HACKED Documentary Analysis and Review

Robert Crager

Collin College

Abstract

The movie documentary HACKED based on a true story surrounding the attack on Bangladesh Bank in 2016 sheds light on one of the biggest cyberattacks to date. Attackers perfectly planned this heist to steal over 80 million dollars over a 2–3-day period, during a holiday where bank employees would have a 3-day weekend. The nation-state-sponsored attackers were able to attack with great scope and complexity, but the security community should have seen this attack coming and prevented something like this from happening.

The year is 2016, Bangladesh is one of the poorest countries in the world, but part of its critical infrastructure, the Bangladesh bank, is keeping the country alive and thriving. However, everything is about to change, the Bangladesh bank is about to experience the biggest cyber heist the world has ever seen. It was February 4, 2016, Bangladesh bank employees are heading home for their 3-day weekend ahead of them because of a Muslim holiday. Everyone leaves the office and doesn't look back as they begin their 3-day weekend. Meanwhile, hackers are infiltrating the Bangladesh bank's network and preparing for one of the biggest cyber heists of the century.

Hackers of the Bangladesh bank managed to intrude into their network and steal approximately 80 million dollars before the following Monday morning when Bangladesh bank was finally able to stop the fraudulent transactions. The malicious actors were able to later launder and wash over 80 million dollars of stolen money. They managed to attack and steal this much money from one of the most heavily guarded banks in the world. The issue, of course, was that the bank was only heavily guarded in a physical manner, not guarded through traditional digital mechanisms but, as the narrator of the film put it, "sometimes physical barriers aren't enough" (3:30). The attackers managed to perfectly time the entire heist to avoid detection and escape with the cash.

The entire heist was premeditated and consisted of the attackers extensively studying the infrastructure the bank, or entire banking system at the time used to securely exchange and authenticate transactions, SWIFT. Attackers managed to gain access to the SWIFT messaging system "likely through a spear-phishing attack" (Chien 7:40) and maintained persistent access until the perfect weekend, the weekend of Thursday, February 4, 2016. That weekend, as previously mentioned was a Muslim holiday, so it would be a 3-day weekend, giving attackers time to run off with the stolen funds. The attackers began creating and sending fraudulent transactions to the New York Federal Reserve in the United States on Thursday. Some of the transactions were declined, but most were approved (approving over 80 million dollars worth of funds transfers). Attackers made the transfers go to bank accounts of RCBC bank that were created a few months before the attack by an employee (Maia Nuketo) that knew a person involved in the heist. From there, attackers withdrew some of the funds to get cash, or used electronic funds, and brought them to a casino in the Philippines owned by a man named Kim Wong, where they effectively washed the money. By the time employees at Bangladesh bank realized what had happened, it was too late, the attackers were gone with the money. Some of the funds were recovered later and other funds were frozen for investigative purposes. However, not all the funds were recovered, there remains (to this day) about 67 million dollars of stolen funds out there.

This heist was the worst cyber-attack anyone had ever seen at the time. This heist not only attacked the integrity of the Bangladesh bank but also the integrity of the entire banking system because attackers gained a foothold in the network through the critical infrastructure of the banking system. While there are many theories as to whom the attackers were, one thing is for certain, this attack had to have come from a very powerful nation-state or sponsored actor. It would essentially be impossible for any typical cybercriminal to have access to the resources (both technology and personal) to be able to attack this scope. Furthermore, the attackers were very motivated, studying their target for months, if not, years before acting on their plan. It is for those reasons that multiple sources believe the attack was carried out by the North Korean-sponsored group Lazarus group. Not only is the Lazarus group capable of an attack of this scope, but they have the motives for it as well. North Korea has been an economically starved country, essentially sanctioned by every other country in the world, and they’ve needed to find ways of making money, trading, or providing for their people in some way. They have previously attacked other large nation-states purely for economic purposes, so it would make logical sense.

While the heist was something that most people wouldn’t have seen coming, it was something that could’ve been preventable in the first place. By studying this incident we can understand what the attackers' motives were during and before the attack to prevent similar or the same type of attacks from happening again in the future. The attackers were motives were likely based on routine activity theory (RAT) because they had the necessary skill to attack this size, saw the opportunity, found a suitable target (multiple for that matter), and found that there was a lack of capable guardian in the entire incident since no bank or institution, in particular, wanted to take the blame for being attacked (SWIFT, Bangladesh bank, RCBC, etc.). Furthermore, the attackers were economically motivated because they purely stole money from the bank and didn’t cause additional harm to raise awareness for any subject in particular.

Some ways we could prevent attacks similar to this one from happening in the future is to essentially think like an attacker. If we notice that there is one underlying system that most banks (or other entities) rely on, then we know that attackers are likely to attack that entity itself, akin to a watering hole attack. If we don’t ensure the integrity and robust security of the underlying system, then we are immediately at risk of attack. This entire scenario is similar to Jenga blocks, if you build a service or institution (3rd level Jenga blocks) on another program or service (1st level Jenga blocks), then if someone pulls the first level Jenga blocks out from underneath the third level ones, the higher-level institution will collapse.

All in all, this bank heist on Bangladesh bank was not a traditional bank heist by any means, but we (the security community) should have seen something like this coming. The heist took advantage of a weak infrastructure that multiple, if not, all banks were built on and almost brought the entire system to a halting stop. The nation-state-sponsored attackers managed to plan this heist over several months and gain access to critical infrastructure for the bank ultimately causing the funds to be stolen. While many say this attack couldn’t have been prevented, we should have prevented this exact attack from occurring by taking some preventative measures. Lastly, we need to study the motives and the operation of this attack to fully understand how attackers were able to slip past multiple defenses, how defenders were able to not fully secure their applications (SWIFT-related), how no one can track the attackers down entirely, and how banking institutions and other related parties are able to not take any responsibility for this attack.

References

Hacked | Documentary | Cybercrime | Hackers | Cyberheists | Cyber Crime | Cybercriminals | Hacking. (2020). *YouTube*. Retrieved September 18, 2021, from https://youtu.be/fP4YbGRBboE.

Maloney, C. B. (2016). *Bangladesh bank heist*. Congresswoman Carolyn Maloney. Retrieved September 19, 2021, from https://maloney.house.gov/issues/bangladesh-bank-heist.

Tsing, W. (2019, November 15). *The advanced persistent Threat files: Lazarus Group*. Malwarebytes Labs. Retrieved September 18, 2021, from https://blog.malwarebytes.com/threat-analysis/2019/03/the-advanced-persistent-threat-files-lazarus-group/.