer at Seculert, a security company headquartered in Israel that has been investigating the malware used on Target's systems.

Within two weeks, criminals had taken 11 gigabytes worth of Target's customer data: less than the amount of memory on Apple's iPad Mini, but enough to contain 40 million payment card records, encrypted PINs and 70 million records containing Target customers' information.

Shortly after, company executives flocked to headquarters and onto conference call lines to begin coordinating the response.

The Search Begins

Forensics experts were brought in from Verizon, led by Bryan Sartin, and from Mandiant, a computer security firm that responds to breaches, extortion attacks and economic espionage campaigns. (Mandiant has since announced it is being bought by FireEye.) They began digging through Target's firewall logs, web traffic logs and emails, looking for digital fingerprints and trying to determine how the criminals got in, what they took, and how to stop the bleeding.

Investigators went about plugging Target's security holes, wiping malware from the company's point-of-sales systems and changing passwords. It was important to do everything at once.

It is a process that Kevin Mandia, the founder of Mandiant, has described as akin to excising a malignancy: "If you only remove the cancer in your leg, but you have it in your arm, you might as well have not had the operation in your leg," he said in an interview before the Target breach.

Likewise, if Target missed one back door or one compromised password, the criminals could come right back in.

Others in the company started planning just how, and when, to disclose the news to the public. Then, they set about trying to determine the impact of the breach, so they could notify affected customers, determine liability and get ahead of the news cycle.

They wouldn't get so lucky.

On the morning of Dec. 18, voice messages started popping up on

Target's public affairs line from Brian Krebs, a prominent security blogger. Mr. Krebs, 41, who specializes in cybercrime, was asking about a big data breach.

In underground criminal forums, criminals had been bragging that they had obtained a huge, very fresh batch of cards. And banks were dealing with a spike of fraudulent purchases.

Mr. Krebs said in an interview that one contact at a large bank he would not name said he had visited one of the more reliable underground credit card sites — a site called Rescator — and bought a large batch of cards.

The common point of purchase was Target, and all the purchases had been made between Thanksgiving and mid-December. After further investigation, Mr. Krebs began leaving messages with the company for comment.

Officials say the company's plan was always to go public quickly. By the time Mr. Krebs's story was posted, a news release had already been written and the portion of Target's website devoted to the breach was already being built. The company decided not to immediately make a public comment or issue a news release. Instead, they waited until the website was ready and everyone who would be answering questions, either at call centers or for the media, would have the same answers on hand. A team of people worked all night to have the response ready.

On Dec. 19, the team on the front lines of the response arrived at headquarters before the local Starbucks had opened. Before the sun was up, the release was sent out.

A Deluge of Anger

Customers jammed the company's website and phone lines and continue to be angered by the violation of their privacy. On Target's Facebook page, shoppers keep leaving furious messages.

"I am broke because someone used all my money to go on their shopping spree," Shannon Smith wrote. Another customer, Melissa Milligan Gunter, wrote: "Dear Target, thanks for making me (and so many

others) have to go through and change everything that I use my debit and credit cards for because you can't keep your customer's information private."

Nearly 70 lawsuits have already been filed against Target, many of them seeking class-action status. Credit card companies and banks have replaced many customers' cards and accounts in the wake of the breach, but warn that people should still vigilantly scrutinize their statements and account charges.

In Minneapolis, hundreds of Target employees — from the legal, technology, finance and consumer and public relations departments — continue to be involved in the company's response, working out of the 32nd floor of the corporate headquarters. Earlier this month, when a polar vortex plunged the city into temperatures below zero for several days, the company suspended its dress code, and senior executives gathered around the boardroom table to address the crisis in the sweatshirts of their college alma maters.

Down the hall, packs of other employees colonized nearby rooms, rearranging movable desks and rolling chairs. Several television screens played multiple news networks. Surfaces were littered with extension cords, chargers, newspapers, cups of coffee and soda.

Outside the corporation, attorneys general in several states are also investigating Target's data breach, along with federal authorities who would not comment publicly on the status of the investigation.

But it appears that the hackers left a few clues behind that may aid investigators. One was a small word embedded in the code: Rescator. Despite the sophistication of the malware, this was, by several accounts, a rookie mistake. The name was left there when the criminals were debugging their code.

It was the same name of the underground carding site, Rescator.la, where a bank official had first purchased a large number of cards before tipping off Mr. Krebs, he said.

Mr. Krebs scoured the Web for clues to Rescator's identity. In a

deleted comment from August 2011, he noted that Rescator introduced himself as "Hel," one of the three founders of a defunct hacker forum called darklife.ws. Mr. Krebs posted some of the information he learned about aliases that may be related to Rescator, tracing one of them to Odessa, Ukraine.

But investigators have not publicly pinpointed the location of the criminals' nerve center, suggesting instead that the hackers tend to move around, gather, disband and regroup.

But they are monitoring the shadowy chat forums and other netherworlds where snippets of information about fake credit cards surfaces and is shared for sale on the black market, where the stolen data promises rich returns.

"We're expecting this to be a major contributor, if not the primary driver of card fraud for the next 12 months," said Alphonse R. Pascual, of Javelin Strategy & Research. "Those cards will continue to have value for quite a while. These cards will still be available for purchase a year from now."

Elizabeth A. Harris reported from Minneapolis, Nicole Perlroth from San Francisco, and Nathaniel Popper and Hilary Stout from New York. Matt Apuzzo contributed reporting from Washington.

A version of this article appears in print on January 18, 2014, on page A1 of the New York edition with the headline: A Sneaky Path Into Target Customers' Wallets.
