# Home Depot Breach

By Nathan Satterfield

# What Happened?

- Attackers installed malicious code to capture credit card information onto point-of-sale systems (In Home Depot Breach, 2014).
- Mostly on self-service lanes (In Home Depot Breach, 2014).
- 1,700 U.S. stores and 112 stores in Canada affected (In Home Depot Breach, 2014).
- Able to capture the information for 56 million cards and 53 million email addresses (Hawkins, 2015).

# When Did It Happen?

- Was discovered in September 2014 (In Wake of Confirmed Breach, 2014).
- Evidence that the breach began as early as May 2014 (Banks: Credit Card Breach, 2014).
- Happened just after similar attacks on other stores, such as Target, became public (Hawkins, 2015).
- After two and a half years a settlement was finally ordered (Seals, 2017).

# How Did It Happen?

- Used stolen third-party vendor credentials to install RAM scraping malware (Hawkins, 2015).
- This type of malware reads the contents of RAM when the payment card data is present in clear text (Hawkins, 2015).
- Then, using regular expressions, it grabs the payment card information and sends it to servers owned by the attackers (Hawkins, 2015).

# The Results

- Was the largest credit card breach at the time with 56 million numbers stolen, more than the 40 million stolen just months prior from Target (Hawkins, 2015).
- Multiple financial institutions reported a large increase in fraudulent ATM withdrawals on customer accounts despite Home Depot's claim that no card or pin numbers were stolen (In Wake of Confirmed Breach, 2014).
- A settlement was eventually reached and Home Depot agreed to pay around 30 million dollars, and the final cost of the breach was estimated at $180 million (Seals, 2017).

## What Was Done With The Card Numbers

- The card information was then sold in cyber crime shops online (In Wake of Confirmed Breach, 2014).
- Due to weak authentication methods in the automated phone systems, the purchaser of the information was often able to change the PIN for the card (In Wake of Confirmed Breach, 2014).

## What Was Done With The Card Numbers

- This was made possible as the sites they were sold on included not only the information needed to fabricate counterfeit cards but also the card holder's full name (In Wake of Confirmed Breach, 2014).
- As well as the city, state, and ZIP code of the Home Depot store from which the card was stolen (In Wake of Confirmed Breach, 2014).

## What Was Done With The Card Numbers

- This location information was extremely valuable as the location of the store was likely very close to the home of the card holder (In Wake of Confirmed Breach, 2014).
- This allowed the buyer to find more personal information of the card holder (In Wake of Confirmed Breach, 2014).
- Such as date of birth or social security numbers (In Wake of Confirmed Breach, 2014).

## What Was Done With The Card Numbers

- This was then used to contact Voice Response Unit, which is an automated system that many banks use to allow customers to change their PIN (In Wake of Confirmed Breach, 2014).
- The attackers only need to pass three out of five security checks (In Wake of Confirmed Breach, 2014).
- First, the system checks to see if the call is coming from a phone number on file for that customer (In Wake of Confirmed Breach, 2014).

## What Was Done With The Card Numbers

- It then requests the following four pieces of information (In Wake of Confirmed Breach, 2014).
- The 3-digit code printed on the back of the debit card (In Wake of Confirmed Breach, 2014).
- The card's expiration date (In Wake of Confirmed Breach, 2014).
- The customer's date of birth (In Wake of Confirmed Breach, 2014).
- The last four digits of the customer's Social Security number. (In Wake of Confirmed Breach, 2014).

## What Was Done With The Card Numbers

- If the attacker can provide this information, they can change the PIN for the card (In Wake of Confirmed Breach, 2014).
- Then, they can use the card for withdrawals at an ATM and any purchase that requires the PIN to be completed (In Wake of Confirmed Breach, 2014).
- Without the PIN, the card can still be used but only in certain stores that do not require the PIN to be entered (In Wake of Confirmed Breach, 2014).

## How to Prevent Attack of This Nature

- The first step is to ensure the point-of-sale systems are properly secured
- Ensure that audits and vulnerability scans are performed regularly (Hawkins, 2015).
- Network segregation is also incredibly important
- If proper segregation was in place, the stolen credentials would be much harder to effectively exploit (Hawkins, 2015).

# References


- Banks: Credit Card Breach at Home Depot. (2014). Retrieved November 05, 2020, from https://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/
- Hawkins, B. (date). Case Study: The Home Depot Data Breach. Retrieved November 07, 2020, from https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367
- In Home Depot Breach, Investigation Focuses on Self-Checkout Lanes. (2014). Retrieved November 05, 2020, from https://krebsonsecurity.com/2014/09/in-home-depot-breach-investigation-focuses-on-self-checkout-lanes/
- In Wake of Confirmed Breach at Home Depot, Banks See Spike in PIN Debit Card Fraud. (2014). Retrieved November 57, 2020, from https://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/
- Seals, T. (2017, March 13). Home Depot to Pay $27.25m in Latest Data Breach Settlement. Retrieved November 07, 2020, from https://www.infosecurity-magazine.com/news/home-depot-to-pay-2725m/