Case study on Cosmos Bank Malware Attack

Prepared by : Nikita Pol (1504061)

What is Malware Attack??

- A malware attack is a type of cyberattack in which malware or malicious software performs activities on the victim's computer system, usually without his/her knowledge.
- Objective of malware attacks is commonly Make money by stealing sensitive information such as online banking logins, credit card numbers or intellectual properties. This is termed "identity theft," and involves stealing users online credentials and using that to impersonate them.

Crime Scenario

- On 1th August 2018, around Rs 78 crore was withdrawn through ATMs located in 28 countries through 12,000 Visa Card transactions. These were transferred out of the country, including bank accounts in Hong Kong. Another amount of Rs 2.50 crore from 2,849 Rupay Card transactions was transferred within India.
- During those 150 minutes (2.30 hours), some unknown persons hacked into the ATM Switch (servers) at the bank's headquarters and acquired the sensitive data of its Visa and RuPay debit card customers, and there were multiple transactions in 28 countries with a total of Rs 80.50 crore (Visa + Rupay) vanishing.

  As the bank tried to grapple with the crisis, a fresh virtual attack was mounted on Monday (August 13), when the hackers initiated SWIFT transactions and within minutes transferred Rs 13.92 crore to the accounts of "ALM Trading Ltd," with Hang Seng Bank, Hong Kong. The amounts were soon withdrawn from that bank.

Tools/Methods used in Crime

- Attackers were likely able to send fake Transaction Reply (TRE) messages in response to Transaction Request (TRQ) messages from cardholders and terminals. As a result, the required ISO 8583 messages (an international standard for systems that exchange electronic transactions initiated by cardholders using payment cards) were never forwarded to the backend/CBS from the ATM/POS switching solution that was compromised, which enabled the malicious withdrawals and impacted the fraud detection capabilities on the banking backend.

IT Acts and Judicial Details

- Section 66C: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say Logo, trademark etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000.
- Section 66D: The fraudsters through the use of the phishing email containing the link to the fake website of the bank or organizations personates the Bank or financial institutions to cheat upon the innocent persons, thus the offence under Section 66D too is attracted.
- Section 43: deals with penalties and compensation for damage to computer, computer system etc. This section is the first major and significant legislative step in India to combat the issue of data theft. The IT industry has for long been clamouring for a legislation in India to address the crime of data theft, just like physical theft or larceny of goods and commodities. This Section addresses the civil offence of theft of data. If any person without permission of the owner or any other person who is in charge of a computer, accesses or downloads, copies or extracts any data or introduces any computer contaminant like virus or damages or disrupts any computer or denies access to a computer to an authorised user or tampers etc…he shall be liable to pay damages to the person so affected.