TARGET DATA BREACH

Carlos Ocasio

CSCI – 40540

Instructor: Dr. Melton

INTRODUCTION

- Cyberattacks are malicious attempts to expose, alter, disable, destroy, steal or gain unauthorized access of an asset.
- Cyberattacks cost the U.S. economy between $57 billion and $109 billion in 2016 (The Council of Economic Advisers, 2018).
- Government organizations and financial firms are the focus of most cyberattacks.

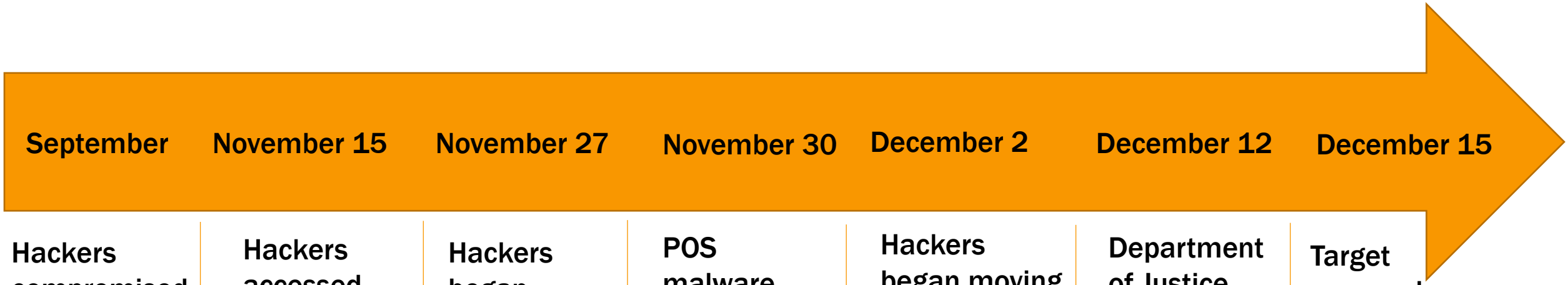
WHAT IS TARGET CORPORATION?

- Target Corporation is a retail that specializes in general merchandise and food.
- Initially began as a department store known as Dayton.
- It is the 8th largest retailer in the United States (National Retail Federation, 2016).

TARGET DATA BREACH

- In December 2013 Target announced that the data from around 110 million users was stolen.
- Considered the second largest credit and debit card breach.
  - Around 45 million cards were affected (Pigni, Bartosiak, Piccoli, & Ives, 2018).
- The hackers were able to obtain name, addresses, phone numbers and emails.

BREACH TIMELINE



Hackers compromised Fazio Mechanical Services.

Hackers accessed Target's Network and installed malware.

Hackers began collecting credit card data.

POS malware fully installed.

Alerts triggered.

Hackers began moving credit card data out.

Additional alerts triggered.

Department of Justice notified Target.

Target removed most malware.

WHAT HAPPENED?

- It is believed that the hackers gathered information from Target and its interaction with vendors, by a google search (Radichel, 2014).
- The hackers obtained a list of HVAC refrigeration companies that work with Target (Radichel, 2014).
- An email containing malware was sent to vendor Fazio Mechanical (Radichel, 2014).
- The malware installed in Fazio Mechanical's network is known as Citadel.

- The criminals were able to access Target's system via Fazio Mechanical's stolen credentials (Radichel, 2014).
- Once the hackers accessed the network, malware was installed on the point of sales systems.
- The software was quickly distributed via automated updates (Krebs, 2014).

TARGET'S NETWORK BREACHED

STEALING CREDIT CARD DATA

- Once the POS received the infected update, the hackers began collecting credit and debit card data from customers.

- Monitoring software Fire Eye alerted staff members of the suspicious behavior, but no action was taken (Radichel, 2014).

STEALING CREDIT CARD DATA

- The stolen credit card data was moved to hacked servers all over the world (Krebs, 2014).
- Another alarm is triggered, and the Department of Justice notifies Target.
- Credit card records sold on the dark web.

