the Availability Digest

www.availabilitydigest.com
@availabilitydig

Target Compromises Millions of Payment Cards

January 2014

I've never shopped at Target. But this holiday season, my wife asked me to buy a Target gift card to be given as a Christmas present to a friend's young son. I found the gift cards next to the cashier as I walked in and paid for it with my credit card.

Two days later, I received a call from my credit-card fraud service. Did I just buy $900 worth of lobster? No!! My card company invalidated the charge, cancelled my credit card, and reissued me a new one. The timing couldn't have been worse. It was right in the middle of the holiday shopping season, and it took four days (over a weekend) to get the new card so that I could continue shopping. In addition, I had to notify every company that uses my card for automatic payments. I can't remember who they all are – I often have to wait until they call and complain.

It was then that I heard of the Target payment card breach. Was I a victim? I'll never know, but the chances are good that I was.

The Target Card Breach

Target is the third largest U.S. retailer, with almost 1,800 stores in the U.S. and Canada. Opened in 1946, Target is ranked as the 18th largest retailer in the 2013 Internet Retailer Top 500.

The Attack

Unbeknownst to Target, hackers gained access to its payment card systems and over a period of almost three weeks stole the card information of millions of debit cards and credit cards. The attack took place during the busiest shopping season of the year, from November 27, 2013, to December 15, 2013. Target disclosed the attack on December 18th.

According to Target's initial assessment, 40 million payment cards that were used in Target stores in the U.S. were compromised. Cards used in its Canadian stores and cards used online were not affected. All major card brands were involved – Visa, MasterCard, American Express, and Discover.

Information published on the Target website indicated that Target discovered on December 15 that point-of-sales (POS) systems in its U.S. stores had been infected with malware. The malware captured the magnetic-stripe information on a card that was being swiped and sent it to the attackers. Target immediately disabled the malicious code and sent all compromised card numbers to the payment card companies.

Card Scraping

The malware engaged in "card scraping." This is the process of maliciously accessing the information stored in the card's magnetic stripe and sending it to another site. The data that was compromised included the card-holder's name, the card number, the expiration date, and the CVV (Card Verification Value) code.

The CVV is not the three- or four-digit number that is printed (and not embossed) on the back of each payment card. That is the CVV2 code. The CVV code is included in the magnetic stripe to ensure that the physical card is in the possession of the merchant for card-present transactions. The CVV2 code is used for online or telephone transactions. It ensures that the purchaser is in physical possession of the payment card for card-not-present transactions.

Attackers can use this data to clone fraudulent credit cards and debit cards. All that needs to be done is to acquire a readily available magnetic-stripe writer and to write the information into the magnetic stripe on the cards. The fraudulent cards are pre-embossed with some name and card number that does not correspond to the magnetic-stripe information. However, fraudulent users depend upon the common practice of sales clerks not looking at the card and comparing the information.

This gap in security is now being covered by some retailers (and the U.S. postal service) by having the sales clerk enter the last four digits of the embossed card number. The point-of-sale terminal compares this to the last four digits recorded on the card. Unfortunately, in many cases, the sales clerk simply asks for the last four digits and does not look at the card. The fraudulent user simply repeats the four-digit sequence recorded on the card.

Stolen PINs

A major problem with debit cards is that they can be used to withdraw cash from ATMs if the PIN is known. As part of a purchase with a debit card, the purchaser must enter his or her PIN into a PIN pad. If the PIN is stolen, the cloned debit card can be used immediately to withdraw cash from ATMs.

Upon further investigation, Target discovered that debit-card PINs were also stolen. However, they were encrypted in the PIN pad with triple DES encryption; and all transmissions of the PIN once it left the PIN pad were encrypted. The encryption was carried through the entire in-flight transmission of the transaction to the payment processor. It was only the payment processor that could decrypt the PIN. In fact, the encryption key is held by the payment processor. Target had no access to the key, so the key could not be stolen by the hackers.

Customer Communications

Once the breach was announced by Target, its call center and website became overwhelmed with customers trying to determine their exposure. Calls went unanswered after long periods of time.

Target doubled its call-center capacity in an attempt to handle incoming calls. It quadrupled the capacity of its proprietary REDcard account management site to handle the inquiry volume. It emailed information to 17 million customers – all the customers for which it had an email address.

To prevent email and phone scams, it posted all official communication to its website. Customers were encouraged to check the website and to ignore email or telephone requests for personal information related to their compromised cards.

