Group 2 Final Project Report

Kwane Galang, Michael Asante, Jonathan Little, Joe Miranda, Luis Pineda, and Nautica Uribe

Outline

1. Intro (Luis)
   1. Incident Description
   2. Response
   3. Resolution
2. Red team (Luis)
   1. Actions taken
   2. What hackers achieved.
   3. Time systems compromised
3. Blue team (Michael)
   1. Failures
   2. Actions taken
      1. Response time
   3. Recovery
4. Prevention (Michael)
   * 1. Improvements
     2. Response plan
5. Fall out /Damages (Kwane)
   * 1. Lawsuits
     2. Reputation
6. Conclusion (Kwane)

Work Cited:

Business Wire. “Trustwave SpiderLabs Exposes Critical Cybersecurity Threats Targeting Retailers.” \*Business Wire\*, 2023, www.businesswire.com. Accessed November 2023.

SpiderLabs. \*Trustwave Threat Intelligence Briefing: The 2023 Financial Services Sector Threat Landscape\*. Trustwave, 2023, www.trustwave.com. Accessed November 2023.

Trustwave. \*Trustwave's 2023 Retail Threat Intelligence Report: Gaining Access\*. Trustwave, 2023, www.trustwave.com. Accessed November 2023.

**Target 2013 Data Breach Incident**

**Group 2 Final Project**

**Luis Pineda, Kwane Galang, Michael Asante, Jonathan Little, Joe Miranda, Nautica Uribe**

**California State University of Los Angeles California**

**FUND NET SYS & CYBER SEC CS 2470-02 (92650)**

**November 13, 2024**

### **Introduction**

In 2013, Target suffered a major data breach that exposed sensitive information of millions of customers, including 40 million payment card numbers and 70 million personal records (Trustwave, 2023). The attack began on November 27th, when cybercriminals compromised Target’s network through a third-party vendor, Fazio Mechanical Services, by using stolen credentials to gain initial access (Business Wire, 2023). Once inside, attackers installed malware on Target’s point-of-sale (POS) systems, which allowed them to capture card data as customers made purchases (Trustwave, 2023). This malware, known as BlackPOS, enabled attackers to exfiltrate vast amounts of data to external servers they controlled (SpiderLabs, 2023). The attack lasted nearly three weeks and went undetected until December 13th and was not mitigated until December 15th. Investigations suggested that the attackers were part of sophisticated Eastern European cybercrime networks, although no specific individuals were apprehended (Trustwave, 2023). The breach resulted in significant financial and reputational damages for Target and a heightened awareness of cybersecurity vulnerabilities related to third-party access (Business Wire, 2023).

### **Response**

In response to the 2013 data breach, Target implemented several measures to address the incident and enhance its cybersecurity posture. The company promptly notified affected customers and offered free credit monitoring services to mitigate potential identity theft risks. Target also invested in upgrading its security systems, including adopting chip-and-PIN technology for its REDcard program to bolster payment security. Additionally, the retailer established a new Chief Information Security Officer (CISO) role to oversee and strengthen its information security strategies. These actions aimed to restore customer trust and prevent future security breaches. Target further collaborated with law enforcement and cybersecurity experts to investigate the breach and improve industry-wide standards for data protection. In the following months, Target also revamped its incident response protocols, ensuring quicker detection and mitigation of potential threats in the future.

### **Resolution**

Following the breach, Target faced multiple lawsuits and reached an $18.5 million settlement in 2017 with 47 states and the District of Columbia, marking one of the largest multi-state data breach settlements at that time. The settlement required Target to adopt enhanced security measures, including encrypting customer information and maintaining a comprehensive security program supervised by senior executives. In addition to the state settlement, Target paid out millions more in other legal settlements and credit monitoring services for affected customers. The company’s efforts to improve its security infrastructure included regular audits, stricter third-party vendor management, and ongoing employee training on cybersecurity best practices. Despite the financial cost, these improvements helped Target regain public trust over time. Today, the Target breach remains a key example in cybersecurity circles, emphasizing the importance of proactive security and robust incident response planning.

### **Red Team Analysis**

#### **Actions Taken**

The red team began their attack on Target on November 27th, however, prior to the breach had conducted reconnaissance to identify potential vulnerabilities, ultimately finding an entry point through a third-party vendor, Fazio Mechanical Services (Trustwave, 2023). By first hacking into Fazio Mechanical Services and waiting for their entry verification for Target, the stolen credentials from this HVAC vendor allowed the attackers to gain initial access to Target’s network, leveraging weak third-party security practices (Business Wire, 2023). Once inside, they carefully moved laterally through the network to locate valuable assets, including Target’s point-of-sale (POS) systems (Trustwave, 2023). To capture payment card information, the red team installed a specialized malware called BlackPOS on the POS terminals, which enabled them to scrape credit card data in real time as transactions occurred (SpiderLabs, 2023). This malware allowed attackers to continuously extract data over several weeks without raising immediate alarms (Business Wire, 2023). They masked the exfiltration process by encrypting the data and routing it through various internal systems, minimizing detection risk (Trustwave, 2023).