DIAGRAM OF THE TARGET BREACH

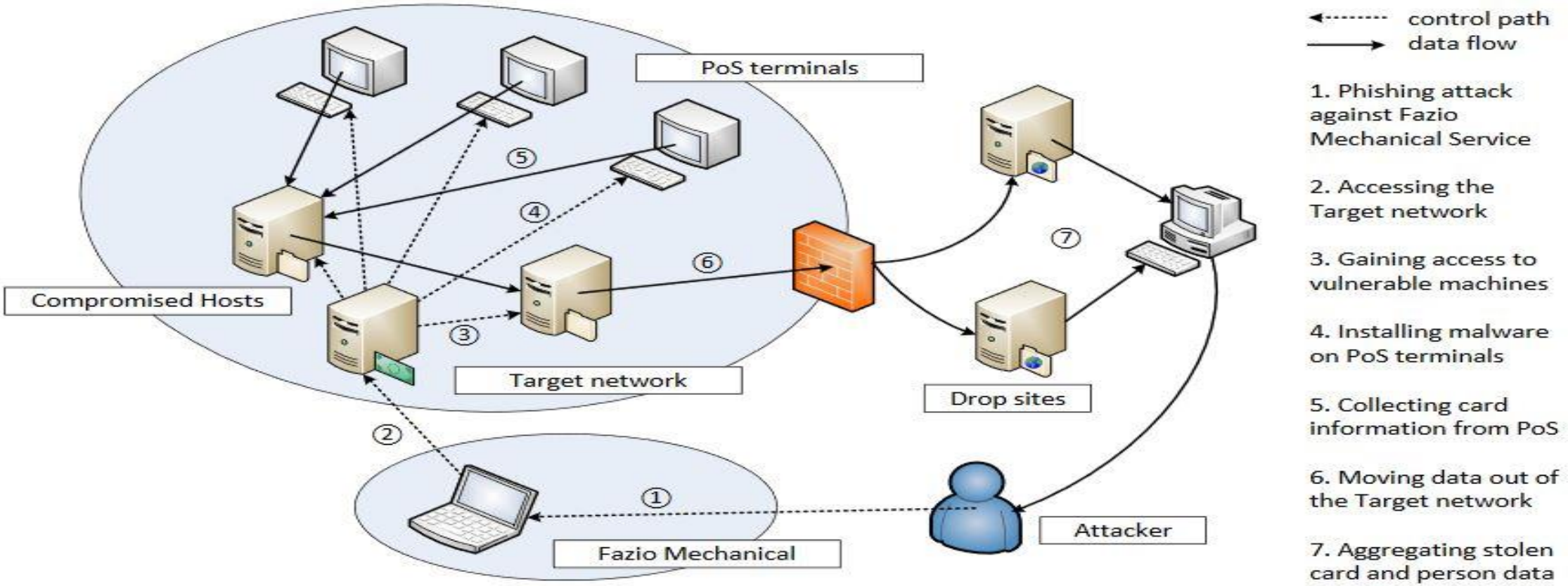


Fig. 2. Attack steps of the Target breach.

AFTER THE BREACH

- The former CEO of the company, Gregg Steinhafel, resigned after the breach.
- Deployment of chip-and-PIN enabled technology.
- Implemented network segmentation.
- Reviewed and limited vendor access.

IMPACT OF THE ATTACK

- 1,800 stores affected.
- 40 million credit and debit cards compromised.
- 70 million accounts compromised.
- 41 million affected consumers.
- 18.5 million settlement.
- 6% sales decline.
- Over 420 million cost.

HOW IT COULD HAVE BEEN PREVENTED

- Proper security awareness training for employees.
- Remove vendor information and other sensitive information from unsecured websites.
- Require vendors to use antivirus software.
- Limit network access.
- Require multi-factor authentication to log into vendor portals.
- Segregate critical systems from the rest of the network.
- Installing proper application software security.

HACKER LINKED TO TARGET DATA BREACH

- Ruslan Bondars was sentenced to 14 years in prison for designing “Scan4You” a program that was linked to the Target Breach.
- Scan4You allowed hackers to determine whether their malware would be detected or not.

REFERENCES

Krebs, B. (2014a, January 14). A closer look at the Target malware, part II. Retrieved from Krebs on Security: http://krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/#more-2440

The Council of Economic Advisers. (2018). The Cost of Malicious Cyber Activity to the U.S. Economy. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

McCoy, K. (2017, May 23). Target to pay $18.5M for 2013 data breach that affected 41 million consumers. Retrieved November 06, 2020, from https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

Newsday.com. (2018). 14 facts you didn't know about Target. Retrieved from https://www.newsday.com/business/facts-you-didn-t-know-about-target-1.12146566

REFERENCES

Operator of Counter Antivirus Service "Scan4you" Sentenced to 14 Years in Prison. (2018). Department of Justice. Retrieved from https://www.justice.gov/opa/pr/operator-counter-antivirus-service-scan4you-sentenced-14-years-prison

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100 million dollar data breach. *Journal of Information Technology Teaching Cases*, *8*(1), 9–23. https://doi.org/10.1057/s41266-017-0028-0

Radichel, T. (2014). Case study: Critical controls that could have prevented target breach. *SANS Institute InfoSec Reading Room*.

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the target: An analysis of target data breach and lessons learned. *arXiv preprint arXiv:1701.04940*