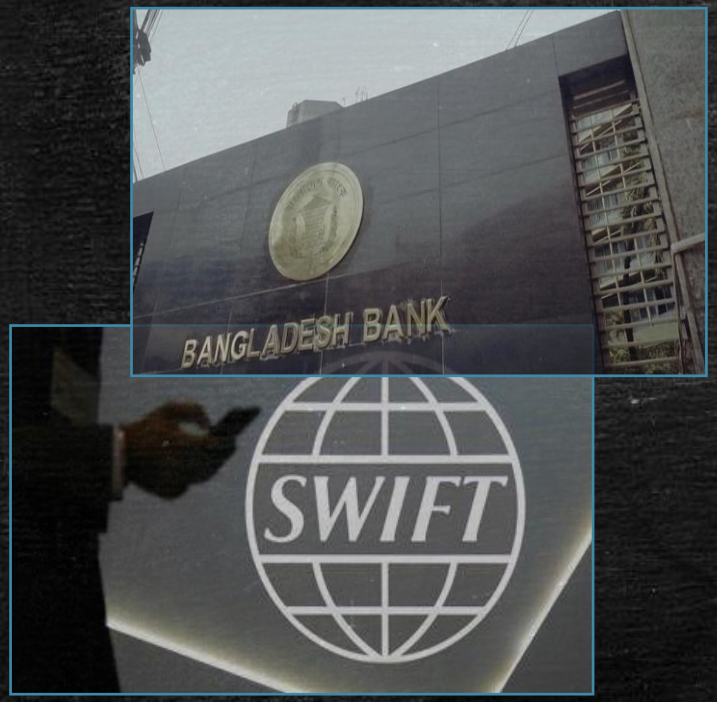
Bangladesh Bank Heist 2016

By: Mirza Kurtovic

Contents

- Background
- The attack
- Further investigation
- Analysis
- Possible prevention methods
- Conclusion

The Heist



- The heist was carried out in February 2016 in Bangladesh
- Hackers broke into the Bangladesh Central Bank systems
- 35 fraudulent transactions totaling $951 million
- 4 successful transfers, hackers netting $81 million
- Dubbed the greatest cyberheist and the greatest bank heist in history

HOW DID IT HAPPEN?

The Attack

The preparation

- In May 2015, a group of men opened 4 bank accounts in the Philippines
- In January 2016, an employee at the Bangladesh Central bank opens an infected email, compromising the entire internal network
- The hackers' malware was designed to steal credentials and enabled lateral movement to connected systems
- 32 systems were compromised before moving to machines connected to the SWIFT financial network

The preparation

- Hiding in plain sight, the hackers could observe employees and their actions, while learning how financial messages are processed within the SWIFT system
- The hackers interfered with connected processes to mask their presence in the system
- They detected an automated printer connected to the SWIFT network that printed out backlogs of transactions
- The printer was deliberately sabotaged to distract the employees and hide the fraudulent transactions

Initiating the transfers

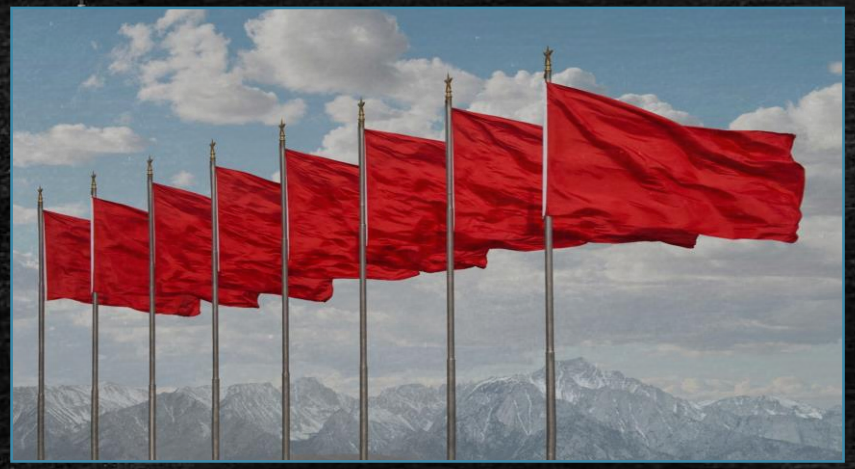
- On February 6th 2016, 35 phony transfers were sent via SWIFT to the Federal Reserve Bank of New York
- The details of the requests stated that the funds are to be transferred from New York to various accounts set up across Asia
- $20 million USD were transferred to a Pan Asia Bank in Sri Lanka to a non-profit company called the "Shalika Foundation"
- $81 million USD arrived to the 4 bank accounts set up under fake identities in a branch of the RCBC bank in the Philippines