#### **What the Attackers Achieved**

The attackers successfully infiltrated Target’s network and obtained sensitive data from millions of customers, achieving a significant data breach with widespread impact. By leveraging the compromised third-party credentials, they gained access to Target’s point-of-sale systems, allowing them to collect approximately 40 million credit and debit card numbers over three weeks (Trustwave, 2023). Additionally, they accessed personal information, including names, addresses, and phone numbers, from 70 million customers, which amplified the breach's scope (Business Wire, 2023). The attackers then exfiltrated this data to external servers, where it was later sold on the black market, creating substantial financial and reputational damage for Target (SpiderLabs, 2023). This breach highlighted the vulnerabilities in third-party vendor security and underscored the effectiveness of targeted malware in capturing large volumes of payment data undetected (Trustwave, 2023). Ultimately, the attackers’ success brought increased scrutiny to cybersecurity practices in the retail sector and served as a costly lesson for companies worldwide.

#### **Time Systems Were Compromised**

The attackers managed to compromise Target's systems from late November until mid-December 2013, exploiting the busy holiday shopping season to mask their activities (Trustwave, 2023). The specific date of breach was Black Friday, which is peak holiday shopping for most of North America. During this period, they maintained continuous access to the network, allowing them to harvest payment card information from millions of transactions in real-time (Business Wire, 2023). The malware, BlackPOS, was installed on thousands of point-of-sale terminals, capturing data as it was processed and sending it to the attackers' external servers (SpiderLabs, 2023). By carefully timing the data exfiltration, they avoided detection by Target's security systems, which were overwhelmed by the high transaction volumes typical of the season (Trustwave, 2023). This prolonged access was critical to the breach’s scale, as it allowed the attackers to extract both payment and personal data across multiple weeks (Business Wire, 2023). Only after several weeks did Target’s security team identify unusual network activity, but by then, the attackers had already exfiltrated vast amounts of sensitive data (Trustwave, 2023).

### **Blue Team Analysis**

#### **Failures in Cybersecurity Defenses**

The 2013 Target data breach revealed significant weaknesses in the company’s blue team operations, which are responsible for detecting, responding to, and mitigating cybersecurity threats. One major failure was delayed detection, as the attackers remained undetected for weeks while exploiting vulnerabilities and exfiltrating sensitive payment data (Card Connect, 2023). Additionally, Target’s network segmentation was insufficient, which allowed attackers to move laterally through the network after breaching a third-party HVAC vendor. This lack of segmentation gave them access to critical systems that should have been isolated (Redriver, 2021). Another notable failure was unaddressed security alerts. Despite using advanced security software, Target failed to act on critical alerts, allowing the breach to escalate unchecked (Darkreading, 2014).

#### **Actions Taken to Address the Breach**

After the breach was identified, on December 13th in 2013, Target implemented several reactive measures. However, the response time was slow, as the breach persisted for weeks since November 27th, before containment on December 15th in 2013.. External cybersecurity experts, including Trustwave, were brought in to support the investigation and mitigation efforts (Trustwave, 2023). Containment measures included isolating infected systems to prevent further compromise and enhancing real-time monitoring to detect unusual activity.

To recover, Target undertook several initiatives. The company restored compromised systems to operational status and overhauled its payment systems, adopting chip-and-pin technology to improve transaction security. Additionally, Target offered free credit monitoring services to customers whose data had been exposed to rebuild trust and address customer concerns (Attorney General, 2017).

#### **Speculative Prevention Measures**

To prevent similar breaches in the future, Target could strengthen network segmentation by implementing policies to isolate sensitive systems, such as payment processing systems, from third-party vendor access (Redriver, 2021). Improving third-party vendor security through regular audits and stricter access controls would minimize vulnerabilities introduced by external partners (SpiderLabs, 2023). Additionally, having two-factor authentication for third-party vendors could be added security and require said vendors to be up to date on their own cybersecurity protocols. Further, the adoption of real-time threat detection systems capable of identifying and responding to breaches immediately would help mitigate potential risks (Business Wire, 2023).