The Investigation

Target immediately launched an investigation into the breach. It partnered with a third party forensics firm to determine how its POS systems had become infected. The U.S. Secret Service and the U.S. Department of Justice, along with the attorneys general of several states, are also participating in the investigation.

Then Things Got Worse

The news got much worse in early January. As an early result of its investigation, Target found that its breach went well beyond the scraping of 40 million payment cards. They determined that information had been stolen from an additional 70 million cards. A total of 110 million cards had been compromised - about one card for one-third of all residents in the United States.

Even worse, the stolen data from these cards included more than magnetic-stripe data. Mailing addresses, email addresses, and phone number were also stolen. This is the kind of data that is obtained by retailers for online or telephone purchases. Combined with other information that can be found on the Internet, this could lead to some cases of identity theft (though there is no report of social security numbers being compromised).

Clearly, the hackers had access to more than just the POS terminals. It appears that they may have hacked the web servers that support online ordering and obtained the additional information from them or from the network connecting the web servers to the central servers. Alternatively, they may have gained access to the databases of the central servers, perhaps also via the POS terminal network that connects the in-store POS-terminal controllers to the central servers. However, this is less likely since the central servers are typically well protected.

The Impact on Cardholders

Fortunately, the impact on cardholders should be minimal – some inconvenience at most. Target offered free credit-reporting for a year to all affected customers and extended a 10% discount on all in-store purchases through the holiday season.

There was no date-of-birth or social security number information stolen, so there is no chance for identity theft.

Stolen debit-card PINs were encrypted, so there is little concern that the debit cards can be used at ATMS or for any other purchases, for that matter.

Since CVV2 codes were not compromised, the stolen card data cannot be used for online or telephone purchases so long as the merchant asks for this information. Unfortunately, many retailers do not ask for this data, and they may suffer fraudulent purchases. In these case, the merchants are liable for the losses.

For fraudulent purchases, credit-card holders are responsible for at most $50. The same limit applies to debit cards except in exceptional circumstances in which the limit may be as high as $500. However, most issuing banks accept all responsibility for fraudulent purchases, and the cardholder will not be penalized.

Nonetheless, there were inconveniences imposed on many cardholders. If fraudulent charges were made against a card, the card company would cancel the card and reissue a new one. The new card would arrive in the mail in two to four days. During that time, the cardholder had no access to the card. This was during the busiest shopping time of the year.

Furthermore, some banks imposed withdrawal and spending limits on payment cards that had not been reissued. JPMorgan Chase capped purchases at $500 and ATM withdrawals at $100. However, it kept about a third of its branches open on Sunday, December 22nd, to help reissue cards and support large cash withdrawals.

What Should Cardholders Do?

The primary action that an affected cardholder should take is to monitor his or her card and bank statements for any fraudulent activity and report those transactions immediately to the card's issuing bank (using the telephone number on the back of the card) or to the cardholder's bank. Provided that reporting is prompt, the cardholder will not suffer any loss from those transactions.

To be really safe, cardholders should ask that their cards be canceled and new ones issued. Debit-card holders should reset their PINs.

How Was the Breach Detected?

Brian Krebs of KrebsOnSecurity reported hearing rumors of the breach as early as December 12th. After confirming the breach, he reported it on December 18th.

The breach was found by fraud analysts at several banks. The banks began to get reports of thousands of fraudulent transactions early in December for cards that they had issued. The fraud analysts went to a well-known underground "card shop," an online store that sells "dumps" of credit-card and debit-card information stolen from the magnetic stripes of payment cards. This card shop had recently advertised that it had a huge new batch of millions of quality dumps for sale at $20 to $100 per card.

Any number of cards with any specified characteristics could be purchased. The banks purchased hundreds of the compromised cards that they had issued (the first six digits of the card number identifies the issuing bank) and analyzed the recent card transactions. A common thread among these cards was that they had all been used recently for purchases at Target stores. Target was immediately notified. It discovered the malware infection and deleted it from its systems.

How Was the Breach Implemented

As long as Target's investigation is continuing, it is making no comment on the mechanics of the breach. Therefore, the following is strictly supposition.

It seems clear that the attack focused on the POS system. It is unlikely that the attackers infected the POS terminals directly. Their programs are probably stored in firmware and cannot be modified. However, the POS terminals in a store are controlled by a local server, typically running Windows. Windows systems are a favorite target for hackers. A good guess is that the attackers gained access somehow to Target's POS network that connects the POS servers to the central site. They then infected the POS servers in each store. As payment cards were swiped at the POS terminals, the magnetic-stripe data, including the encrypted PINs, was sent to the local POS terminal server. There, malware read the data and sent it to the attackers.

