SECURE CODING

ASSIGNMENT - 2

TOPIC : RECENT CYBER ATTACKS / BREACHES

SUBMITTED BY	**SUBMITTED TO**
Rishab Banthia	**Prof. Sibi Chakkaravarthy**
18BCN7076	**Dept. of Computer Science**

CHINESE CYBER ATTACK ON INDIAN POWER GRID

INTRODUCTION

From the past year, the relationship between India and China has not been so good, following the border dispute in May 2020 between two nations which resulted in first combat deaths in 45 years. Economic factors and diplomacy has prevented a full-blown war at the border but still cyber operations continue to provide the nations with potent asymmetric capability to conduct espionage or pre-position within networks for potentially disruptive reasons.

Recently, on October 12 there was a cyber attack by a group which is known to be linked with China and the group's name is RedEcho who had caused damage to the indian power infrastructure. According to the CEO of Recorded Future, Christopher Alhberg, the Massachusetts based enterprise security outfit detected the intrusion that there were 10 indian power sector assets and the Mumbai and the Tamil Nadu’s VO chidambaranar ports came under attack.

The list of those sectors under attack are :

- Power System Operation Corporation Limited
- NTPC Limited
- NTPC Kudgi STPP
- Western Regional Load Despatch Centre
- Southern Regional Load Despatch Centre
- North Eastern Regional Load Despatch Centre
- Eastern Regional Load Despatch Centre
- Telangana State Load Despatch Centre
- Delhi State Load Despatch Centre
- DTL Tikri Kalan (Mundka), Delhi Transco Ltd
- V. O. Chidambaranar Port
- Mumbai Port Trust

BACKGROUND

Recent years have highlighted a growing rivalry between the world’s two most populous countries, as India’s economy and geopolitical ambitions seek to compete with those of China. Since May 5, 2020, Indian and Chinese troops have repeatedly skirmished with one another along the India-China border. Reports indicate several likely causes for the escalation, including China's being more assertive in border regions in light of international pressure over the handling of the COVID-19 pandemic, and India's construction of transportation infrastructure in contested areas. China reportedly amassed a large concentration of troops near the border with India following the initial border escalation, and the dispute appears unresolved. In June 2020, the Indian government announced it was banning the video-sharing social media platform TikTok from the country, citing fears that the app, whose parent company is the Chinese tech giant ByteDance, might be used to collect data on citizens and potentially also be used for espionage to benefit the Chinese government through a wide-ranging cybersecurity law. By November 2020, the Indian government had subsequently banned over 200 Chinese apps in what was described as a “Digital Strike’’ in response to the Sino-Indian border clashes by India's technology minister.

REPORTS

- The cyber cell of Maharashtra submitted a provisional report to the Maharashtra government regarding the massive grid failure which hit Mumbai and surrounding areas on October 12 last year. This 100-page report submitted to the Maharashtra government confirmed that a malware attack was behind the power outage in Mumbai and also stated that about 14 Trojan Horses and unaccounted data of 8GB was found in the system. According to the investigation, the malware was installed in the Maharashtra State Electricity Board (MSEB) system by unverified sources.

- According to the reports of the Recorded Future they observed that through its network intelligence, a high volume of network traffic used by China linked group RedEcho from the Indian power sector assets to servers and also stated that the adversary infrastructure is still active and continues.

- Recorded Future threats research team,Charity Wright of Insikt said the identified infrastructure area includes the length and breadth of Indian geography and census.

WORLDS POWER GRIDS INCREASINGLY VULNERABLE TO CYBER ATTACKS

Not only the indian power grids are under danger but all the power grids around the world are increasingly vulnerable to cyber attacks. One of the main reasons that power grids are increasingly vulnerable to cyber attacks is due to the digitalization and the use of more smart applications.

It is the threat posed by India's first investigation into the October shutdown in Mumbai that may have been caused by cyber-attacks. The strike affected stock markets, trains and thousands of families in the national treasury. The disruptive power of the grid failure - as seen in Texas last month due to a sudden cold - makes the sector a much more targeted target, especially for hostile actors based on the government.

Important state infrastructure such as power grids and nuclear reactors have been and will continue to be a victim of cyber attacks because they currently allow internet connectivity, making them vulnerable.

MARRIOTT DATA BREACH

INTRODUCTION

Marriotts suffered a data breach due to which this breach affected around 500 million people. All the hotels and resorts belonging to the Starwood division were affected.

BACKGROUND

- In 2014, Starwoods guest reservation database had a security vulnerability that allowed unrestricted access.
- In 2015, Starwood suffered a credit card breach from malware on their point-of-sale systems.

- In 2016, Marriott acquired Starwood for $13.6 billion, creating the world's largest hotel chain.
- In 2018, vulnerability in Starwood database was discovered through a security system alert.

EXECUTION AND IMPACT

- Hackers remotely accessed the computer's and installed the 'RAT'.
- Covered footsteps by encrypting and deleting data that was stolen.
- Exfiltrated data by encrypting it to hide detection.
- Suspected chinese government involvement in the attack.
- Targeted vulnerability in Starwood database, which allowed unauthorized access since 2014.
- Around 9.1 million credit card numbers were stolen.
- Around 23.75 million unique passport numbers were stolen.
- Guests' personal information was stolen.
- Marriott International's stock price dropped by 5.6%.
- Affected around 500 million guests.
- Estimated $1 billion in damage and $1 billion in legal fines.
- Could cost billions of dollars to replace these many passports.
- Data stolen was not sold on the dark web.

RESPONSE BY MARRIOTT

- Issued a public statement in November 2018 disclosing the breach to its customers.
- Attempted to address customers' concerns.
- Hired kroll to provide a free year of WebWatcher service.
- Dedicated call centre about the incident for each country.

CONCLUSION

- Exemplifies the importance of cybersecurity practices.
- Hotels are especially targeted for their large consumer base and database of personal information.

- All businesse that collect personal data should implement more rigorous security policies.