# Department of Information Technology
# ISE-I
# Case Study

| | | | |
|---|---|---|---|
| Enrollment No. | 1504061 | Course Name | Cyber Laws & Forensics |
| Student Name | Nikita Uttam Pol | Course Code | IT 4122 |
| Case Study Title | Pune's Cosmos Bank loses Rs 94 Cr to cyber attack. | | |

## Background

An international gang of hackers siphoned off Rs 94.42 crore from the Cosmos Cooperative Bank Ltd, through multiple ATM swipes in 28 countries worldwide on 11th and 13th August 2018. This was an 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.

Malware programs used in cybercrimes typically have some simple and well-known objectives. 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. Cybercriminals can access the victim's bank accounts and use them in a number of ways including physical theft, digitally laundering money or selling the victim's data to other criminals

## Details of crime

The Cosmos Bank admitted that it was cyber-attacked twice, the first attack took place on August 11 (a bank holiday) between 3 p.m. and 10 p.m. and the second on August 13 around 11.30 a.m. - with ATM withdrawals taking place in at least 28 countries, affecting its headquarters on Ganeshkhind Road.

On Saturday, around Rs 78 crore was withdrawn through ATMs located in 28 countries through 12,000 Visa Card transactions.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 The amounts were soon withdrawn from that bank.

## Allegations (if any)

It seems that the attackers were from outside the India who done malware attack on bank system and the cybercrime investigators are claiming that the attack was just a testimonial for them or trail. They can attack several bank systems with same way they have used for this attack. And all banks should be remain highly alerted.

## Crime Investigation

Hackers managed to siphon off over Rs 90 crore through a malware attack on the server of the cooperative bank and cloning thousands of debit cards. The fraudulent transactions were carried out on August 11 and August 13 and the malware attack by the hackers originated in Canada.The bank has also registered an FIR at the Chatushringi police station in the city. A case was registered under sections 43, 65, 66(C) and 66 (D) of the Information Technology Act and relevant sections of the Indian Penal Code. Over the two days, hackers withdrew a total Rs 78 crore from various ATMs in 28 countries, including Canada, Hong Kong and a few ATMs in India, and another Rs 2.5 crore were taken out within India. On August 13, hackers again transferred Rs 13.92 crore in a Hong Kong-based bank by using fraudulent transactions. The cooperative bank's core banking system was not affected and that it has already appointed a professional forensic agency to investigate the fraud. As a precautionary measure, the bank has closed ATMs operations and suspended net and mobile banking facilities..

## Tools & Methods Used(or might have used) by Criminal to commit the crime

Following an earlier patient-zero compromise and lateral movement, on August 10-11, 2018, the bank’s internal and ATM infrastructure was compromised. The exploit involved multiple targeted malware infections followed by standing up a malicious ATM/POS switch (malicious-Central or MC) in parallel with the existing Central and then breaking the connection between the Central and the backend/Core Banking System (CBS). After making adjustments to the target account balances to enable withdrawals, MC was then likely used in fake “*on-us,” foreign-to-EFT, standing-in, etc. activity that enabled the malicious threat actor to authorize ATM withdrawals for over US$11.5 million in 2849 domestic (Rupay) and 12,000 international (Visa) transactions using 450 cloned (non-EMV) debit cards in 28 countries.

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 Act and Judicial details

Infection of IT systems with malware ( Including ransomware, spyware, worms, trojans and viruses) the following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/ person in charge of the computer:

1) 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.
2) 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.
3) 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.

Th above offences are punishable with imprisonment up to three years or with a fine up to INR 500,000 or with both (Sec. 66A, ITA).

## Result of the Case

Jyotipriya Singh, under whose supervision the special investigation team (SIT) is probing the case, has given the statement that While investigating the domestic transactions, on 12th September 2018 they have arrested two persons from different places in the state. They were found involved in the fraudulent transactions. According to her, both the accused were produced before a court on 11th September, which remanded them to seven days of SIT custody.

## Suggestions/opinions about the case

In this case of malware attack on bank server, the attacker took advantage of negligence of employees handling the computer systems and it was easier for attacker to do malware attack on bank server system. So every computer user in organization should know about cybercrime, different ways that cybercrime could take place. They should be alert while using internet on computer system. It it's a way avoid cybercrime. Also the bank server security must be tightened.

## Thoughts on cybercrime & criminals

In my opinion, cyber crime is much more dangerous than regular crime, as it is much harder to track down the criminal; the crime can be committed from anywhere in the world where their identity remains completely hidden. Also, in cybercrime, the criminal can hack through one system and get access to many records of private data, as we depend mostly on technology to store it. But parallelly we are innovating new ways to protect ourselves from the cybercrime. So its very important for user to use internet with alert mind.