Target Data Breach of 2013

by Matthew Weigel

Overview of the Incident

In November 2013, hackers gained access to Target's network and stole customer data.

Over 100 million customers were affected.

Incident could have been prevented

The Attack

- The cyber-attack began on November 27, 2013, days before Black Friday.
  - Optimal time due high traffic of in-store shoppers

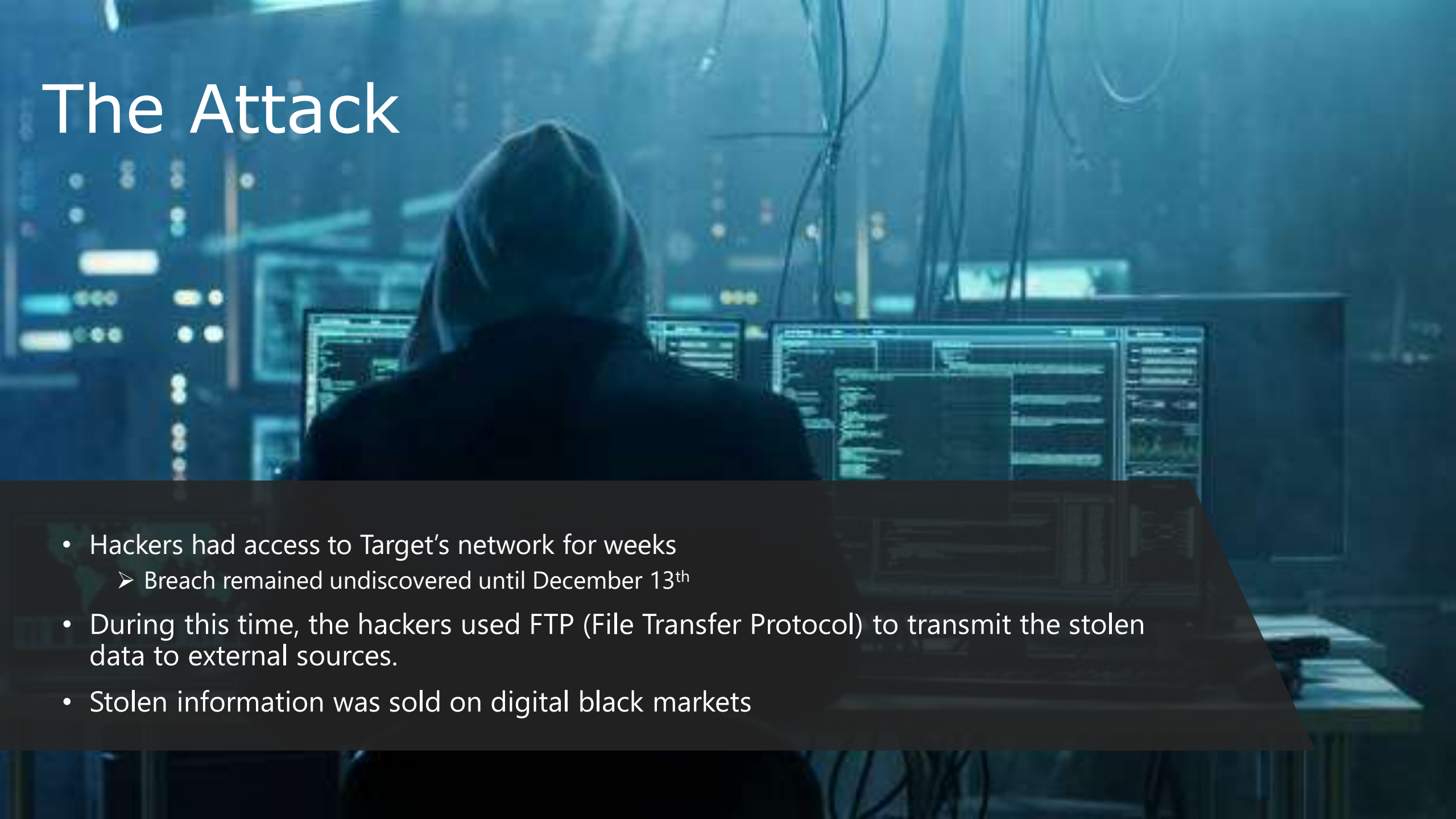
The Attack

- The hackers most likely performed preliminary reconnaissance to find the best point of entry into Target's network.
- One of Target's refrigeration contractors, Fazio Mechanical, was targeted.
  - The hackers used phishing emails to steal credentials from a Fazio employee.
  - The credentials were used to access Target's external billing system.

