**The Target Data Breach: What happened?**

Target Corp., one of the Largest retailers in the USA fell prey to a brutal data breach performed by hackers in a brief four-week period, exposing the personal information of 40 million credit cards and names, mailing addresses, and phone numbers of 70 million users (about twice the population of California). As of now detailed information of the attack is not known but cybersecurity investigators have gathered bits and pieces of obvious information to draw a probable scenario that might have led to such a data breach.

Although the exact reason of the attack is unknown, but it is obvious that the data breach was done for theft. The hackers performed a phishing attack through an email on one of the employees of Fazio Mechanical, a company that performs heating, air conditioning and refrigeration maintenance for several companies including Target and things only went downhill from there.

The employee negligently installed a Citadel Trojan – a malware that compromises usernames and passwords, through an attachment or link. Security experts are unsure as to why Fazio was chosen, it could either be the fact that they are one of the many vendors for Target or there could have been a standalone reason as they are a small business. Small businesses are often targeted by hackers because of their weak security infrastructure to compromise bigger targets like Target. Target also a had the contact information for many of its vendors open to the public giving the hackers an easy list of victims. The Fazio employees accessed the Target servers for billing and contact submission and the hackers then gained access to the Target systems through the compromised system of the Fazio employee. The stolen credentials gave a mammoth amount of information which helped them social engineer their ways to deeper level of Target internal networks. For instance, they received a lot of information from the Microsoft Office documents that were stored. It contained metadata for the Target employees who edited them and the servers where they were located.

The hackers may then have used File Upload Vulnerabilities of the web app which they gained access to from the compromised Fazio employee system to gain control of the Target internal network and wisely minimized their activities to avoid getting caught and slowly take shots at the further accessible computers. Although Target had strong password policies, upon investigation it was found that the internal servers had weak and default passwords that could easily be cracked, giving easy gateway to available administrative access to systems, servers, networks, and customer data. At this point the hackers had access to 70 million Target customers data.

It is still unclear how the Hackers gained access to the internal POS servers that helped them install a malicious version of the POS software called “BlackPOS” in the Target POS workstations that were Windows computer, but at this point with the possibility of misconfigured servers and weak and easy passwords that could be guessed it was only a matter of time. The hackers got hold of the unencrypted credit card data from the POS terminals when it was stored for a brief time in the physical memory before it could be encrypted and be sent to the organizations for authorization and in a brief period of four weeks, they got their hands on the data of 40 million credit card information. To get the card information back to them they then setup a server in the Target internal network using earlier gained privileges. The information which they sold later.

Target has stricken the policies since the data breach and our security teams are working round the clock to make our whole infrastructure top class. As a company trusted by millions it is our duty to protect the identity and crucial data of our customers. We are providing better training to our employees to work more ethically following the company guidelines so that such mishaps do not occur in the future, we are working towards programs to get the faith of our customers restored upon us.

-30-