CIS4367.01 **Brandon Thompson**
Prof. Elibol Due Date: 2/28/2020

Homework 7

PROBLEM :

Research the 2013 Target data breach and prepare a report about the attack. Provide the following:

- Brief description of the attack.
- Timeline of the attack.
- Root cause analysis. What happened? How it happened? (Technical analysis).
- Discussion of how the company became aware of the breach.
- What were the consequences of the breach? Effects of the breach (Reputational? Financial? Operational?)
- Are there any lessons learned?
- Discuss breach in terms of confidentiality, integrity, and availability in general.

SOLUTION:

In 2013 Target notified 110 million shoppers that their personal and financial information had been compromised. The attack started on November 27, 2013 (Black Friday) and Target notified the US Justice Department by December 13. By December 15th, Target had a third party forensic team in place and the attack mitigated. **Gathering information:**

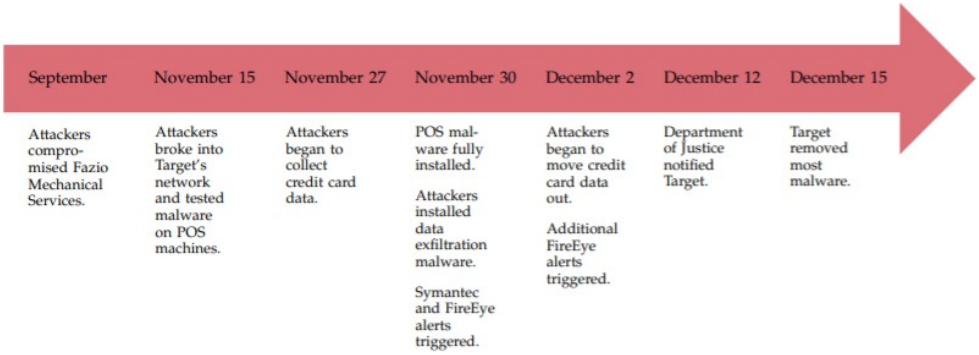

Figure 1: Timeline of the Target data breach (Shu et al.)

We do not know how attackers were able to gather information about Target's network before the attack, however there is a plethora of information about supplier interaction and Microsoft management systems for security patches.

Compromise system: Target's network was to well protected, being the large corporation that they are. Third party vendors, however, do not have as many resources. An employee at Fazio Mechanical was duped in a phishing email that installed `Citadel`, a banking trojan on Fazio computers. Attackers then had to wait for the vendors Target portal login.

After vendor access: Target has not released this information but it is possible that attackers used SQL injection, XSS or a 0-day attack on the web application to elevate privileges and then access internal systems.

Internal Servers: Speculated that attackers used an attack cycle in `Mandiant's APT1 report` defined by Figure 2 to move laterally through the network.

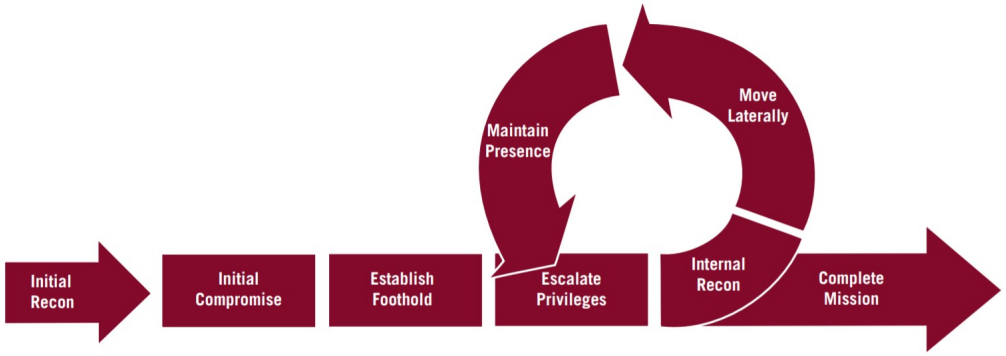

Figure 2: Mandiant's Attack Lifecycle Model (Page 27 of Mandiant APT1 report).

Point of Sale Systems: Malware code utilized RAM-scraping to grab card information from memory of POS-devices. Malware checks if time is between 10AM and 5PM to send a `winxml.dll` file over a temporary NetBIOS share to an internal dump server within the network. Meaning POS systems that were not able to access the internet were still vulnerable. Attackers the moved stolen data off-site.

Target was made aware of errors in their system by their FireEye security system but chose to ignore the initial warning. Later flags revealed a much larger problem than was originally thought.

Lessons Learned:

- Monitor system activity more closely.
- Implement POS management tools.
- Least privilege on vendor accounts.
- Two-factor authentication.

By improving on this list, Target could have reduced the chances of this data breach

occurring. The third party vendor initially compromised could have better trained their employees against phishing attacks.

In terms of **Confidentiality** the Target breach was a major loss of confidentiality because it released important financial information about a large number of users. **Integrity:** There was not a loss of integrity, attackers wanted to stay inside the network for as long as possible in order to get as much data as possible. **Availability:** Again, attackers did not want to alert the system admins to any major issues within the system, just fly under their radar for as long as possible. The more the system was available, the more card numbers they could collect.

References:

- `https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/`
- `https://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf`
- Breaking the Target: An Analysis of Target Data Breach and Lessons Learned by Xiaokui Shu, et al.