Bangladesh Bank Cyber Heist: Incident Analysis

Ramkumar Balu
rbalu@gatech.edu

1 INTRODUCTION

In one of the largest cyber heists that took place in February 2016, the Central Bank of Bangladesh (Bangladesh Bank) lost $81 million from its account held in Federal Reserve Bank of New York (Mazumder & Sobhan, 2021). The hackers originally attempted to steal a whopping $951 million in a well-planned sophisticated attack. They compromised the bank's network and navigated the SWIFT[1] gateway to send 35 fraudulent fund transfer requests on behalf of the bank.

This paper applies Diamond model of Intrusion Analysis on the discussed cyber incident. In the later part, the paper discusses policy assessment at various levels as well as the policy impact that happened in response to the incident.

2 APPLYING THE DIAMOND MODEL

Diamond model is a simple yet powerful analytic tool that serves as a formal method for intrusion analysis (Caltagirone et al., 2013). As shown in Figure 1, the four vertices of the diamond (core features) correspond to adversary, capability, infrastructure, and victim, while the edges represent the relationship between them.

2.1 Core Features

2.1.1 *Adversary*

BAE systems was the first to find similarities between Bangladesh Bank (BB) heist and Sony Pictures Entertainment (SPE) hack that happened in 2014 (BAE Systems, 2016a). Kaspersky, after a yearlong investigation, published a report linking "*Lazarus Group*[2]" to the BB heist (Kaspersky, 2017).

Adversary Operator— Private cybersecurity companies such as Kaspersky, BAE systems, and Symantec Corp attributed the attack to Lazarus group. The FBI filed

[1] Society for Worldwide Interbank Financial Telecommunication (www.swift.com)
[2] North Korea based Advanced Persistent Threat (APT) group

criminal complaint against one of the members of the group, Park Jin Hyok (U.S. v. Park, 2018).

Adversary Customer—The FBI and NSA alleged that the attack was carried out on behalf of the North Korean government based on its similarities with SPE hack (Elias Groll, 2017; U.S. v. Park, 2018). However, the North Korean government denied all the allegations.

