THE ECONOMICS OF CYBERSECURITY

GROUP 2: TARGET DATA BREACH = DAVID, SIDD, NICHOLAS, JACOB

In December of 2013 news reports came out that over 40 million credit card numbers had been stolen from Target. Target later revised the number up to 70 million credit card numbers.

Two months prior to the breach, a phishing email containing malware was opened by a refrigeration vendor. The malware stole credentials leading to a vendor portal. From here, it is believed that the attackers were able to move within Target's network and conduct reconnaissance. A vulnerable domain controller allowed access in the Point of Sale system. This system was then compromised with malware allowing credit card information to be stolen as the cards were swiped at the terminal. The cardholder's name, credit card number, CVV, and card expiration data is encrypted as it leaves the PoS system and the company's network. There is a period of time when this data is stored in the system's RAM in cleartext and can be read by malware installed on the machine. The stolen data was then transmitted to several drop locations. Within days, fraud analysts were able to confirm that batches in the millions of Target credit card numbers were available for purchase on "card shops". These underground "card shops" have websites showing Bank Identification Numbers, which are the first six digits of a debit or credit card. Analysts were able to purchase cards that matched Target's breach of November 27 to December 15, 2013.

Sources:

1. https://www.computerworld.com/article/2487643/target-s-point-of-sale-terminals-were-infected-with-malware.html
2. https://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/
3. https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

Q4. RESEARCH AND IDENTIFY THE COSTS TO TARGET AS A RESULT OF THIS BREACH:

According to the sources provided, threat actors were able to compromise a third party vendor to Target via phishing. The threat actors moved laterally throughout Targets network and attackers pilfered 11 gigabytes of data.

Target was forced to pay 18.5M to cover lawsuits from those who were harmed in the attack. In one of the biggest data breaches to hit a U.S. retailer, Target had reported that hackers stole data from up to 40 million credit and debit cards of shoppers who had visited its stores during the 2013 holiday season.

Total cost of breach was $202M. One of the costs for Target was paying for a credit monitoring service for affected customers, even though that is sort of useless.

Approximately 40 million credit and debit card accounts possibly have been impacted by the breach. Also, about 70 million people were affected.