BANGKO SENTRAL NG PILIPINAS HACKING ATTEMPT (2012)

In an attempted hacking incident in the Bangko Sentral ng Pilipinas that occurred in September 2012, the attackers were trying to steal the funds. The attackers are believed to be with the Anonymous Philippines. The attempted hacking attack was discovered when a strange activity on the website was spotted in the system of the Bangko Sentral ng Pilipinas. However, the cyberattack was prevented right away due to the website firewall and intrusion prevention that were embedded in the central bank system, which monitors suspicious activity or unauthorized access to the network, which can alert the administrator for a possible threat in the system.

The threat ongoing?

The hacking attempts on the website of Bangko Sentral ng Pilipinas (BSP) were effectively stopped. The BSP at the time emphasized that while cyberattacks are an ongoing danger, keeping strong security systems is crucial for preventing successful breaches. BSP keeps upgrading its cybersecurity protocols, especially in reaction to international cyber-attacks like the theft of Bangladesh Bank. Although hacking efforts remain, the BSP has consistently enhanced its security systems and firewalls to protect against these threats.

What type of attacker(s) was/were involved, and how did they perform the attack?

The Bangko Sentral ng Philippines hacking attempt did not disclose the reports of the hacking process' availability. Yet, the attack was a component of the cyberthreats directed towards financial institutions, especially in the wake of the well-publicized cybercrime that targeted Bangladesh's central bank. The hacker focused on the security system's holes in the bank.

Individuals who did the hacking were not publicly identified. The attack was connected to a larger network of cybercriminals that were involved in similar attacks on financial institutions internationally, the investigation suggested connections to the notorious Lazarus Group that are known for its high-profile cyber heists and the ones responsible for this hacking attempt remain at large with little hope of them getting caught and would be put to jail. Primary operations of Bangko Sentral ng Pilipinas was affected. However, the incident also raised concerns about the security of other financial institutions in the Philippines and gave a nationwide review of cybersecurity practices in the banking sector.

The 2012 incident involving the Bangko Sentral ng Pilipinas (BSP) was part of a larger cyber heist targeting the Bangladesh Bank. Hackers managed to steal $81 million from the Bangladesh Bank’s account at the Federal Reserve Bank of New York. The BSP Fined the RCBC 1 billion Php for its failures, but thankfully the attack on the BSP was stopped before any anything happened Reaction of relevant/necessary authorities

1. Bangladesh immediately sought assistance from international cyber security experts.

2. The BSP imposed a 1 billion Php fine On the RCBC for its role in facilitating the attack.

3.The Philippine Senate conducted hearings to investigate the incident, scrutinizing the actions of RCBC and other involved parties.

4.International Cooperation as the incident underscored the need for international cooperation in combating cybercrime.

5.Regulatory Changes: In response to the heist, there were significant improvements in anti-money laundering measures and cybersecurity protocols.

What countermeasures were used stop/prevent the attack?

Enhance the cybersecurity infrastructure by regularly updating the patch systems to fix suspicious activities. Conduct regular training sessions for employees on cybersecurity best practices Develop and regularly test incident response plans to quickly address any issues work closely with global cybersecurity agencies to share information and strategies to ensure safety.

What are the other local or international crimes related to the crime discussed?

Similar cybercrimes and attacks have targeted financial institutions worldwide, including the infamous Bangladesh Bank theft in 2016. These alarming incidents highlight the global and persistent nature of cyber threats to the financial sector, emphasizing the need for robust security measures.

Recommendations

To prevent similar attacks, it is important to:

Strengthen cybersecurity measures.

- Create a greater collaboration between financial institutions and cybersecurity agencies.
- Educate the public and employees about the importance of cybersecurity.
- Implement and enforce much strict cybersecurity laws and regulations.
- Regularly conduct regular security audits to identify and address vulnerabilities.

References

Agcaoili, L. (2016). Bangko Sentral foils attempts to hack its website. https://www.philstar.com/headlines/2016/04/28/1577936/bangko-sentral-foils-attempts-hack its-website

Mateo, J. (2017). Year of hackers: Bangladesh bank heist, Comeback https://www.philstar.com/headlines/2017/01/06/1659976/year-hackers-bangladesh-bank-

heistcomeleak?fbclid=IwZXh0bgNhZW0CMTAAAR1NaNp7DkpgcW1qyHgtof8sJoArQZY9kNDwzyQ0a9b0HhtwV gqJnZMAhFA_aem_89Cc8kyFs45ubWldqfnNqg

de Vera, B. & Dumlao-Abadilla, D. (2016). BSP foils attempt to hack website. https://business.inquirer.net/209914/bsp-foils-attemp-to-hack-website

Lema, K. (2016). Philippine central bank says foiled attempts to hack its website. https://www.reuters.com/article/technology/philippine-central-bank-says

Group Members:

Acodili, Kenneth Lii

Cagas, John Cedric

Caruz, Rhysa

Jaojao, Cristine Joy

Rodriguez, Mark Jim