Target Store Credit Payment Card Breach

Bryce Furrow

CSCI 301: Survey of Scripting Languages

ON TARGET

What, When, and Where

- December 18, 2013
- international-scale cyberattack
- stolen credit and debit card information

(Clark, 2014)

The Beginning

- started in late November – before Black Friday
- Target knew but did not tell the public

(Kassner, 2015)

How could something like this happen?

Software issues,
but also plain negligence…

How It Happened - Part 1

- Directed at third-party vendor vulnerability, not Target
- Fazio Mechanical
- Phishing email
- Citadel malware
- Acquired login credentials

(Kassner, 2015)

ON TARGET

Key Note - Citadel

- Normally identifiable by company anti-malware software
- Limited protections in use – no real-time

(Kassner, 2015)

How It Happened - Part 2

- Breach Target servers
- Directed at Target's point of sale (POS) systems
- Trojan.POSRAM
- Stole the card information when swiped

(Kassner, 2015)

How It Happened - Part 3

- Relayed back to attacker's servers
- Sold information on digital black market

(Kassner, 2015)

Damages to Consumers

- Affected over 100 million Target customers
- Likely faced a swarm of fraud cases

(Clark, 2014)

ON TARGET

Damages to Target

- Lost lots of money and consumer trust – 46% drop and beyond (Clark, 2014; *Case Study: What We've Learned From the Target Data Breach of 2013*)
- Lost even more money, facing 140 lawsuits in 3 years (*Case Study: What We've Learned From the Target Data Breach of 2013*)
- Cost $252 million even before the lawsuits (*Case Study: What We've Learned From the Target Data Breach of 2013*)
- Mass layoffs (Clark, 2014)
- Target CEO, Gregg Steinhafel, had to step down (Clark, 2014)

Other Damages

Banks had to reissue 21.8 million cards

(*Case Study: What We've Learned From the Target Data Breach of 2013*)

ON TARGET

How could this have been prevented, and how can it be prevented in the future?

Employee Changes

- Basic employee cybersecurity training
- Password rotation (Kassner, 2015)
- Limitations on who has network access, and limit privileges of those who do (Kassner, 2015)

ON TARGET

Software Changes

- Invest appropriate funds into anti-malware software and cyberattack countermeasures
- Two-factor authentication with those that have internal access to sensitive information.
- Increase system monitorization
- Improve firewalls

(Kassner, 2015)

ON TARGET

EMV technology – card protection

(*Case Study: What We've Learned From the Target Data Breach of 2013*)

ON TARGET

References

Case Study: What We've Learned From the Target Data Breach of 2013. CardConnect. (n.d.). Retrieved November 30, 2021, from https://cardconnect.com/launchpointe/payment-trends/target-data-breach.

Clark, M. (2014, May 5). *Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed For The Giant Retailer*. International Business Times. Retrieved November 30, 2021, from https://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056.

Kassner, M. (2015, February 2). *Anatomy of the Target data breach: Missed opportunities and lessons learned*. ZDNet. Retrieved November 30, 2021, from https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.