COMP2216 Principles of Cyber Security - Cyber Attack Analysis

Username: ppj1u18
Cyber Attack: Target Data Breach

Task 1 - Impact, Response and Recovery Analysis

Impact

The 2013 Data Breach was due to a successful massive cyber-attack launched by cyber-criminals and directed towards one of the largest retail companies in the United States – Target. The company has stated that the personal and financial information of 110 million credit/debit card wielding shoppers had been compromised. More specifically, attackers pilfered 11 gigabytes of data, removed this sensitive data from Target's network to send to off-site FTP servers, and then sell it in the digital black market. Target then finally had a third-party forensic team mitigate the attack.

Response

Just following the mitigation of the attack on December 15th by a third-party forensic team, on December 18th, a security blogger Bloan Krebs broke the story to the public, following which Target also informed its customers. Experts developed an unofficial attack timeline that illustrates points of the attack and highlights several points where it could be stopped. Additionally, Target faced a huge amount of criticism and embarrassment, was forced to make several changes regarding their security posture, and reissue payment cards.

Recovery

Since no data was lost in the attack, no recovery could have been performed. Target still has all its services running so operations should go on as usual.

Task 2 - Weaknesses and Attack Techniques Analysis

Weaknesses

#	**CWE entry**	**Justification** (suggested length: max 100 words for each weakness)
1	CWE-359: Exposure of Private Personal Information to an Unauthorized Actor	Fazio Mechanical's login credentials, along with login credentials for the portals used by Fazio were all exposed to the cybercriminals when a Fazio employee was targeted with a phishing email (Capec 163). This then also allowed the attackers to gain foothold in Target's internal network. Cybercriminals were neither authorised to access this sensitive information, nor did they have the consent of Fazio Mechanical to get this information. Upon search, it was more reasonable to pick this CWE (CWE-359 more specifically) entry over CWE-200(more general) as a Fazio employee's login details can be classified more specifically as personal private information as simply compared with sensitive information.
2	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	As written in the article, Chris Poulin, a research strategist for IBM and security blogger Brian Krebs stated that the attackers abused a vulnerability in the web application, such as SQL injection to gain a point of presence and then attack internal systems in the Target network. The attackers may have interfered with the queries that an application makes to its database, this would have allowed them to get hold of AD credentials that would further allow attackers to gain access to the Ariba portal and then the rest of the portals in the network.
3	CWE – 316: Clear-text storage of sensitive information in memory	When customers swiped their credit/ debit cards at the Target POS terminal to authorize their transaction, the data encoded in the cards got stored in the system's RAM (random access memory). The data in the POS system cannot be encrypted; and the system can only process any data that has already been decrypted in the memory. Cybercriminals used RAM scraping malware to access the system's memory, easily read the information stored in cleartext format and then export the copied information via Remote Access Trojan malware.

Attack Techniques

#	CAPEC entry	ATT&CK Technique	ATT&CK Tactic	**Justification** (suggested length: max 100 words for each attack technique)
1	CAPEC-163: Spear Phishing	User Execution	Execution	User execution would have occurred after the attackers established access into the network by delivering the spear phishing email. A Fazio employee would have activated a malicious executable by either clicking on a Spear Phishing Link or Attachment. After the user input their login credentials, they (the sensitive information) would have been retrieved by the attackers and would be used to login to Fazio Mechanical's network (linked directly to CWE-359).
2	CAPEC-66: SQL injection	Exploit Public-Facing Application	Initial Access	According to the article, the attackers may have used commands or executed SQL queries to retrieve Ariba Portal login details and to move through the Target's internal network. The attackers would have gathered information about the internet facing application, such as application version. Once the application information was gathered the attackers would have tried to enter the system by exploiting SQL injection vulnerability (CWE-89).
3	CAPEC-94: Man In the Middle Attack	Exfiltration Over Physical Medium	Exfiltration	Cybercriminals obtained credit/debit card information stored in a plaintext file (CWE – 316) from the memory of POS payment terminals as cards were swiped, through man-in-the-middle attack (Ram scraping approach), which involves the interception of the processing at the retail checkout point of sale system.