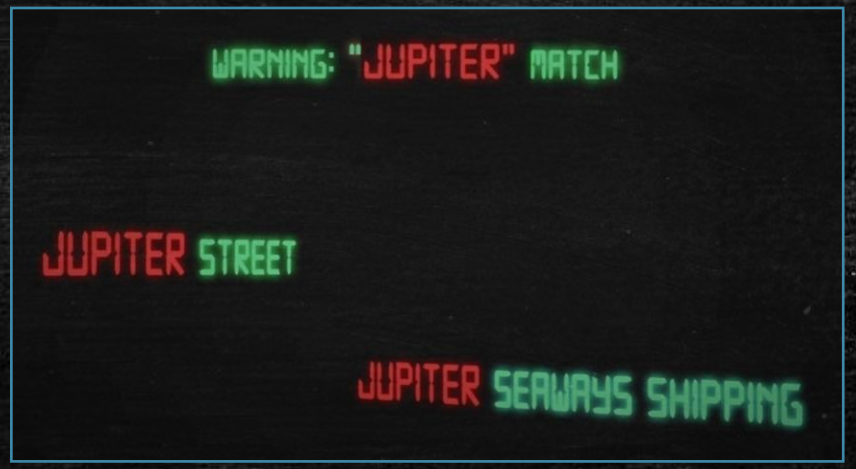
Initiating the transfers

- The money from the 4 bank accounts was quickly withdrawn and laundered through casinos, where the electronic money transfers were converted to untraceable cash

Initiating the transfers

- Unfortunately for the hackers, 30 transfer requests were automatically red flagged due to a company name on the details matching a shipping company blacklisted for evading US sanctions against Iran. $850 million Dollars in total were blocked





Initiating the transfers

- Another lucky break was caught when an employee from the Pan Asian Bank in Sri Lanka noticed a spelling mistake on the receiving company's name. The hackers misspelled "Shalika Foundation" as "Shalika Fandation". This mistake cost them another $20 million Dollars.

The reaction

- By the time the workers at the Bangladesh Central Bank noticed the absurd amount of transfers it was too late.
- Joined efforts between the FBI, Philippines and Bangladesh Governments to prevent money laundering in the region proved to be fruitless.
- Two of the men responsible for setting up the 4 bank accounts were identified, but they fled to Macau before they could be apprehended

Further investigation

- By analyzing the malware in the bank's systems, Cyber Security experts uncovered similar tools and methods used in many other cyberattacks on financial institutions across the globe.
- They uncovered the name of the attackers. It was a group called "Lazarus"
- Possible connection with North Korea?

Analysis

Key concepts behind the attack

- Masterful reconnaissance
- Timing and patience
- Selecting attack vector
- Escape plan

Conclusion

Possible prevention methods

- Spam filters, antivirus protection and awareness trainings
- User management and role management by the principle of least privilege
- Strong password policy
- Use of multi-factor authentication whenever possible
- Segmenting networks and securing remote access
- Intrusion prevention/detection mechanisms
- Monitoring user and account activity do detect threats and implementing secondary verification/review systems on large transfers

THANK YOU FOR YOUR ATTENTION