Case Study Report

Bangladesh Bank Heist 2016

Group Name: Ontija x2

Dejan Simonovic	723125
Waqar Abbas	661342
Wessam Koraim	722265
Ahmed Massoud	722508

1. Introduction:

There is an ever increasing risk of financial services and institutions being victim of a cyberattack, because a successful attack on these institution can yield a lot of reward. As the saying goes, “the bigger the risk - the bigger is the reward”, these institutions targeted by many non state and in some cases state actors who are looking to score big and finance their own agendas. According to an estimation, financial institutions are 300 times more likely to be attacked than any other business with an online presence. The possibility of cyber attacks on financial institutions and firms have driven them spent more and more on prevention from these attacks, 18 million dollars per firm versus 12 million dollars for firms across all industries. In other words, a normal american business experiences a cyber attack four million time per annum, while an american financial business faces a huge number of almost a billion attacks per annum.

One billion cyber attacks per annum is a remarkable number to be faced by an institution, but the US Postal service wa attacked almost four billion times in 2016, which was, according to reports, used as a backdoor to attack rest of the departments operated by US government. One billion attack per annum amounts to almost over 2000 attack a minute or over 30 attacks during a single tick of a clock. During the past five years, the number of attacks, weather for the theft of money or the sensitive data owned by financial institutions have nearly increased three times

Financial institutions have always been the primary customers of cybersecurity technology vendors and expertise. Consumer data and enormous credit to be moved around has made them a target for cyber criminals. The treat for financial disaster, reputation damage, regulatory consequences in the face of cyber attack, has motivated them to invest in the field and cybersecurity defensive capabilities.

Banking and cybersecurity are getting more intertwined. New vulnerabilities are discovered daily and new exploits are emerging at very fast pace. In addition, consumers have been given many diverse ways for interacting with their money which, if not done properly and secured, can prove disastrous, for both client and the bank.

The big question is how do you successfully target a financial institution and manage to get away with digital booty of almost billion USD? This requires time, extensive organization, expert specialized individuals, and exploiting your target’s weak spots, which is usually the human error.

Over a weekend in the beginning of February 2016, a band of unknown cyber criminals instigated a cyberattack on Bangladesh central bank in Dhaka, and managed to initiate unauthorized transactions of a staggering amount of almost $951 million. Although most of the money was eventually recovered, several transactions did get through resulting in the loss of $81 million. This single event is considered to be one of the biggest bank heists seen in the modern time.

The thieves were well organized and equipped, had well managed funding, and were patient in preparing the exploitation of the bank's vulnerabilities. Their success was mostly contributed to exploiting the weaknesses in the institution they robbed.

2. What Happened:

On Thursday, Feb. 4, 2016 at Bangladesh's central bank the programmed printer, which is connected to the SWIFT software, was not working, where this printer's main goal was to print out real-time transactions, but that day the director of Bangladesh's central bank noticed it was not working, as usually a plenty of transactions are printed each day. The director assumed it is a glitch, so he decided to fix it on Sunday, which is the start of week in Bangladesh.

On Sunday, Feb. 7, 2016, the bank's employees were doing their best to get the printer to work again and after lots of trials, they managed to get it to work, and they rebooted the printer. Soon after fixing the printer issue transactions started printing out one after the other. The printer was printing too many transactions than expected, and soon the director alongside with the employees noticed that something was not right. After focusing a bit, they discovered 35 doubtful payment orders for enormous amounts of money, that have transferred from Bangladesh's central bank private account to many other accounts to several other nations. Shockingly, no person working in Bangladesh's bank have given green light for these payment orders, what added more confusion is that the SWIFT security system was unhackable, as it has military grade security, however it was not functioning too. Each time the bank's director tried to open it, an error message appeared, saying "A file is missing or changed". The director and his/her colleagues gathered around the dedicated Swift computer, following directions on the monitor on how to restart the software to run normally as before. Shortly after noon, the director recovered three messages from the Federal Reserve Bank of New York.

The payment orders totaled to almost 1 billion US dollars (951 million US dollars). The director's response to the incident was delayed because of the malfunctioning printer. After investigations it turned out that one month before the theft that an employee at the Bangladesh bank was checking his/her email at work, it seemed to the employee that there was nothing out of the ordinary. However, the employee unknowingly opened a malware program through a faulty email, which on the spot starting setting up an infected program in the bank's security system. This program allowed the tresspassers to gain access to bank's network and confidentials of the bank, and within the month before the incident the intruders were studying the bank's operation and routine. After a month, on Thursday, Feb. 4, 2016, the hackers managed to enter the bank's system for the last time. The cybercriminals entered the system in order to issue payments through the SWIFT network, which they managed to get the credentials for from the malware installed a month ago, moreover, these issued payments were legitimately issued as they are being issued from the bank itself.

