Edmark R. Gariando

BSIT 3-1

Bangladesh Bank Heist

Summary

- On January 2015, an employee clicked a suspicious phishing e-mail that popping up inside the Bangladesh Bank that contains a zip file of an applicant's CV. The hacker gained access to the network trying to infiltrate other computers and started injecting different kinds of malwares. They spent some time to learn on where the money came from the banks and how they can transfer it. After learning how the system works, they manipulated the SWIFT bank system and made a different transaction around the world. They attempted a thirty-six transaction but only four of them went through. Hacker successfully transferred a total of 81 million dollar to their five RCBC accounts in the Philippines.

After these activities, they try to split the money such as playing it in the Casino so that authorities cannot suspect them, the robbers finished their gambling quietly cashed out their chips, walked out of the casino, and left the country, flying to China. The hackers able to successfully steal millions of dollars from the Bangladesh Bank. The identity of the hackers remains unclear but, investigations states that it comes from international hacking group known as "Lazarus Group" who's responsible in different bank hacking activities.

Reaction/Conclusions

- The Bangladesh Bank heist served as a reminder of the potential impact of cyber threats on a country's financial system. It highlighted the fact that even a single click on a suspicious link can faces different consequences for an entire system. Enhancing cybersecurity measures and providing comprehensive training to employees regarding malware can play a crucial role in preventing such incidents.