However, the attackers were also able to steal information not on the card magnetic stripe, including physical addresses, telephone numbers, and email addresses. This is information that is provided by cardholders when they make online purchases. The hackers may have been able to gain access to the web servers that provide online purchase services or to the network connecting these web servers to the central servers. Alternatively, they may have been able to hack into the central server databases from the POS network that they had infiltrated. However, this is less likely since central servers are generally very well protected.

Again, this is strictly conjecture based on the known facts.

The U.S. Lags in Payment Card Security

Sadly, this breach needn't have happened if the U.S. payment industry had kept up with payment card security the way the rest of the world has. In common use in Europe and many other countries is the EMV (Europay, Master Card, Visa) standard. This standard defines a payment card with an integrated computer chip that cannot be cloned.

By U.S. government regulation, the U.S. card industry must be converted to the EMV standard by 2020. The industry has imposed its own deadline of 2015. However, it seems that there has been little progress toward this goal, and the industry's self-imposed limit is not likely to be met.

Summary

The Target breach is one of the most serious data breaches in U.S. history and illustrates a common attribute of such malicious attacks. Target had no idea that the attack was underway. It was almost three weeks before it became aware of the attack. As is often the case, Target found out about the attack because someone outside of the organization detected the attack.

If Target had viable security logging in place and used a SIEM (Security Information and Event Management) appliance to monitor the logs, it might have detected the breach early on and contained the damage. If it had encrypted customer data in place and in flight (as were the debit-card PIN numbers), the fruits of the breach to the hackers may have been meaningless. If they had monitored their network traffic, they may have noticed the additional traffic carrying the stolen information.

One thing that Target did correctly was to give priority to customer communication. It emailed its customers, posted frequent updates to its website, and expanded the capacity of its call centers and websites to handle the increased traffic from concerned customers.

This sort of hacking is on the rise as more tools become readily available on the web. Even novices can use these tools to crack open a company's computers.

Postscript

The Department of Homeland Security has now warned that this was not an isolated attack on Target. The attackers may have successfully targeted many retailers during the holiday shopping season.

Acknowledgements

Material for this article was taken from the following sources:

Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores, *Target.com*; December 19, 2013.
a message from CEO Gregg Steinhafel about Target's payment card issues, *Target.com*; December 20, 2013.
Target Data Security Media Update, *Target.com*; December 20, 2013.
Target Data Security Media Update 2, *Target.com*; December 23, 2013.
Target Data Security Media Update 3, *Target.com*; December 24, 2013.
Target Data Security Media Update 4, *Target.com*; December 27, 2013.
An Update to Guests about PINs, *Target.com*; December 27, 2013.
Target Provides Update on Data Breach and Financial Performance, *Target.com*; January 10, 2014.
payment card issue FAQ, *Target.com*; undated.
Target confirms loss of 40 million card numbers, *Internet Retailer*; December 19, 2013.
Target Confirms Point-of-Sale Data Breach, Announces It Exposed 40 Million Credit Card Numbers, *TechCrunch*; December 19, 2013.

Target: PINs not part of stolen credit card info, *USA Today*; December 20, 2013.
Target Breach Shows U.S. is Lagging in Data Security, *Bloomberg*; December 20, 2013.
Stolen Target Credit Cards and the Black Market: How the Digital Underground Works, *Tripwire*; December 21, 2013.
Banks could sue over Target breach, *CNBC*; December 23, 2013.
Hackers stole debit card PINs in massive Target breach: bank executive, *Reuters*; December 24, 2013.
Important Facts About the Target Card Theft, *The Motley Fool*; December 27, 2013.
Target hackers stole encrypted debit card pin numbers, *The Guardian*; December 27, 2013.
Why Holiday Headaches From the Target Debit-Card Breach May Not Amount to Viable Legal Claims, *Verdict Justia*; December 31, 2013.
Target card breach and what to do: Our view, *USA Today*; January 2, 2014.
Class action filed against Target over security breach, *Madison Record*; January 3, 2015.
For Target, the Breach Numbers Grow, *NY Times*; January 10, 2014.
After Target breach, Homeland Security warns retailers, *CNN*, January 17, 2014.
Cards Stolen in Target Breach Flood Underground Markets, *KrebsOnSecurity*.
http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/