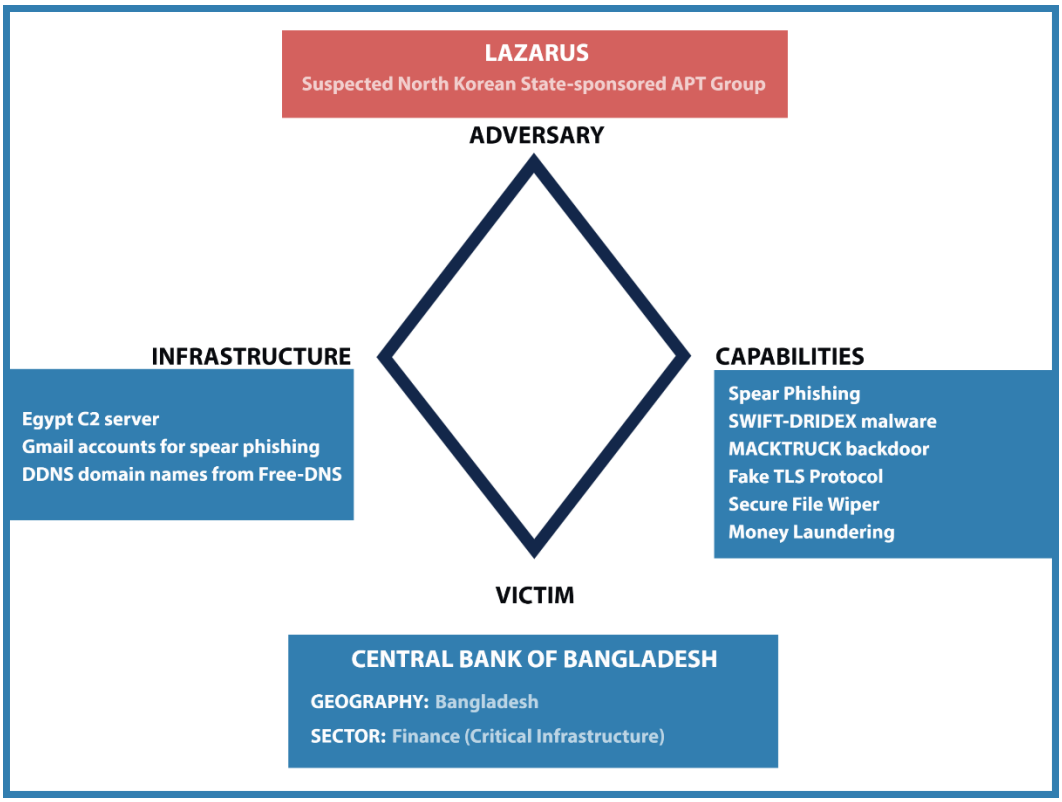


Figure 1—Diamond Model for Bangladesh Bank Cyber Heist

2.1.2 *Capability*

The attack used highly sophisticated tools and techniques which suggested that the adversary is an APT group. The various capabilities used against the Bangladesh Bank are as follows,

- **Spear Phishing** – For initial access to the bank's network, the hackers used job application themed[3] spear phishing emails with malicious attachments (U.S. v. Park, 2018).

[3] Same tools and techniques used in Sony Pictures Entertainment hack (2014).

- **Command and Control** – The adversary used C&C servers and had direct control of the infected systems using a backdoor.
- **SWIFT-DRIDEX** – The attackers developed a custom malware based on DRIDEX to interact with victim's SWIFT Alliance Access software (BAE Systems, 2016b; Basoya & Arora, 2020). The malware helped them send fraudulent payment requests and cover traces by tampering SWIFT responses.
- **Fake TLS Protocol**[3] – Custom network protocol developed to mimic TLS traffic to bypass network security measures (DiMaggio, 2022).
- **Secure File Wiper** – A unique file wipe-out module was used to erase traces (BAE Systems, 2016a).
- **Other malwares** – The forensic analysis found traces of malwares codenamed NestEgg, Macktruck[3] and Sierra Charlie[4] that were used for lateral movement, persistence, and backdoor access (U.S. v. Park, 2018).
- **Money laundering** – The attackers made the stolen money disappear by running it through a Philippine bank and a few casinos.

2.1.3 *Infrastructure*

The BAE Systems investigation revealed an Egypt IPv4 address (shown in Table 1) that was used as C&C in one of the malwares (BAE Systems, 2016b). The IP address location suggests that it could be a compromised host or controlled by an intermediary (type 2 infrastructure).

Forensic review of an infected computer at BB revealed two domain names, whose DDNS[5] accounts were later linked to Lazarus (U.S. v. Park, 2018).

The FBI found email addresses used by the adversary to send spear-phishing emails (infection vector) and perform reconnaissance on BB employees (U.S. v. Park, 2018).

[4] Shares common framework with Brambul worm used in SPE hack (2014).
[5] Dynamic DNS

Table 1 — Attacker Infrastructure

Infrastructure	Type	Service Provider
196.202.103.174	Type 2	TE Data, Egypt
mlods[.]strangled[.]net bepons[.]us[.]to	Type 1	Free-DNS[6]
yardgen[at]gmail.com agena316[at]gmail.com watsonhenny[at]gmail.com rasel.aflam[at]gmail.com rsaflam8808[at]gmail.com	Type 1	Google

2.1.4 *Victim*

Victim Persona – Bangladesh Bank is the central bank of Bangladesh owned by the nation's government.

Victim Asset – Victim assets in this case include workstations belonging to the Bangladesh Bank, SWIFT Alliance Access software, and Bangladesh Bank's funds (end-target) held in NY Federal Reserve Bank.

2.2 Meta-Features

2.2.1 *Timestamp*

Although the final phase of the attack happened between February 4–5, 2016, the investigations revealed that the attackers entered the bank's network a year before (U.S. v. Park, 2018).

