COMELEC Data Breach 2016

In 2016, a group of hackers called LulzSec stole information from the COMELEC, the group that runs elections in the Philippines. They took a lot of information about people who were registered to vote, including names, addresses, and even fingerprints. This was a big deal because it put a lot of people at risk of having their identity stolen.

What is the event about and when did it happened?

The COMELEC data breach of 2016, happened on March 27, 2016. The defacement of the Comelec website by a hacker group called Anonymous Philippines happened at near midnight on March 27 (Estospace, 2016).

Where the attack was first discovered, how far did it spread and when it was finally contained?

The breach was discovered when a group of attackers called Anonymous Philippines posted the stolen data online. A cyber-attack on the website of the Philippines Commissions on Elections (Comelec) has resulted in personally identifiable information (PII) of roughly 55 million people being leaked online (Security Week, 2016).

Is the threat ongoing?

The threat of data breaches and identity theft is still ongoing, the threat of hackers stealing information is still a problem. Even though the COMELEC data leak happened in year 2016, it showed how easy it is for hackers to get information from important government websites (Wikipedia contributors, 2024)

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

According to some news articles the attackers were two groups, Anonymous Philippines and LulzSec Pilipinas. They hacked the COMELEC website and downloaded 340GB of data from the COMELEC database. The attack involved personal information belonging to 55 million registered Filipino voters. LulzSec claimed responsibility for the attack through their Facebook account, and they released their stolen data online

Were the perpetrators caught?

According to some news articles, the perpetrators of the attack were apprehended by National Bureau of Investigation one of the suspected hackers, identified as Paul Biteng a 20-year-old IT graduate student who is a member of the hacking group Anonymous Philippines in his home in Sampaloc, Manila. The authorities took three weeks in order to track down the hacker. A Week later the second hacker named Joenel de Asis also a 23-year-old Computer Science graduate was apprehended by NBI at his house in Muntinlupa. They identified de Asis as one of the ringleaders of the notorious hacker group, Lulzsec Pilipinas. Paul Biteng, Joenel de Asis and perpetrators are to be charged of violations of the Cybercrime Prevention Act of 2012, Republic Act No. 10175.

Who, or what entities were affected by the attack?

The entities affected by the attack are, the 55 million registered Filipino voters whose personal information was leaked, the COMELEC officials whose administrative accounts were compromised, and the CSOs (Civil Society Organizations) who were impacted by the lack of secure online communications and the difficulty of managing development content. The incident also highlighted how weak the Philippines is against hackers (ABS-CBN News, 2024)

How much damage did it cause?

The incident damaged reputation of the Commission on Elections Philippines (COMELEC) and the Philippine government and affects the public trust in their system. The COMELEC paid PHP1.2 billion (USD 23 million) to address the data breach, which included conducting an investigation, upgrading systems, and giving free credit monitoring to those affected. Over 55 million voters' personal information was exposed, including full names, residences, dates of birth, and passport numbers, which could be exploited for identity theft, fraud, and other cybercrimes (Masaga, 2023).

How did the necessary authorities react to the attack?

The COMELEC officials have suffered legal and political criticism as a result of the hack, including calls for their resignations and charges of incompetence and data privacy violations. The hackers sold the stolen data on the dark web, potentially making millions of pesos from customers (Macairan, 2016).

What countermeasures were used stop/prevent the attack?

According to Jacob and Pacis (2018) the reason why they are easily to attack of the data breach because of the use of weak Passwords, outdated Software, lack of encryption, And the absence of a Comprehensive cybersecurity Plan. Despite not disclosing any specific protections against the most recent attack, the COMELEC is highlighting the importance of proactive cybersecurity measures to protect its systems. This calls for frequent security audits to identify vulnerabilities in voter databases and election systems, encrypting sensitive data in transit, and training staff members on cybersecurity best practices in order to lower the likelihood of a data breach.

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

On April 6, almost one week later, cybersecurity company Trend Micro released a blog post outlining the Comparing the leak to what might be "one of the biggest government-related data breaches in history." The 2015 breach of the US Office of Personnel Management resulted in the revelation of private data belonging to almost 20 million Americans (Jacob & Pacis, 2018)

In your opinion, what could be done to improve the situation and prevent similar attacks from happening in the future?

In order improve the situation and prevent similar attacks from happening in the future especially in governments, they should prioritize a system protection and regular system updates and monitoring. They also need to keep their software up-to-date and watch for any strange activity. This will help them stop hackers before they can steal information and to reduce their risk of cyberattacks and minimize the damage that will cause to future incidents.

References

Masaga, E. J. B. (2023). COMELEC data breach (2016) Case Study. *ResearchGate*. Retrieved from, https://www.researchgate.net/publication/369184215_COMELEC_data_breach_2016_Case_Study

The Philippine Star. (2016, April 29). 2nd Comelec hacker nabbed. Retrieved from, https://www.philstar.com/headlines/2016/04/29/1578281/2nd-comelec-hacker-nabbed

Wikipedia contributors. (2024, February 2). Commission on Elections data breach. Wikipedia. Retrieved from, https://en.m.wikipedia.org/wiki/Commission_on_Elections_data_breach

Hacker who allegedly leaked Comelec data now in NBI custody. (2016, April 29). Cnn. https://web.archive.org/web/20160513114309/http://cnnphilippines.com/news/2016/04/29/Comelec-hacker-data-leak.html

Second Comelec hacker arrested. (n.d.). The Standard. https://web.archive.org/web/20160430104529/http://thestandard.com.ph/news/-main-stories/top-stories/204610/second-comelec-hacker-arrested.html

ABS-CBN News. (2024, July 19). Comelec's Bautista faces criminal raps over massive data leak. ABS-CBN News. https://news.abs-cbn.com/news/01/05/17/comelecs-bautista-faces-criminal-raps-over-massive-data-leak

Wikipedia. (n.d.). *Commission on Elections data breach*. Wikipedia. https://en.wikipedia.org/wiki/Commission_on_Elections_data_breach

Jacob, J., & Pacis, J. (2018). *Revisiting the breach: A briefing paper on the 2016 COMELEC data leak*. Foundation for Media Alternatives.

Macairan, E. (2016, May 17). 2nd Comelec hacker nabbed. Philstar.com. Retrieved from: https://www.philstar.com/headlines/2016/04/29/1578281/2nd-comelec-hacker-nabbed

Eden Estospace (2016). Massive data breach exposes all Philippines voters. https://www.telecomasia.net/content/massive-data-breach-exposes-all-philippines-voters/

Security Week (2016). 55 Million Exposed After Hack of Philippine Election Site. https://www.securityweek.com/55-million-exposed-after-hack-philippine-election-site/

Group Members:

Saura, Jhon Lexter

Sacal, Xyrha Viel

Ybañez, Alistair

Sanglay, Daniel Cedrick

Telamo, Saturnino JR.