The Attack

- The hackers then made it into Target's internal network from the vendor portal.
- Once the hackers accessed Target's network, they uploaded another type of malware Target's POS (Point-of-Sale) machines.
  - Any Target customer who swiped their credit card at this time could have their information compromised.

The Attack



- Hackers had access to Target's network for weeks
  - Breach remained undiscovered until December 13th
- During this time, the hackers used FTP (File Transfer Protocol) to transmit the stolen data to external sources.
- Stolen information was sold on digital black markets

The Malware

- BlackPOS
  - Relatively crude but effective crimeware product designed to be installed on POS devices and record all data from credit and debit cards swiped through the infected system.
  - A type of “RAM-scraping” malware
  - Captured the credit card data stored on the card’s magnetic stripe in the instant after it has been swiped at the POS terminal.

Who Was Responsible?

- Ukrainian hacker named Andrey Hodirevski
  - A main member of DarkLife, a Russian hack team
  - Had, “a high reputation and credibility among other carders and hackers”, (Dmitry Volkov).

The Aftermath

- Over 100 million customers were affected
  - 40 million credit cards were compromised
- Target had to pay $154 million in settlements.
  - $10 million to affected customers
  - A combined $86 million to Mastercard and Visa
  - $39 million to banks and credit unions
- Total cost of the breach was $292 million
- Target CEO lost his job

How it Could Have Been Prevented

- At the time of the attack, the HVAC and refrigeration contractor Fazio was not using the appropriate anti-malware software.
- Target could have limited the amount of publicly available vendor information.
- Target could have potentially disrupted the attack by requiring two-factor authentication for its vendors.

Lessons Learned

Staff must be properly trained to detect phishing scams and other early threats.

Networks should be properly segmented to protect the most the sensitive data from potential intrusions.

System intrusion warnings should be taken seriously and responded to appropriately.

References

A “Kill Chain” Analysis of the 2013 Target Data Breach. (2014, March 26). Retrieved March 2, 2022, from http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883

Bjorhus, J. (2014, November 23). Foreign Gangs Top List of Target Data Breach Suspects. Retrieved March 2, 2022, from https://www.startribune.com/foreign-gangs-top-list-of-target-data-breach-suspects/283597021/?refresh=true

Chen, J. (2022, February 08). Ram scraping attack. Retrieved March 2, 2022, from https://www.investopedia.com/terms/r/ram-scraping-attack.asp

Entech. (2019, May 1). Anatomy of a Data Breach – What We Learned from Target. Retrieved March 2, 2022, from https://www.entechus.com/blogs/anatomy-of-a-data-breach-what-we-learned-from-target

Kassner, M. (2015, February 02). Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned. Retrieved March 2, 2022, from https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

References

Krebs, B. (2014, January 15). A First Look at the Target Intrusion, Malware. Retrieved March 2, 2022, from https://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/

Krebs, B. (2014, February 12). Email Attack on Vendor Set Up Breach at Target. Retrieved March 2, 2022, from https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

Lynch, V. (2020, August 24). Cost of 2013 Target Data Breach Nears $300 million. Retrieved March 2, 2022, from https://www.thesslstore.com/blog/2013-target-data-breach-settled/

Morad, R. (2015, March 26). Target Data Breach Victims Could Get up to $10,000. Retrieved March 16, 2022, from https://www.lifelock.com/learn/data-breaches/target-data-breach-victims-could-get-up-to-10000