**The Great Bangladesh Bank Heist**

The global banking system is extremely complicated. This also makes security for the global banking system extremely complicated. In February of 2016, hackers exploited the complexity of the banking system to attempt a heist of $951 million from the Central Bank of Bangladesh, and if not for a stroke of luck would have gotten the entire lump sum. Even as it is, they managed to make off with $81 million, all still missing to this day.

There are two key components to the global financial system. First, the United States Federal Reserve. The Fed acts as a sort of bank for other banks. Because of its massive size, the Fed can implement all sorts of services and security not possible for smaller institutions. So many banks, even the central banks of many countries, keep their money in accounts at the Federal Reserve. The second key component is a system for transferring money, called the Society for Worldwide Interbank Financial Telecommunication, or SWIFT for short. SWIFT allows banks to withdraw funds or transfer money across the world in a secure fashion. In order to use the SWIFT system, you must have the credentials for the institution you are representing. In theory, this makes sure imitation is not possible.

Of course, imitation happened nonetheless. On February 4, attackers using the credentials of the Central Bank of Bangladesh ordered fraudulent payments to accounts in the Philippines and Sri Lanka totalling $951 million. Since the Bangladesh bank keeps its funds at the Fed, this transfer of money had to go through the Fed before being approved.

Unfortunately, the Fed frequently only reviews payments after they have gone through. This is how the $81 million disappeared. By dumb luck, the fraudulent orders contained the word “Jupiter”, which also happens to be the name of an Iranian ship currently sanctioned by the United States. This raised flags that caused the transfers to be more carefully scrutinized, and is the only reason the attackers didn’t make off with the full billion.

Because the investigation is ongoing, details about how these credentials were stolen are still somewhat speculative. However, there are some good clues. Security at the Central Bank of Bangladesh was very lax. Their computer systems did not even have a firewall. Malware was found on many of the machines, and some of the malware was linked to participating in the attack. Speculation has it that a trojan that exploits Microsoft Word macros to steal credentials was responsible for much of the attack. Additionally, it is believed that the attackers might have had some inside help. Whether this was an insider who was intentionally helping or an employee who was negligent in security practices is unknown.

What can be learned from this incident? There are quite a few things that could have prevented this attack. First of all, the payments approved by the Fed were all extremely unusual. The fed received 20 times as many payment requests from Bangladesh on the day of the attack than is normal, and many of them even had formatting errors. Further, the payments were to individual accounts, which is extremely abnormal. If the Fed had real time checking in place to look for unusual patterns, the attack would never have worked and no money would have been lost. And on the Bangladeshi side, poor security practices all around led to a very wide attack surface for hackers to exploit.

Perhaps the worst part of this is that the Bangladesh government is not releasing their report on this incident. Several other banks have been targeted by similar attacks, and since Bangladesh is not releasing their findings, other banks are in the dark as to what parts of their security systems to beef up.

There is one element of good to come out of this. The committee that runs the SWIFT messaging system is requiring banks that use their system to follow stricter security guidelines so that attacks like this are less likely in the future.

Sources:

<http://www.reuters.com/investigates/special-report/cyber-heist-federal/>

<http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO>

<https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>

<http://www.reuters.com/article/us-cyber-heist-bangladesh-exclusive-idUSKBN13X1S4>

<https://www.bloomberg.com/news/articles/2016-05-10/bangladesh-bank-heist-probe-said-to-find-three-groups-of-hackers>

<http://www.bankinfosecurity.com/bangladesh-bank-heist-probe-finds-negligent-insiders-a-9586>

<http://www.economist.com/news/finance-economics/21707719-government-claims-publishing-report-would-undermine-efforts-retrieve>

<http://www.straitstimes.com/business/dridex-malware-linked-to-bangladesh-heist>

<http://www.philstar.com/headlines/2017/01/06/1660122/year-hackers-bangladesh-bank-heist-comeleak>