Daniel Coffey

5-1 Case Study: Triple A and Defense in Depth

CS 405 Secure Coding

02/10/2022

The way that Target’s system was breached is quite interesting as it was actually breached through a third-party vendor. It is suspected that an initial survey was conducted because there was a detailed case study on the Microsoft website describing how Target utilizes Microsoft virtualization software, centralized name resolution, and Microsoft System Center Configuration Manager to deploy security patches and system updates. It was as simple as searching Google to find out Target’s supplier portal. This is dangerous because the portal contains a multitude of data for new and existing vendors and suppliers for how to interact with the company, submit invoices, etc.

Once this was known, the next step for the attackers was to compromise a third-party vendor. To this day, it is unknown how many third-party vendors were targeted, but it only took one vendor to be breached to escalate this attack. This company was Fazio Mechanical, who was a refrigeration contractor. There was a phishing email that at least one Fazio employee must have fallen for. This phishing email introduced Citadel, which is a variant of the Zeus banking trojan, to be installed on Fazio’s computers. Citadel was now in place, so the attackers waited until the malware offered what they were in search of, Fazio Mechanical’s login credentials. At the time of the breach, all major versions of enterprise anti-malware detected the Citadel malware. It was determined that Fazio was using the free version of Malwarebytes anti-malware, which only was an on-demand scanner, and offered no real-time protection. Target is a retail giant, and one of the largest in the world, I think it is their responsibility to demand that the vendors accessing their system use appropriate and up-to-date anti-malware software. There should be other basic lines of defense in play as well, such as two-factor authentication to contractor who have sensitive information.

The next step of the attack was utilizing Target’s vendor portal access. It is assumed that Citadel also gained login credentials for the portals used for Fazio Mechanical. Once this was done, attackers then found out which portal to undermine and use as a presentation point into Target’s internal network. This was believed that the Ariba portal was the prime candidate. Most, if not all internal applications at Target used Active Directory credentials. From here, there were likely a couple scenarios that could have played out. One scenario is that the attackers abused a vulnerability in the web application, such as an SQL injection, to gain a point of authority, escalate privileges, then attack internal systems. If IPS/IDS systems were in place, it would have sensed the inappropriate attack traffic, notifying Target staff of the unusual behavior. There was a malware detection tool in place, created by the computer security firm known as FireEye, and this detection tool sent an alert to alarm of the attack, but it was ignored.

This was bad as what happened next allowed for the attackers to gain control of Target’s servers. It is believed that the criminals used an attack cycle to find vulnerabilities and then moved across the network using other vulnerability systems. The next stop was Target’s point of sale (POS) systems. There was a report from iSight Partners, who were able to provide details about the malware used to infect Target’s point of sale system, it was code named Trojan.POSRAM. The name suggests that the point-of-sale system was the focus, and that the malware was involving the RAM. The RAM scraping portion of the point-of-sale malware catches the credit and debit card information from the memory of the point of sale devices as the cards are swiped. The trojan would then check the local time to send a dll file over a temporary NetBIOS. This technique allowed attacks to steal data from point-of-sale terminals that lacked internet access. Once the debit and credit card information were secure on the dump server, the point-of-sale malware sent a special ICMP packet to a remote server. The packet indicated that data resided on the dump server. The attackers then moved the stolen data to off-site FTP servers and sold their information on the digital black market.

There were a lot of lessons learned and changes that were made. Target employed better monitoring and logging of system activity. Target also set up application whitelisting point of sales systems and applied point of sales management tools. Next, they improved firewall rules and policies and limited or disabled vendor access to their network. They then developed the use of two-factor authentication and trained people on password variation.

There are some best practices that can also be implemented such as Triple-A policies and defense in depth. The Triple-A policies are authentication, authorization, and account. Authorization verifies a user’s identity, and it happens when a user enters the proper password and for a username. In this scenario, the password will verify that the user is the owner of the username and should be the one on the account. It confirms validity of the asserted identity. The next policy is authorization. Authorization is a security technique that establishes a user’s privileges to perform specific tasks in a system. It utilizes a role-based power a user can have in the system once they have been authenticated as authorized. The last policy is accounting. Accounting monitors the resources that a user uses for the duration of their network access. This can be system time, or the amount of data sent and received during a session. Defense in depth is a succession of defensive mechanisms which are layered to protect valuable data and information. The concept behind this practice is that if one layer in the mechanism fails, another is there to immediately step up to try to prevent an attack. The redundancies for this approach are intentional to increase the security of a system and address numerous attack vectors.

**References**

Dignan, L. (n.d.). *Target’s data breach: It gets worse*. ZDNet. Retrieved February 10, 2022, from https://www.zdnet.com/article/targets-data-breach-it-gets-worse/

Kassner, M. (2015, February 2). *Anatomy of the Target data breach: Missed opportunities and lessons learned*. ZDNet. Retrieved February 10, 2022, from https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/