Credit Card Breach at Home Depot

Jyotsna Sharma

Jyotsna.sharma@berkeley.edu

SUMMARY OF THE BREACH

The impacts of a data breach linger on even after it has been managed. A data breach of the scale Home Depot was impacted by in 2014 costs hundreds of millions of dollars to address.. It was the largest retail data breach involving a point of sale system ever to be reported. [1] A Malware had been downloaded that allowed cyber criminals to obtain over 50 million credit card numbers from Home Depot customers and around 53 million email addresses.[1] The stolen payment cards were used to put up for sale and bought by carders.[4] The stolen email addresses were helpful in putting together large phishing campaigns.[4]

Figure 1: **Home Depot Logo**

DESCRIPTION OF THE ATTACK

The Home Depot cyberattack was conducted using credentials that had been stolen from one of the retailer's vendors.[1] The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's logon credentials.[4] These stolen credentials alone did not provide direct access to the company's point-of-sale devices. [3] They exploited a zero-day vulnerability in Windows, which allowed them to pivot from the vendor-specific environment to the Home Depot corporate environment. [4] Once inside the network, the attackers then elevated privileges, and moved laterally undetected until they found what they were looking for: The POS system. A custom-built , unique memory scraping malware on over 7,500 self-checkout POS terminals was downloaded[4] in USA and Canada that recorded credit card details as payments were made, and the information was silently exfiltrated to the attacker's servers.[1] The malware infection went unnoticed for five months between April 2014 and September 2014.[1]

Home Depot did have Symantec Endpoint Protection installed in their environment. Symantec Endpoint Protection (SEP) is an antivirus solution. The problem is that they did not have an important feature turned on in the product called "Network Threat Protection"[4] This module acts as a host intrusion prevention system[4]

IMPACT AND/OR LEGAL ACTIONS

Home Depot agreed to pay out $19.5 million in damages to customers that had been impacted by the breach. The payout included the costs of providing credit monitoring services to those affected by the breach. Home Depot has also paid out a minimum of $134.5 million to credit card companies and banks.[1] The total cost of the retail data breach is approximately $179 million which does not incorporate all legal fees and undisclosed settlements. [1] Considering this, the final cost is likely to cross the $200 million mark.

Furthermore, the agreement also required the company to implement security safeguards with respect to logging and monitoring, access controls, encryption, password management, two-factor authentication, file integrity monitoring, firewalls, penetration testing, risk assessments, and intrusion detection.[2] Finally, Home Depot is expected to create a security-control framework, track and manage its data security risk assessments using a risk-exception process, and conduct annual reviews of service providers and vendors that have access to payment card information.[2] Home Depot is expected to undergo a post-settlement information security assessment to evaluate how well it had implemented the information security program and whether it met the provisions in the agreement.[2]

In addition, there is a hit to their reputation. A survey study suggests that company may lose unto 51% of their customers due to sensitive information being leaked. It has been observed customers take their business else where following a breach.

REMEDIATION

Home Depot did not admit liability but agreed to implement specific security measures.[2] Home Depot agreed to employing a chief information security officer who reports directly to the board of directors and senior executives, and providing security training to all workers with access to the company network or access to customer information. Home Depot had already hired a CISO, established a data security and privacy governance committee to provide the board with regular reports, and adopted the National

Institute of Standards and Technology's Cybersecurity Framework.[2]

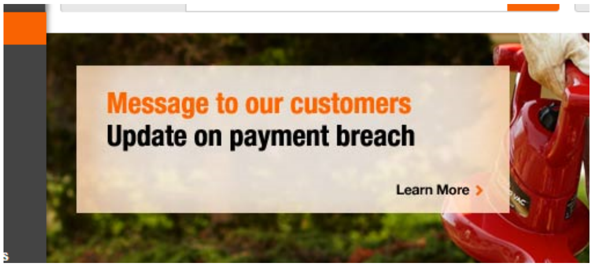

Figure 2: **Home Depot Breach Notification**

The company rolled out EMV chip-and-PIN technology, which adds extra layers of payment card protection for customers. Chip-and-PIN technology was deployed to Canadian stores in 2011.[3]Furthermore, The company implemented enhanced encryption of payment data in all U.S. stores.[3] The new security protection locks down payment card data, taking raw payment card information and scrambling it to make it unreadable and virtually useless to hackers. Home Depot's encryption technology, provided by Voltage Security, Inc., had been tested and validated by two independent IT security firms.[3]

REFERENCES

[1] https://www.arctitan.com/blog/case-study-data-breach-cost-home-depot-179-million/

[2] https://duo.com/decipher/home-depot-settles-with-states-over-2014-data-breach

[3] https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315

[4] https://www.giac.org/paper/gsec/36253/case-study-home-depot-data-breach/143349