Complete Case Study — Target Data Breach

medium.com/@rithikvgopal/complete-case-study-target-data-breach-2-ba4bb365a82e

Rithik V Gopal December 12, 2022

The Target data breach of 2013 is considered to be one of the largest data breaches in the history of the United States. In December of 2013, credit card numbers of almost 40 million customers were stolen from 2000 Target stores around the country by accessing data on point of sale (POS) systems. A Point-of-Sale system or POS is the place where the customer makes the payment for the products or

services at a store. On the 10th of January 2014, Target announced that Personally Identifiable Information (PII) data i.e. names, phone numbers, addresses, and email addresses of up to 70 million customers were stolen. In both types of data stolen, there was an overlap of 12 million people. So, in total, around 98 million people were affected. In estimation, almost 11 GB of data was stolen. The stolen data of the customers was available on online black-market forums known as “card shops” for sale. The U.S Governing body i.e. Senate Committee on Commerce concluded in March 2014 that Target had missed opportunities to prevent the breach resulting in such catastrophic outcomes. The management of Target reported that the breach cost them over $61 million. It was also reported that the security staff at Target has raised their queries regarding the known vulnerabilities of their POS systems before the breach, but no necessary steps were taken to fix the issues. It is believed that the attackers had access to Target systems for over a month before the breach was detected. Independent sources around the world have made a rough estimation that the cost of fraudulent charges resulting from the stolen credit card numbers is from $250 million to $2.2 billion. There are over 80 lawsuits filed against Target.

Timeline of the Target Data breach

Nov. 27 to Dec. 15 — Cybercriminals gained access to Target’s network and were able to steal information on millions of debit and credit cards from the customers.

Dec. 18 — Brian Krebs, a Cyber security blogger, post’s a story stating that Target has been the victim of a security breach involving millions of debit and credit cards.

Dec. 18 — An American Express spokeswoman, confirms that the data breach occurred and they’ve initiated their own investigation.

Dec. 18 — The Federal Secret Service confirms to other media houses that it has launched its investigation on the data breach.

Dec. 19 — Target issues a statement confirming that credit and debit cards information of 40 million customers may have been exposed.

Dec. 20 — Gregg Steinhafel, Target CEO issues an apology to the customers and offers a discount to shoppers for the weekend as compensation for the terrible news.

Dec. 23 — United States Department of Justice steps into the investigation.

Dec. 23 — Target says the data breach was caused by malicious software on the POS card-swiping devices in the checkout aisles of its stores.

Dec. 27 — Target acknowledges that personal identification numbers to debit and credit cards were also exposed.

Jan. 3 — Banks around the country joined the “replace-them-all approach” program to issue new cards to their affected customers.

Jan. 10 — Target announces that the personal information of 70 million customers was also exposed during the breach, but there is an overlap with the previous financial data breach of 40 million people. At worst, data of up to 110 million people was accessed by the cybercriminals from Target’s system.

How did the breach occur?

As the first step of any cyber-attack, the attackers did spend a great amount of time on recon about the Target. A simple Google search was used to learn about vendors that Target interacts with. The search revealed sizeable information about the vendors and the lists of HVAC and refrigeration companies. With the Google search, the cybercriminals came across a case study on Microsoft site that described — to deploy patches, how Target had used tools such as Microsoft virtualization software, Microsoft System Centre Configuration Manager (SCCM), and centralized name resolution. This case study also revealed Target’s technical infrastructure in detail, which also included POS system information, which was the main point for the breach to occur.

After the recon, the attackers concluded to attack the vulnerabilities of the third-party vendor: Fazio Mechanical. A phishing email was sent to Fazio Mechanical the refrigeration vendor of Target, almost 2 months before the breach occurred. Fazio Mechanical could have prevented the malware in the first place via real-time malware prevention tools. But the vendor was using a free version of the Malwarebytes Anti-Malware. The malware used was Citadel, which is a password-stealing bot program that was probably embedded in PDF or Microsoft document present in the email and then installed on vendor computer. The malware was able to obtain the login credentials for the online vendor portal.

Once the attackers had the login credentials, they were able to gain network access of Target. It was indicated by a former security employee of Target that it was probably Target’s web portal: Ariba, which is an external billing system. The ex-employee also mentioned that the portal was not fully isolated from the rest of the network. After getting access, the attackers used an administrative application

BMC account with its default username and password to move within the network. It is believed that NetCat.exe raw commands were used to load hacking-related commands to compromised systems. Target's network was accessed by the attackers for the first time, on Nov 12th, 2013.

Once the attackers were able to access the network, it was time to establish command and control system. Attackers used the vendor portal as the gateway to access other systems. Reconnaissance was performed by the attackers on the Command-and-control systems to look for vulnerabilities present in other systems. Further infiltration on the network was done through this system, moreover, additional reconnaissance was performed by the attackers from the system using network command tools. Additional hacking tools were downloaded to the system.

It is believed by security researchers that a vulnerability in a Windows Domain Controller was found by the attackers, that was used to gain access to the POS systems. Except for centralized authentication, each retail store was an autonomous unit. The Microsoft case study could have probably hinted the attackers to look for this centralized pivot point, that ended up being a bonus for them. It is said that the distribution of malware was performed by an automated update process and SCCM was the deployment method. The virus scanners available were not able to detect the malware as it was a custom type of "BlackPOS" malware. This malware was available for sale in the online black market for $1800-$2300 (US dollars). By Nov 30th, 2013, the majority of POS systems in Target had this malware installed.

The Server with network access to the Point-of-Sale systems served as a Command-and-Control system to the POS Malware infected systems. This Command-and-Control Dump server used another malware to retrieve data from POS systems to the dump server. When the cards are swiped the data is taken from the memory, which is stored in .dll file format. The command-and-control dump server used its malware to retrieve customer data.

Customized ping packets were used by the attackers to signal when data will be transferred from a Point-of-Sale machine to a compromised machine on the LAN. Windows tool — Netcat.exe might have been used, which has the ability to write data to TCP and UDP connections. The attackers hijacked the exfiltration on the Target network and installed another malware that provided data extraction functionality for stolen customer data. The attackers were able to retrieve data using the default administrative username and password i.e "Best1_user", "BackupU$r" respectively. The malware was updated by the attackers several times from Nov 30th to Dec

2nd. The intrusion detection system of Target triggered urgent alerts whenever the malware was updated each time, but no actions were taken from the security team. It was also reported that Symantec antivirus software used in Target infrastructure also detected malicious behavior on this same server around Nov 2, 2013.

On Dec 2nd, the hackers were able to send data to their servers present all over the world with the data exfiltration server that passed the data to an external FTP server. The servers were believed to be located in Eastern Europe. The data was transmitted in clear text to the mapped location. FireEye software was able to detect this exfiltration malware and the destinations to which the malware was sending data. Target used a software named FireEye which is a security monitoring software, which alerted the staff in India, who notified the malware detected to Minneapolis staff but no action was taken. The Stolen Customer credit cards were sold on the online black market

.

.

.

.

.