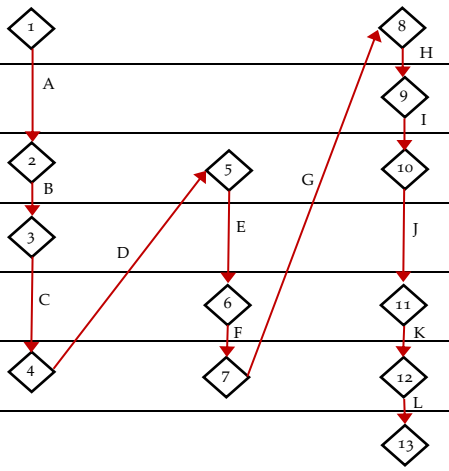
2.2.2 *Phase*

The attack included most of the phases of cyber kill chain with some phases executed multiple times. For example, after initial foothold, the attackers further learned about the internal banking infrastructure and delivered customized

[6] Free DNS - https://freedns.afraid.org/

malware that interacted with the SWIFT gateway. The phases are illustrated in a simplified activity thread shown in Table 2.

Table 2 — Simplified activity thread illustrating Lazarus group's attack against Bangladesh Bank. The Diamond events 1 through 4 represent the initial access through spear phishing. The events 5 to 7 represent backdoor installation whereas 8 to 13 represent the SWIFT compromise using DRIDEX malware.

	Lazarus Group
Reconnaissance	
Weaponization	
Delivery	
Exploitation	
Installation	
C2	
Action on Objectives	
	Bangladesh Bank

2.3 Social-Political Meta-Feature: Adversary-Victim Relationship

The Bangladesh Bank incident is a straightforward robbery where cybercriminals dared to steal almost a billion dollars from a central bank's reserve. There are interesting speculations on the adversary's motivation. Among several alleged crime-for-profit activities of the North Korean state, the superdollar (counterfeited U.S. currency) alone was estimated to have generated a profit of at least $15 million per year (Perl & Nanto, 2007). After earnest efforts by U.S. including 2013 redesign of dollar notes, the circulation of counterfeit currencies was greatly reduced (Buchanan, 2020). To continue its high defense spending including development of nuclear weapons and ICBMs, the central command economy had to do better.

Persistent Relationship – In Bangladesh Bank incident, the adversary was more towards the *Enduring* side in the Degree of Persistence spectrum. The hackers were inside the Bank's network for almost a year and used capabilities to not get detected.

Victim of Interest vs Victim of Opportunity – The Bangladesh Bank was a victim of Interest. While aiming for a billion dollars, there are only handful of entities to rob such as central banks.

Shared Threat Space – Financial institutions with access to fortunes fall under the same threat space. In fact, after BB, the same adversary was found to have attacked a bank in Philippines (Symantec, 2016).

2.4 Technology Meta-Feature: Connecting Infrastructure and Capability

The malwares used in Bangladesh Bank attack seems to be part of a wider attack toolkit. The MACKTRUCK malware which was used to have backdoor access to the bank's workstations, communicated with C&C servers using a protocol disguised as TLS traffic (Kasza & Yates, 2017). The malware used popular domain names to create fake TLS handshake sessions with the C&C server. This made the network traffic look legitimate. The underlying data exchange with the C&C used HTTP REST standard.

The DRIDEX based malware which was used to control the SWIFT Alliance Access software had an encrypted config file (BAE Systems, 2016b). The malware behavior was highly configurable such that it can be easily reused for similar attacks in future. The malware monitored SWIFT events and periodically communicated them to the C&C using HTTP REST messages (BAE Systems, 2016b).

3 POLICY ASSESSMENT

In response to the 2016 Bangladesh Bank heist, policy changes occurred at organizational and industry level. However, there were little to no public policy changes at the national and transnational level where it could be more effective.

3.1 National Level

Bangladesh, since 2013, has seen an increasing trend in cyber-attacks especially against its financial sector (Kundu et al., 2018). The risk posed by these threats to financial sector are very severe. If all the fraudulent transactions totaling to

almost $1 billion were successful, it would have been disastrous to the Bangladesh economy, whose GDP in 2016 was approximately $221 billion[7]. The Government of Bangladesh had launched "National Cybersecurity Strategy[8]" in 2014 (Md. R. Uddin, 2017). However, no immediate public policy change could be seen in response to the 2016 bank heist.

