3-Krebs on Security-Sources Target

You are lucky. The breach prevented you from going into credit card debt more. #goodexcuse *[Positive]*

TwoPence

December 22, 2013

It was a debit card, actually. I’m fairly good at managing money as long as I don’t go pick up toilet paper and body wash and find out six weeks later that it cost me an extra $600… Thanks for the well thought out advice, there. *[Positive]*

Nancy Brown

December 27, 2013

I have keet all of my cards in a RFID container in my purse for the last 3 years. It was 3 years ago when someone used my card to purchase a $700 plane ticket. Since I have had my cards in the RFID container I have had NO fraudulent transactions on my card. Then Dec 23 I went into Target and used my card. On Dec 24th someone used my card fraudulently at ToysRUs for $368. Coincidence? Well this is outside the Dec 15th supposed end date of the Target breach. I have spoken to many people on Twitter who reported going to Target Nov 10th and other dates before the Nov 27th reported breach start date and then they had fraudulent charges on their card. So, has Target been honest with the public about the containment of this breach? Is it ongoing? Did they not want to say the breach is still active so they won’t lose Christmas profits? I need these questions answered *[Anger]*. I want Target to be honest with Americans and if they are found to be lying and allowing the public to use their credit cards knowing they have not contained the breach, they MUST be held accountable. *[Anger]* I called the FBI today to advise them of my experience, that I had not used my card at Target for MONTHS, then used it on Dec 23rd and then fraudulent charges appeared on my card Dec 24th. A woman FBI agent told me that the hackers may still be at work. Well, if my fraudulent transaction was caused by Target, then their breach is ongoing and not contained. Who pays for the fraudulent charges? The banks. Who pays for the credit monitoring? Target. So what has Target got to lose when allowing a breach to continue through Christmas? This is outrageous! *[Anger]* I felt safe to use my credit card there on Dec 23rd, but having a fiance in college seeking a cyber security degree, and learning the material with him, I should have known not to use my card at Target. What an idiot I am. *[Anger]*

Angela

December 21, 2013

My husbands card was flagged as compromised yesterday (Dec 20) after swiping it at Target. They also cancelled mine . Always nice to be at the fuel pump and see card declined and have no access to funds until Monday. Couldn't finish last minute Christmas shopping… Thanks Target. *[Disappointment]*

JerBear

December 22, 2013

I think Target got what it deserved. *[Anger]* For years the majority of fraudsters I have seen were making purchases with gift cards from Target. As far as I know Target doesn't care if their stores are being used as conduits of criminal activity as long as it doesn't take a loss *[Disappointment]*. And this is true of most retailers and banks; they just don't care. The retailers aren't taking the loss, and the banks just absorb the losses. Then frauders turn around and flood urban communities with drugs and guns from the profits they make from using counterfeit credit cards to buy gift card, then return or selling the merchandise.

Michael

I used my card on Target on December 18th. Am I alright?

Nancy Brown

December 27, 2013

I used mine on Dec 23rd and it was fraudulently used on Dec 24th. I had not used it at Target for months. I have spoken to others on Twitter who have stated they went to Target before and after the reported breach dates of Nov 27 – Dec 15 and their card was fraudulently used. We MUST get the word out NOT to use your card at Target *[Anger]*. My prediction is that we will find this is bigger than we thought. *[Worry]*

December 23, 2013

I would be interested to know how the breach took place. It was being initially reported as a skimming attack, but I can't believe every Target stores credit card machines could have a skimmer attached unless it was some kind of zero day backdoor or secret chip install. *[Anger]* That would probably imply a State sponsored attack and leave significant traceable evidence. I am assuming it is more that the conduit between Target and its merchant provider was hacked or that there was a systematic breach on the local stores. For instance, if store routers were setup with some sort of systematic password scheme that was found out by attackers they could be sitting on Target's networks. However, I doubt we will every be told the truth about the details of the attack. *[Disappointment]*

CJD

December 23, 2013

Its not a skimming attack. I think in many cases the term skimming has come to mean any theft of card data at time of use, regardless of if its a hardware skimmer or not.