Task 3 - Attack Analysis

Phase 1

Reconnaissance Phase

The attacker conducted a simple internet search that turned up Target's supplier portal which included a page listing HVAC and refrigeration companies one of which was Fazio Mechanical, a refrigeration contractor.

Weaponization Phase

The attacker weaponized malware (Citadel) targeting Fazio as an email attachment.

Delivery Phase

The attacker sent the payload to the victim (contained in the phishing email) through the mail server.

Exploitation Phase

Malware in phishing email activated upon clicking on the link; attackers waited until Citadel malware (a variant of the Zeus banking trojan) gleaned login credentials for the portals used by Fazio.

Installation Phase

Malware Citadel installed in Fazio's network. Attacker maintained access to Fazio's systems for some time before breaking the target's network. Gained persistence through user execution.

Command and Control Phase

The attacker established a communication channel by running the malicious code in the Citadel Trojan on Fazio's computers which sent back login details to the attackers.

Phase 2

Reconnaissance Phase

The attacker gathered Target's technical information, including POS system information, and knowledge about which portal to subvert and use as a staging point into Target's internal network (Ariba Portal - a prime candidate). Additionally, attackers knew that internal administrators would use their AD logins to access the system from inside and that the server had access to rest of the corporate network in some form or another. According to the article, they used the attack cycle in Mandiant's APT1 report to find vulnerabilities.

Weaponization Phase

The attacker used weaponized malware (code-named Trojan.POSRAM) to infect Target's POS system.

Delivery Phase

Delivery to Target's several internal Windows servers through Target's network.

Exploitation Phase

The attacker exploited a vulnerability in the web application, such as SQL injection, XSS, or 0-day to gain a point of presence, then attack internal systems.

Installation Phase

A malware (code-named Trojan.POSRAM) installed, was used to infect Target's POS system. Attacker maintained access to Target's systems for some time before breaking the target's network.

Command and Control Phase

The attacker had 'hands on the keyboard' between the outside Internet and Target's cardholder network. If local time is between the hours of 10AM and 5PM, Trojan attempts to send winxml.dll over a temporary NetBIOS share to an internal host (dump server) inside the compromised network over TCP port 139, 443 or 80. Standard known communication portals used (TCP, ISMP).

Actions on Objective Phase

The attacker transmitted the stolen data to outside servers - in plain text via FTP. The attackers then sold the credentials. Once the credit/debit card information was secure on the dump server, the POS malware sent a special ICMP (ping) 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 it on the digital black market.

Task 4 - Attacker Analysis

Goals, Motivations and Skills

The goal of the attacker was to get access to Target's internal servers and their Point of Sale terminal. The attacker must be quite skilled – with knowledge of developing Citadel malware to get access, designing a phishing email, and with in-depth knowledge of Target's internal network. Additionally, it involved attackers developing RAM scraping malware and the main motivation was to sell the collected credit and debit card records in the black market.

Actor Type

A cybercriminal is most likely behind this attack, as the attacker is interested in illegal profit, and wants to make money by selling the collected credit card data. Additionally, the cybercriminal uses both malware and social engineering/email as attack vectors, both of which were deployed in the Target data breach.

Nation states are interested in High quality intelligence, sabotage activities/critical infrastructures or Subversion e.g. political election but the Target data breach did not agree with any of these types of intentions, as the main interest of the Target attack was illegal profit.

Hacktivists do carry out data breaches with malware as their attack vector, but they are motivated by political, religious or social ideologies rather than illegal profit.

Insiders have legitimate access to valuable resources, however in the Target Data breach, the attackers only had access to information about third party companies. The attackers only gained illegitimate access to resources such as login credentials to Fazio Mechanical and its internal portals, through the installation of the Citadel malware by the sending of a phishing email. It is possible to say, however, that the breach was due to an unintentional insider attack; if employees of Fazio Mechanical were taught to recognize the difference between a regular email and a phishing email, the attack could perhaps have been prevented.

Script Kiddies/ Noobs are less skilled hackers, motivated by the desire to join real hacker groups, and use tools found on the internet. It is not very likely that script kiddies were behind this attack as both the Citadel malware and the Trojan malware are very complex, and as a result, a great depth of knowledge is needed to develop them.