Although the National Cybersecurity Strategy talks about critical infrastructure, more work to be done on prioritizing nation's critical infrastructure security. A central agency, like U.S. CISA, can be set up to coordinate with critical infrastructure providers, improve situational awareness and build resiliency towards cyber threats.

Moving millions of dollars across borders is not trouble-free. Yet, major part of the stolen money is still not recovered. The attackers used old school money laundering techniques to vanish the stolen funds (Katz & Fan, 2017). The stolen funds were initially transferred into 4 accounts in RCBC[9] Bank and were routed through several casinos in Philippines. In 2016, casinos didn't come under AMLC[10] scrutiny in Philippines (Hofilena & Sy, 2017). It is evident that Philippines needs to tighten its Anti-Money Laundering (AML) laws and ease bank secrecy law to be on par with international standards.

In response to the incident, the AML act was amended to include casinos (*Republic Act No. 10927*, 2017). Hofilena & Sy (2017) propose further amendments including granting AMLC the authority to issue *ex parte* freeze order directly rather than going through several court procedures.

3.2 Transnational Level

At the transnational level, there is scope for improving cyber-attribution. When nation states are involved in cyber-attacks, correct attribution is critical for geopolitical accountability and deterrence (Mueller et al., 2019). However, assigning responsibility to a state is not simple, especially when states contract out attacks through APT groups. Microsoft, in its Digital Geneva Convention proposal, called for a neutral international organization to attribute state-sponsored attacks (Microsoft, 2017). RAND corporation advocated for a Global Cyber

[7] Data from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=BD
[8] https://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf
[9] Rizal Commercial Banking Corporation, Philippines
[10] Anti-Money Laundering Council, Philippines

Attribution Consortium independent of nation-states (Davis et al., 2017). The need for such a neutral expert group is evident so that the attributions are taken seriously by the international community.

Regarding law enforcement efforts, Bangladesh has no existing MLA treaty with Philippines. Philippines claims that their AMLC coordinated regularly with financial intelligence of Bangladesh. However, Katz & Fan (2017) claims that the gamblers were allowed to continue their casino play even after Bangladesh officials called Philippines for help. Though eventually the remaining funds were frozen, it was too late. This shows the importance of MLA treaties with emphasis on immediate action for ongoing crimes.

3.3 Industry Level

Although the attackers didn't exploit any vulnerabilities in the SWIFT payment network, the incident demanded response from the Belgian cooperative society. SWIFT can mandate standards at the industry level through private contracts like ICANN[11]. In 2017, the SWIFT provider launched Customer Security Program (CSP) in response to the Bangladesh Bank incident (SWIFT, 2017). As part of CSP, the SWIFT published Customer Security Controls Framework (CSCF) that includes mandatory and advisory security controls for its customers. Participants are needed to attest their level of compliance annually.

Also, after three years, in 2019, SWIFT Payment Controls feature was launched that performs real time validation of payment messages according to the policy set by the customer (SWIFT, 2019). SWIFT claims that it can identify uncharacteristic payments that could be a threat.

3.4 Organizational Level

Shortly after the incident, BB announced that it is planning to set up an internal Cybersecurity Unit (CSU) to oversee IT system security (A. Z. Uddin, 2016). It took nearly 3 years to establish CSU which is now responsible to manage cyber risk, strengthen the security policy and formulate implementation plan for BB (Bangladesh Bank, 2019).

[11] Internet Corporation for Assigned Names and Numbers

4 CONCLUSION

The Diamond Model analysis demonstrated the features of the event as well as the relationship between them. The policy assessment provided useful insights into the policy gaps at various levels.

