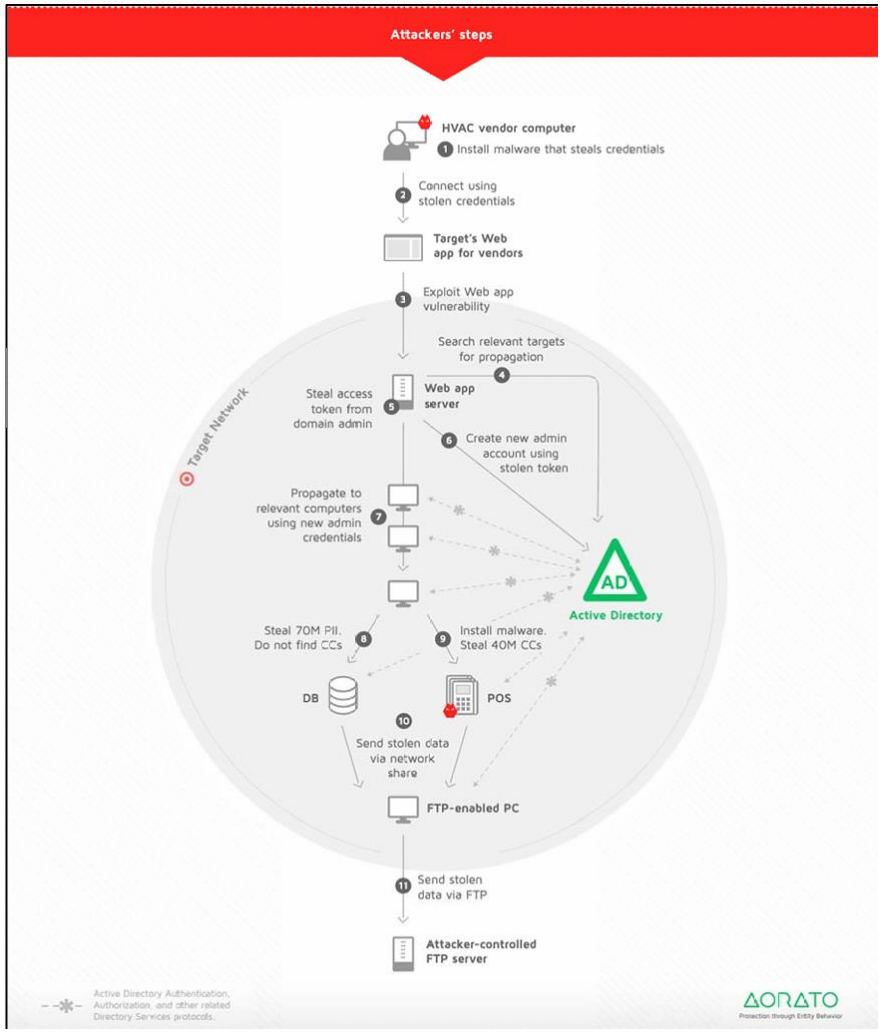
TARGET CYBER ATACK

Audrey Waggener

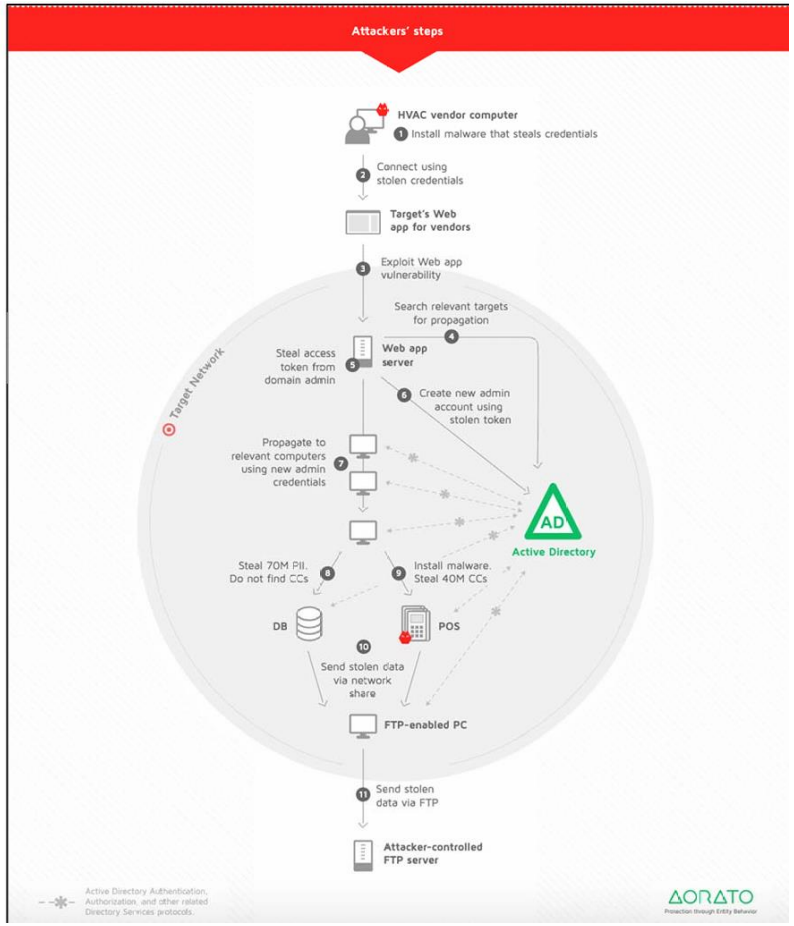
OVERVIEW AND ATTACK VECTOR

- December 19, 2023: Target's Point of Sale machines were compromised.
- Attackers were able to get ahold of 70 million customers Personally Identifying Information and 40 million customers credit card information.
- Attackers used multiple types of malware relying heavily on a technique known as "Pass the Hash" where they used legitimate IT applications nefariously to get administrator privileges.



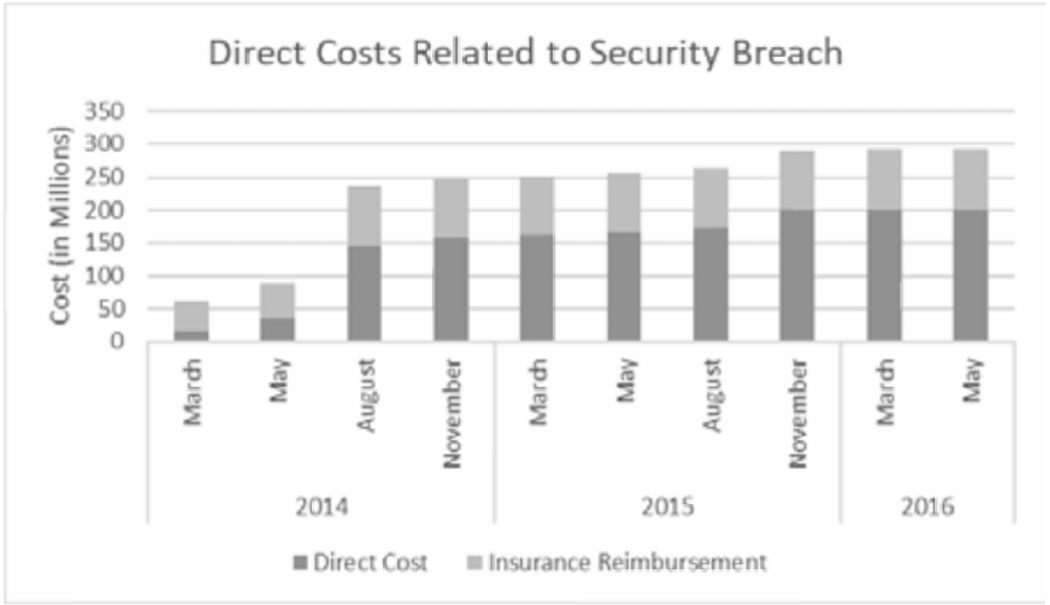
OVERVIEW AND ATTACK VECTOR

- Attackers initially breached Target's system through a third party contractor, Fazio Mechanical Services through the use of phishing emails to get login credentials.
- They then used that access to upload a web shell to gain remote server control, harvested password hashes, and created a stealth account to keep access.
- Even with this access the attackers could not get credit card information due to Target's compliance with PCI DSS.
- They instead installed malware that disguises itself as antivirus software on the POS machines and had customers card information sent to their own server.



IMPACT

- Customers who shopped between November 27 and December 15 of that year were impacted.
- Attack caused the public to trust major corporations less with their personal and credit card information due to how large it was.
- Target faced many lawsuits and the breach cost the company $162 million in expenses.



INCIDENT RESPONSE

- Target notified customers four days after they discovered the breach.
- Their systems discovered the malware on November 30 but the alert was not investigated.
- Credit card companies were the ones who notified Target after noticing excess fraudulent activity.
- The delay in notifying customers and lack of transparency hurt customer trust.

Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website. If you have further questions, you may call us at 866-852-8680.

Gregg Steinhafel

Gregg Steinhafel

Chairman, President and CEO

LESSONS LEARNED

- Led to realization and expectation that companies not only need to protect their corporate network and their data but also all networks of vendors and third parties throughout the supply chain.

- Also led to acknowledgement that response and recovery should be a key part of corporate crisis management programs.