Analyzing the issued payments, they were 35 transfer requests totalling 951 million US dollars to the Federal Reserve Bank of New York. The hackers chose the Federal Reserve Bank of New York as Bangladesh's Bank has an account there with loads of money to be used for international agreements. These 35 transfers were for sending money from New York to several accounts in Asia.

Next day, Friday, Feb. 5, 2016, in New York the Federal Bank was busy processing the transfer requests of Bangladesh's bank, and the Fed Bank did not have any reason to stop the transfer as it is issued by SWIFT instructions which are completely legitimate.

As mentioned in the second paragraph the Bangladesh's bank employees figured out the 35 suspicious transfers after fixing the printer, and getting the SWIFT security system to work properly. However, Bangladesh's bank got really lucky as New York's bank has flagged 30 of these transfer requests for manual review, this happened because in one of the SWIFT orders there was coincidentally a name of a shipping company that have been blacklisted for political reason between US and Iran, which was complete luck in favor of Bangladesh. As a result, 871 million USD worth of transfers have been blocked. However, there were still 101 million USD worth of transactions that has not been stopped.

Regarding the rest 5 transactions, the first one was a transfer to some NGO in Sri Lanka, however this request have routed through a German bank in Frankfurt, and fortunately the German account noticed something suspicious with the transfer because there was a spelling mistake in the name of the NGO which later turned out to be a fake

NGO, the spelling mistake was writing “Fandation” instead of “Foundation”. Moreover, this transfer which was sent to Pan Asia Bank in Sri Lanka was also noticed to be suspicious from the side of Pan Asia Bank because it was worth of 20 million USD which is an enormous transfer for an NGO. As a result, an employee sent back the transactions for further verification to the German bank, which then noticed the spelling mistake as mentioned and therefore the transaction was sent back to the New York Bank for further confirmation and hopefully the money was retrieved back.

Finally there 4 remaining transactions that could not been traced as these transactions were headed to a bank in the Philippines. This was also planned by the hackers, because after the transaction has been sent to the Philippines the New York Bank sent a request to the this bank, however because of the new Chinese year celebration in the Philippines timing was not in favor of the Bangladesh’s bank, and the money was quickly laundered into casinos and cash, and hence it was untraceable.

3. Threat Analysis:

Usually hackers try to steal individuals banking credentials but in our case the hackers aimed for a higher goal, the hackers were targeting the source of all money in bangladesh even worse, getting access to the SWIFT network connected device .

Firstly, let's explain what SWIFT means. It stands for The Society for Worldwide Interbank Financial Telecommunication (SWIFT) which is essentially a secure network for enabling governments and financial institutional worldwide to send and receive information about financial transactions securely and reliably.

According to wikipedia “The majority of international interbank messages use the SWIFT network. As of 2015, SWIFT linked more than 11,000 financial institutions in more than 200 countries and territories, who were exchanging an average of over 32 million messages per day. SWIFT has a highly secured network. However, it doesn’t hold responsibility for the security of its customers’ local SWIFT infrastructure, although it does provide assistance to ensure customers are able to manage cyber attacks.”

Unfortunately the security measure at the bangladesh bank wasn’t good enough to stop this attack which has been patiently executed over a full year period.

The attacker managed to get into the network through one of the employees mistake by opening an email that allowed them to install their malware into the computer then deployed a trusted windows software to monitor the bank employees activities. Using this initial foothold, attackers were able to move laterally across the bank's internal network, they managed to compromise 32 systems before getting to the systems connected to SWIFT network.

On these devices the hackers managed to get the local admin credentials and installed more monitoring software to learn how financial messages were sent and identify the different services and capture swift credentials and that was what they needed to initiate their transactions requests.

And to make sure that their operation won't be discovered they manipulated the printer connected to the swift system and prevented it from printing anything which made it easier for them initializing their requests without being caught.

But the question is How could the bangladesh bank prevent or reduce the damage of this attack. They should have improved their security in many ways to not allow some stages of this attack.

For example awareness for the employees that security starts with them and how they should not use, open external websites that could be suspicious, so a little bit of knowledge could have prevented the bank a loss of 81 millions dollar. Also this awareness will teach them not to use easy passwords just to be able to remember them.

Also if the security experts in the banks made sure that they have good softwares that discovers malware and prevent them from being initiated that could have been an easy way to stop all this despite the human error. Another thing that security engineers at the bank could have done is removing admin rights from users so they can't install any softwares on their computer unless they get the credentials for the administrator and make sure that these credentials are unique and not reused between all the machines to avoid giving away access to everything once these credentials are compromised.

Also changing the credintional from time to time could have helped in preventing the hackers from keeping their access in the network for a long time, also if they had a chance to use multi factor authentication as a way to authenticate to the systems, it

could have made it impossible for the hackers to get in the network or get higher privileges in the network easily.