In addition to technological measures, Target could develop a more robust incident response plan. This would involve providing incident response training to internal teams to ensure prompt and effective reactions to threats. Establishing formalized protocols for identifying, containing, and mitigating breaches would help streamline responses. Strategic partnerships with cybersecurity firms would also ensure rapid containment and remediation during future incidents (Trustwave, 2023).

### **Fall out/Damages**

#### **Lawsuits**

Target has faced a few lawsuits due to the 2013 data breach. With the security service of Trustwave, Target was filed in a lawsuit by the Trustmark National Bank and Green Bank (Darkreading, 2013). The lawsuit displays a company, Trustwave, mentioned in a complaint as owning the "specialized knowledge in PCI compliance," supposedly provided as Target's QSA (PCI-approved Qualified Security Assessor) while observing their systems for signals of unexpected disturbances (Darkreading, 2013). "Trustwave also delivered round-the-clock tracking services to Target, which tracking methods were planned to catch any attack invasions within Target's programs and incorporations of PII or other classified data" (Darkreading, 2013). In addition, a lawsuit is also filed against Target by 47 U.S. states. (Attorney General, 2017) This lawsuit accused Target of the attackers' theft of over 100 million personal information or credit cards by customers in the U.S. (Attorney General, 2017). Overall, those cases illustrated how the company was accused of failing to provide its consumers with sensitive information, which led to a poor reputation.

#### **Reputation**

Target’s data breach in 2013 suffered vital reputational damages. One of which is the amount of money that they lost. The estimated value of the data breach goes above the mandatory settlement of $18.5 million; the company loses more than $200 million (Redriver, 2021). Furthermore, the top-level employers, including Target’s CEO, were unemployed/lost their jobs, and more than 140 lawsuits were filed in three years (Card Connect, 2023). In addition, during the fourth quarter of 2013, especially during the holidays, Target’s earned profits were diminished by 46 percent by the attack; additionally, the presence of customers shopping in their closest households became wary after the data breach at Target due to the concerns about their credit card security (Redriver, 2021). All of those events led to the company’s great downfall in the customer’s trust, causing sales to drop and causing a negative insight into their security practices. Because of this, Target had to work heavily to restore its public reputation and make advancements in its cybersecurity infrastructure (Redriver, 2021).

### **Conclusion**

Target is one of the companies that faced a significant data breach. Moreover, retailers/merchants must recognize that the wide span of security threats could be more substantial than the standard PCI compliance (Card Connect, 2023). Staff members should understand and practice scam detection and engage in the protection of network and computer security. Keeping track of the networks and paying more attention to disturbing or unexpected patterns in a system’s network is crucial for Target to safeguard their systems and, consecutively, the customer’s data (Card Connect, 2023). Warning signs should be implemented and carried out as quickly as possible regarding a cybersecurity response plan that everyone can retrieve. All in all, taking responsibility in a company or business is essential, especially after a data breach incident, to ensure the safety of shielding their consumers/customers the best way they can to prevent any cyber threats in the future (Card Connect, 2023).

**References**

Business Wire. (2023). *Trustwave SpiderLabs exposes critical cybersecurity threats targeting retailers*. Business Wire. Retrieved November 2023, from [www.businesswire.com](http://www.businesswire.com).

SpiderLabs. (2023). *Trustwave threat intelligence briefing: The 2023 financial services sector threat landscape*. Trustwave. Retrieved November 2023, from [www.trustwave.com](http://www.trustwave.com).

Trustwave. (2023). *Trustwave's 2023 retail threat intelligence report: Gaining access*. Trustwave. Retrieved November 2023, from [www.trustwave.com](http://www.trustwave.com).

*Darkreading. (2014). Target, PCI Auditor Trustwave Sued By Banks*. Darkreading. Retrieved November 2023, from <https://www.darkreading.com/cyber-risk/target-pci-auditor-trustwave-sued-by-banks>

Attorney General. (2017). *Settlement reached with target following major consumer data breach*. Attorney General. Retrieved November 2023, from

<https://www.attorneygeneral.gov/taking-action/settlement-reached-with-target-following-major-consumer-data-breach/>

Redriver. (2021). *Warnings (& lessons) of the 2013 Target Data Breach*. Redriver. Retrieved November 2023, from<https://redriver.com/security/target-data-breach#:~:text=Following%20the%20holiday%20season%2C%20customers,to%20restore%20its%20public%20reputation>.

Card Connect. (2023). *Case Study: What We've Learned from the Target Data Breach of 2013.* Card Connect. Retrieved November 2023, from <https://www.cardconnect.com/launchpointe/payment-trends/target-data-breach/>