5 REFERENCES

1. BAE Systems. (2016a). *CYBER HEIST ATTRIBUTION*. https://baesystemsai.blogspot.com/2016/05/cyber-heist-attribution.html
2. BAE Systems. (2016b). *TWO BYTES TO $951M*. https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html
3. Bangladesh Bank. (2019). *CYBER SECURITY UNIT*. https://www.bb.org.bd/en/index.php/about/deptdtl/78
4. Basoya, A., & Arora, M. (2020). *Deciphering the SWIFT-DRIDEX relationship in Bank*. https://dl.packetstormsecurity.net/papers/general/Deciphering-SWIFT-DRIDEX.pdf
5. Buchanan, B. (2020). *How North Korean Hackers Rob Banks Around the World*. Wired. https://www.wired.com/story/how-north-korea-robs-banks-around-world/
6. Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. *Threat Connect*, *298*(0704).
7. Davis, J., Boudreaux, B., Welburn, J., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. (2017). Stateless Attribution: Toward International Accountability in Cyberspace. In *Stateless Attribution: Toward International Accountability in Cyberspace*. https://doi.org/10.7249/rr2081
8. DiMaggio, J. (2022). Hunting and Analyzing Advances Cyber Threats. In *The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*. No Starch Press.
9. Elias Groll. (2017). *NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist*. Foreign Policy News. https://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/
10. Hofilena, J. G., & Sy, J. L. (2017). Gone without a Trace: A Re-Examination of Bank Secrecy Laws and Anti-Money Laundering Laws in Light of the 2016 Bangladesh Bank Heist. *Ateneo Law Journal*, *62*(1), 90–140.

11. Kaspersky. (2017). *LAZARUS UNDER THE HOOD*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
12. Kasza, A., & Yates, M. (2017). *The Blockbuster Sequel*. Palo Alto Networks, Unit 42. https://unit42.paloaltonetworks.com/unit42-the-blockbuster-sequel/
13. Katz, A., & Fan, W. (2017). A Baccarat Binge Helped Launder the World's Biggest Cyberheist. *Bloomberg Markets*. https://www.bloomberg.com/news/features/2017-08-03/a-baccarat-binge-helped-launder-the-world-s-biggest-cyberheist
14. Kundu, S., Islam, K. A., Jui, T. T., Rail, S., Hossain, M. A., & Chowdhury, I. H. (2018). Cyber crime trend in Bangladesh, an analysis, and ways out to combat the threat. *International Conference on Advanced Communication Technology, ICACT*, *2018-February*. https://doi.org/10.23919/ICACT.2018.8323800
15. Mazumder, M., & Sobhan, A. (2021). The spillover effect of the Bangladesh Bank cyber heist on banks' cyber risk disclosures in Bangladesh. *The Journal of Operational Risk*. https://doi.org/10.21314/jop.2020.249
16. Microsoft. (2017). An attribution organization to strengthen trust online. In *Microsoft Policy Paper*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI
17. Mueller, M., Grindal, K., Kuerbis, B., & Badiei, F. (2019). Cyber Attribution: Can a New Institution Achieve Transnational Credibility? *The Cyber Defense Review*, *4*(1).
18. Perl, R., & Nanto, D. K. (2007). North Korean Crime-for-Profit Activities (February 16, 2007). In *CRS Report for Congress (RL33885)* (Issue RL33885).
19. *Republic Act No. 10927*, (2017). https://www.officialgazette.gov.ph/2017/07/14/republic-act-no-10927/
20. SWIFT. (2017). *Customer Security Programme (CSP)*. https://www.swift.com/myswift/customer-security-programme-csp
21. SWIFT. (2019). *Three years on from Bangladesh*. https://www.swift.com/news-events/webinars/three-years-bangladesh
22. Symantec. (2016). *SWIFT attackers' malware linked to more financial attacks*. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8ae1ff71-e440-4b79-9943-199doadb43fc&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

23. Uddin, A. Z. (2016). BB to set up cyber security unit. *Newage Business*. https://www.newagebd.net/article/843/bb-to-set-up-cyber-security-unit
24. Uddin, Md. R. (2017). The National Cybersecurity Strategy of Bangladesh: : A Critical Analysis. *Journal of International Affairs, 21*(1 & 2).
25. U.S. v. Park. (2018). *UNITED STATES DISTRICT COURT CENTRAL DISTRICT OF CALIFORNIA*. https://www.justice.gov/opa/press-release/file/1092091/download