Another critical thing that should have been done is isolation for the important parts in the network for example the SWIFT part and making sure that there can not be any external access to these segments in the network.

Finally Monitoring the users' accounts activities and the network behaviour to be able to predicate and fight threats and also spot the weird or suspicious behaviours in the network that could have helped in preventing this horrible loss for the bank and also for the country.

4. The Aftermath:

Electronic money transfer ended up in Philippines, where it was laundered and transformed to a cash using casinos. In the Philippines, two Chinese man were held accountable for opening fake accounts, but they were just middlemen. Still, they were crucial part of further investigation. The authorities believed that middlemen could lead them to the true culprits, but they fled to Macao where it was impossible to track them.

Despite hackers' efforts to delete traces of malware activities, malware was not completely removed, and cybersecurity experts were still able to conduct the analysis of the malicious code. Analysis conducted led experts to believe that this group was probably responsible for many similar attacks on financial institutions around the globe. Assigning privileges was obviously not done correctly and this incident clearly showed the role of privileges in serious security breaches. It also put the emphasis on the importance of proper security practices.

Malware was sent probably by email. It collected passwords and usernames and was able to cover its own tracks. Bangladesh Bank systems were compromised by attackers and applications were modified so that attackers got access to the bank's SWIFT terminals, which transfer payment orders between organizations and countries. With bank credentials in their possession, hackers managed to access SWIFT system.

SWIFT is a corporate organization owned by the banks that use it. Hackers used SWIFT messaging system to send messages to the Fed. The realization was always that SWIFT weak points are at the end points in the banks. It was recognized that banks need to take care of their own physical as well as cybersecurity. In the SWIFT

announcement, it was said that there was no indication of possible compromise of SWIFT core messaging service. Customer security program was launched in 2016 to help customers in reinforcing local security of their SWIFT related infrastructure.

Bangladesh bank could have avoided the attack or at least control the extent of the damage, if it had implemented several necessary controls. Recommended actions could be: controlling applications to reduce risk of malware, removing local admin rights and make credentials unique, securing privilege account credentials and change them on a regular basis, using multi factor authentication as widely as possible, segmenting network and isolating all remote access and monitor all remote access to highly sensitive systems to detect threats. With taking all these steps and by prioritizing the security of privileged accounts, bank could have been able to stop attackers from performing the heist.

All institutions connected to the heist deny their responsibility. However, they took some steps for improving their cybersecurity.

There was still question about responsibility. There must have been someone, who was to blame for this event. Bangladesh Senate performed an inquiry on money laundering, but Bangladesh Bank denied that anyone from inside the bank was involved and also denied negligence. No one was charged by the police in Bangladesh.
Several possible directions of inquiry were opened. This event could be caused by one or many combined factors.

Many questions arose: how malware got activated inside bank's internal system and is this the critical mistake of one person? Were security policies to blame and is bank itself responsible for keeping its infrastructure safe and secured? What is the responsibility level of bank branch manager?

Very little is publicly known about the person who triggered the event. It might be deliberate act of bank's employee. However, this assumption was quickly abandoned, and attention was brought towards bank manager.

Accounts in RCBC bank in Philippines were opened by the branch bank manager. She knew about the regulations and bank policies. She opened the accounts on the recommendation of Manilla casino owner for individuals who had fake identities. She claimed to have opened five accounts for some individuals with a promise that significant amount of money will come there.

Casino owner denied that, stating that he has nothing to do with money which came in the country and that he was only referring these four individuals to the bank manager. For failing to comply with bank regulations, RCBC bank was fined with significant amount.

Senate report documented timing of the payments, many of which were just minutes from each other. Bank manager's lawyer stated that when funds were received, she checked the remittance validity with the head office and received emails confirming they are from valid sources. It was said by her lawyers that she did not have authority to unilaterally prevent fund transfers.

From RCBC, money went to the Phil Gram remittance company, from where money was laundered through casinos. One stumbling block in an investigation was the unusual level of privacy afforded to bank accounts due to the existing Bank Secrecy Act which prevented investigators of getting anybody's account. Casinos were often used to convert electronic money into cash, though in this case there is no evidence that casino or its owner knew that the funds were stolen. At the time, casinos were not covered by money laundry laws and were not obliged to report large transactions.

Some recommendations were made to extend the reach of money laundering law and to provide easier access to bank accounts. Federal Reserve New York flagged some of the transactions as suspicious due to mentioning of the name Jupiter in transactions orders which coincidentally corresponded to name of the Iranian tanker. Another reason for suspicion was that these payments differed significantly from usual payments made by Bangladesh bank. Payments were not formatted properly and were payments to individuals rather than to organizations.