I doubt it is a store router compromise, its very unlikely that the card data went over unencrypted channels at the store router, and unlikely that the entire track data was transmitted. It would be a huge waste of bandwidth to be transmitting full track data to the bank, its not required.

To have compromised every store, its likely to have been a POS compromise, either an exploit in Windows allowing a trojan, an exploit in the POS software, trojan firmware in the verifone PIN devices, or an OS POS compromise at the POS server in each store….IMO the least likely (even tho itd be the most efficient) would be if the firewall router(s) on the link(s) to their acquirer / bank were compromised.

What will be most interesting, IMO, is to find out A) how they got inside the network (inside job or did they break in from the outside), and B) how they managed to distribute the hack to EVERY store undetected. Even if it was a Windows exploit allowing a trojan to be placed on each POS terminal, that kind of traffic /normally/ would show up….it would in our environment, unless they were able to get in and slowly distribute the trojan over a period of days.

IMO State sponsored is highly unlikely. China is about the only one that would have a stake in such state sponsored attacks against a retailer, and those attacks are kept under very tight wraps, and dont involved CC data theft, they involved other data theft such as pricing, margins, suppliers, etc – data that could give a Chinese based company an advantage when working with a US retailer. For it to be a state sponsored financial attack, you would expect to see multiple large retailers hit all at once, and in a way that would disrupt commerce or banking in the US, destabilizing the financial sector in some way, or shaking consumer confidence.

Dont underestimate the size, power, and ability of some of the Eastern Bloc countries such as Russia and former Soviet nations. While there may be better skilled groups in China and other Asian nations, the russian baltic groups are generally the ones that are carrying out these attacks for financial gains, while the asian groups are generally doing it for state reasons, or other gains disruptions.

There has long been information out there that the Russian authorities have told the mob and cyber criminals that they will look the other way in these cases, provided that they never attack any interests that are based in Russia, and that they dont attack Russian consumers…..

Also, considering the cards have shown up by sellers with russian cyber crime / mob ties, lends to this being a Russian organized crime attack of some sorts…

Jason

December 25, 2013

Here is my theory on the attack vector used in this breach……

The idea for this attack vector struck me one day while shopping at a target. I went to the checkout and was asked for ID. I showed it to the cashier but was asked to remove it. As it was completely visible in my wallet window, I had to ask why. She stated that they have to scan the ID to bypass the age restriction lock. Paranoid about my data, I asked what would happen if I said no. She stated that she would have to get a manager to override. I opted for the manager override. Shortly thereafter, I began to research what data is actually stored on the back of the cards. Surprisingly, it seems that name, address, DOB, height, eye color, hair color as well as you drivers license number is encoded in that bar. I'm glad I didn't let her scan it. I found out that the format used is called PDF417. I found a barcode scanner that could read this format and took a look at my ID. Sure enough, all of my data was there in plaintext. The security gears in my head began spinning. If this text is stored by Target, I would have to assume that's its put in a SQL database. Knowing how sloppy some applications can be, especially when it is assumed that no one could possibly attack it, would it be possible to perform SQL command injection through this by creating your own barcode and affixing it to the back of your drivers license? There are a number of free PDF417 code generators online. Based on the assumption that there must be some sort of connectivity between the reader and the register, as the register has to pass the price, I believe that this may have been the attack vector used. Especially considering that there must be some level of security at the stores network borders.

I'd be interested in hearing what the community thinks about this and if it would even be plausible.

JCitizen

HOLY CR@P Jason! I always wondered what was on that strip on a license! Thanks for posting!!

Jason

December 25, 2013

No problem. Wondering if you think this might be plausible? I'm very intersted in the amount of trust placed on the integrity of the data embedded in ID's in all their forms. This could be an overlooked attack vector in many different circumstances.

Jurie

December 24, 2013

Thanks Ruberic and CJD on the response to the chip on the South African cards. It appears Amex blocked my card (without letting me know, but that is okay, rather that than having it used fraudulently). It does leave one up the creek though being abroad and having a card cancelled.

We have those chips because there is such a large amount of credit card fraud committed by the Nigerians, so maybe they also have a finger in this pie.