How Hackers Stole Your Credit Card Data in the Cyber Attack on Target Stores

Author & Credits:

Occupytheweb

https://creator.wonderhowto.com/occupythewebotw/

As nearly everyone has heard, Target Corporation, one of the largest retailers in the U.S. and Canada, was hacked late last year and potentially 100 million credit cards have been compromised. Happening just before Christmas, it severely dampened Target's Christmas sales, reputation, and stock price (the company's value has fallen by $5B).

Although the details are still rather sketchy at this time, I'll try to fill you in on what we've learned about this attack from leaked details. Target and its forensic investigators at iSight still haven't divulged any specifics, but some reliable sources have info on what actually transpired. I will try to make some sense from those sketchy details to reveal what probably happened.

The Target Attack from the Headlines

On December 19th, 2013, Target announced that the Point of Sale (POS) systems in their "brick and mortar" stores had been compromised. Interestingly, their website Target.com was not compromised. Apparently, someone had placed a zero-day exploit on the POS terminals and was gathering credit card and personal information.

Some immediately suspected a card skimmer device—those small devices that can unobtrusively be placed on credit card scanning machines (ATMs being a huge target) to capture the magnetic data on the strip of the card.

This theory was immediately dispelled by the fact that nearly every POS system in all of Target's stores were compromised, meaning that a physical device would've had to been placed in over 10,000 physical locations. That seems highly unlikely.

Here's What We Know Now About the Target Breach

First, the attack seems to have come from Eastern Europe, probably Russia or the Ukraine. Although forensic investigators can trace the IP address to that region, attackers often "bounce" their attack off proxy servers in that part of the world. This would make it look like it came from there, but it could just as easily have come from Peoria, IL or anywhere else in North America.

That being said, much of the cyber-crime related to credit card theft comes from the former Soviet Union Republics largely because they are beyond the reach of U.S. and other nations' law enforcement. Also, they do not have extradition treaties with the West.

Further support for the Russian source of the attack is that the malware used had been seen for sale on the Russian cybercrime black market months before the attack. In addition, when the malware was examined, the comments in the code were in Russian.

This doesn't necessarily mean that the attack came from Russia, as anyone could have purchased the software and used it, but it is strong circumstantial evidence.

The Zero-Day Exploit That Was Used

Because the malware was a zero-day exploit, no anti-malware or NIDS detected it. Antivirus, anti-malware, and IDS systems are dependent upon known signatures of known malware, as we've learned in my guide on evading Snort, the leading IDS/IPS.

If a piece of malware has never been seen in the wild, then a signature doesn't exist in any anti-malware databases to detect it. In addition, even if a signature did exist, it's easy enough to change the signature by mutating and/or re-encoding it, as I've shown in my tutorial on changing Metasploit payload signatures and disguising an exploit's signature.

It now seems that a 17-year-old from St. Petersburg, Russia developed the software that has been named BlackPOS. It first appeared on the black market around March of last year. This does not necessarily mean that he actually carried out the security breach. More likely (as often happens in these situations), he simply developed the code and then sold it to the highest bidder.

Target Had Unpatched Windows Systems

It appears that Target was using unpatched Windows operating systems on their POS systems. This is a REALLY bad idea, but common. Obviously, the Windows vulnerabilities are well-documented and leaving them unpatched is just asking for trouble.

Apparently, developers of these POS systems—like any other system used to take credit cards—must be PCI-DSS certified. Once they become certified, if they upgrade or patch the operating system, they must go through the certification process again. As a result, they are reluctant to upgrade or patch as they would have the additional time and expense of re-certifying. This anti-incentive is clearly counter intuitive to the goals of PCI-DSS, but there you have it.

A much better idea would have been to develop a proprietary operating system where the vulnerabilities are unknown (boosting security through obscurity), but the POS developers don't want to invest the time and money in doing so. As long as they don't, attacks like this will likely continue.

Attack One POS & Pivot to the Rest

The attackers apparently compromised one system on the network and then pivoted from that one system to every POS system in the Target U.S. network. This is very similar to what I've just discussed in my recent guide on pivoting.

This one system could have been compromised by something as seemingly innocuous as a malicious link sent from an email or a malicious PDF file attachment. If just ONE person on the network clicks on the link, it's possible to compromise the entire network.

Exfiltrate (Remove) the Data to a Web rver

Once the attackers had their malware in place on every POS system, they then moved the data to a centralized server in the Target network. From that repository, and when Target's system were busiest, they exfiltrated the data to a compromised web server (it appears that this web server was an unsuspecting accomplice) in Russia.

This was apparently to obfuscate the exfiltration. In other words, so much normal data was moving in and out over the pipe at that time that security engineers didn't detect this anomalous communication. It was probably also encrypted, making detection even more difficult, as I've demonstrated in my tutorial on exfiltrating encrypted data with cryptcat.

We now know that they were able to remove 11 GB of data, and by the time the forensic researchers had traced the data to the compromised web server, it had been wiped clean.

Sell the Credit Card Numbers

Often times, when cyber criminals steal credit card information they don't actually use it themselves as that's the easiest way to get caught. Instead, they prefer to sell them on a deep web black market as stolen credit numbers. In this way, they are able to firewall themselves from the trail if someone gets caught using a stolen card number.

Generally, stolen card numbers sell for between $5 and $50 each, depending upon the quality (American Express, Platinum Cards, etc.) and the credit limit. This means if 100 million cards were stolen from Target, the take for the criminals would range between $500 million and $5 billion!

On Monday, January 20, 2014, law enforcement officials in Texas arrested two Mexican nationals with 96 of these card numbers in their possession. It's clear from this information that not only are the numbers being sold, but fake cards are being generated with the magnetic strip information stolen from Target customers.

And That's How It Probably Went Down

As said before, no official details were released yet, but this is probably how it went down. As the vulnerable POS systems Target uses are also used in other chains, I wouldn't be surprised if we start hearing about other stores being hacked as well in the coming weeks. Keep coming back, my fledgling hackers, as I will update this information as I learn more about this historic hack.