Large amounts of the payment requests that come to Fed are automatically executed because they are SWIFT authenticated. Fed staff had some concerns about the payments, but the timing was just not right for inter-bank communication. Though the Fed systems were not compromised, this event was seen as an opportunity to further strengthen the security of global payment system. Federal Reserve bank claimed it has been performing screening of and diligence on funds transfers.

Since no one was deemed responsible for causing the loss, question remains of how to tighten the security in a way that will prevent such attempts in the future. That is where cybersecurity strategy comes into play with special focus on risk management, cybersecurity awareness and preparedness.

5. Strategies to prevent future attacks:

In this day and age of globalization, almost every business/organization of moderate to high footprint in the world, has an online presence. This helps them to reach their customer in every nook and corner of the vast market. This presence makes them vulnerable to cyber attacks that can cause financial and sometimes non financial damages, such as decrease in company value in the eyes of its existing customers, losing future perspective customers, damage to public relations. Sometimes these damages can go as far as bankrupting the victim institution. Such serious threat requires measure to safeguard and prevention of such attacks, and investing both time and capital in the technology which will help achieve this goal.

Following strategies could be applied by the victim institution of this case study, Bangladesh Bank, to prevent any similar attack in the future.

- Control applications to prevent malware:

  The applications could updated with features that would be able to detect and prevent the execution of malware by restricting the application permissions or by using other similar methods. Email servers can be configured to scan the attachments and disable the hyperlinks in the email to prevent accidental executions. Unknown attachments or hyperlinks associated with lesser known domains could be tagged or reviewed by experts.

- Remove local admin rights and make credentials unique:

  Sometimes the institutions make a local administrator account to handle all high risk tasks and that account is usually used by many employees who have to perform those tasks. This presents a risk of credentials leaking out and paints a bullseye on the back of the institution. So the institution need to remove the local admin rights and make the credentials unique for every terminal.

- Secure, rotate and control access to privileged terminals:

  The institution need to rotate and change credentials of secure terminals periodically. This period can be as low as daily change in credentials. This will prevent and leakage of credentials and will resist and long term attack as discussed in this study.

- Use multi-factor authentication:

The use of this technique is quite common today where a user who want to login into his account also has to verify his identity via another method, either through email or SMS authentication. This method can also be implemented by using two keys, one for the employee who wants to access a secure terminal and one for the manager who would have oversee the tasks being done on the secure terminal.

- Segment networks and isolate remote access:

  The network to which the secure terminals are connected can be segmented so they could no be accessed by the the terminals which exists in the other segments of the network. Furthermore remote access should be disabled for the secure terminals so that they cannot be accessed from outside the institution network, and even from outside their network segment which they do not belong to.

- Monitor user and account activity to detect threats:

  The institution should monitor user and account activities to rule out the possibility of and inside attack. The activities can be monitored via number of higher level applications.This would provide a much needed window to act fast and stop the unknown or unauthorized task in its track.

- Active intrusion Detection:

  The institution also need to invest in intrusion detection and prevention technologies. The institutions network could be monitored for any unusual activity that can amount as a cyber attack, and could be stopped before it incurs irreversible damage.

- Building Resiliency:

Technology and expertise that can help in building the secure wall around the network of the institution is also available to hacker who can exploit it for their own needs. Cyber attack techniques are becoming more and more sophisticated with the passage of time. Nowadays the cybersecurity professionals don't ask the question “if we are hacked” but rather “when we are hacked”. So the institutions needs to build up protocols and process that it will follow in case of a cyberattack.

- Cybersecurity awareness:

Besides investing into technology and expertise required to build up cyber defense around the institution, it is also necessary to invest into awareness and training of all employees regarding cybersecurity do’s and don’ts. No matter how state of art

technology any institution have deployed, it could still fall down like a house of cards with a single human error.

6. Conclusion:

Bangladesh bank was hit for almost 1 billion dollars of taxpayer money which is not a small amount for thirld world country like Bangladesh. It is hard to determine whether it was a stroke of luck of deliberate use of sanctioned companies to funnel out the money but it saved almost 90% of the amount by being tagged at New york band and Deutsche bank. Another thing of note is that the malware was present in Bank's network for a long time and took its time and was used by the unknown hackers to plan and strategize the perfect moment to strike against the bank. SWIFT network is considered to be secure and used by almost all the financial institutions around the world, but here it was exploited to carry out the attack. This can be an example of the "the chain is as strong as its weakest link". Investing in a protective cybersecurity technology is important in this day and age but investing in cybersecurity knowledge and process and teaching them to the human resource is equally important, because no matter how advanced and state of the art technology is, it is still operated by human beings who are prone to error.

Bibliography:

1. Society for Worldwide Interbank Financial Telecommunication, Wikipedia https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication

2. SWIFT Systems and the SWIFT customer security program. https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf
3.