

Ancel Carson

Prof. Doug Lim

COSC3403-01

16 January 2019

Target Credit Card Scam

In December of 2013 Target released a statement that between Black Friday and Christmas there had been a major security breach. The breach affected almost 70 million Americans as their information was stolen. Information such as names, physical addresses, email addresses, phone numbers, and credit card information was all collected in this breach. It is reported that 11 gigabytes of data were collected during the attack. Of the 70 million people affected around 40 million credit and debit card accounts were impacted.

The breach occurred because the security used by target Target failed to catch a bot hack that made its way onto their servers. “The breach started after a phishing email duped an employee of Target third-party vendor Fazio Mechanical, allowing Citadel, a password-stealing bot variant, to be installed on Fazio computers. Once Citadel successfully snagged Fazio's login credentials, the attackers breached Target's Ariba vendor portal, gained entry into the retailer's internal network and took control of Target servers.”

This breach was considered the most significant breach in history largely due to the events that occurred afterwards. As a result of the breach Target's CEO at the time was fired marking the first time a CEO had been fired for this reason. Another result was of course the loss

of money by all of those affected. There is no exact number to the amount lost but it none the less caught the attention of all corporations and pointed to the importance of credit card security.

Works Cited

Natalie Gagliardi. "The Target breach, two years later." *ZDNet*, 27 November 2015,
<https://www.zdnet.com/article/the-target-breach-two-years-later/>. Accessed 15 January
2019.

"Sources: Target Investigating Data Breach." *KrebsonSecurity*, 13 December 2013,
<https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/>.
Accessed 15 January 2019.