# COSMO Bank Attack

The Cosmos Bank attack in Pune, India, occurred on August 11, 2018, when cybercriminals injected malware into the bank's core banking system. This allowed them to compromise the switch application and monitor transactions. The attackers used fake debit cards to make unauthorized withdrawals from ATMs globally, resulting in financial losses of approximately ₹94 crore (around $13.5 million USD). The incident highlighted vulnerabilities in the bank's security measures.

# TIMELINE

- **August 10, 2018**-preparation for the attack
- **August 11, 2018**-Injection of malware ,monitoring of transactions
- **August 11, 2018 (Afternoon)**-[DURATION- approx 2 hours]first series of attack,global atm withdrawals
- **August 13, 2018**-[DURATION-30minutes]-second series of attack

# DETAILS

- Rs 94 crore in just 3 days
- malware attack
- cloned debit cards-ATM transactions from India(12000atm)
  28 other countries

- Money transfer of approx 13.92 crore transferred via swift

total of Rs 94 crore was siphoned off in this case, which was registered at the Chaturshringi police station under sections 120B, 420, 467, 468, 469, 471, 34 of the Indian Penal Code (IPC) and relevant sections of the Information Technology Act.

information verified under India Press

# SECTIONS UNDER WHICH THE ACCUSED WERE GIVEN JUDGEMENT

- **120B**-Section 120B gives the punishment for people who commit criminal conspiracies.
- **420**-Section 420 in the Indian Penal Code deals with Cheating and dishonestly inducing delivery of property
- **467**-If someone forges a document that pretends to be a valuable security, will, adoption authority, or any authorization for financial transactions or property exchanges, they can be punished with life imprisonment or imprisonment for up to ten years, and may also be fined.
- **468**-forged shall be used for the purpose of cheating, shall be punished with imprisonment
- **469**-forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose
- **471**-[document or electronic record] which he knows or has reason to believe to be a forged
- **34**-provides only a general definition of what constitutes joint liability

# Convict list

- Fahim shaikh
- mohammad saeed iqbal hussain jafari
- fahim khan
- Shaikh mohammed abdul jabbar
- mahesh rathod
- naresh maharana
- UA waz (anthony)
- bashir ahmed
- feroz shaikh
- abdulla shaikh
- salman baig

# Methods of Attack

- **Attack Techniques:** The cybercriminals hacked into the Cosmos Bank's system through a malware attack on its servers.
- **Gaining Access:** The attackers compromised the bank's network by targeting the switch application, which is connected to the payment gateway of the National Payments Corporation of India (NPCI).
- **Exploited Vulnerabilities**: The attackers used malware to disable security mechanisms and monitor and manipulate transactions

## malware attacks

- The cybercriminals infiltrated Cosmos Bank's network by injecting malware into its core banking system.
- The malware was likely used to bypass security measures and gain unauthorized access to sensitive systems and data.

## Compromised Switch Application

- The attackers specifically targeted the bank's switch application, which facilitates communication between the bank's systems and the payment gateways (such as the National Payments Corporation of India or NPCI).

## Creation of Fake Debit Cards:

- Once inside the system, the attackers were able to create fraudulent debit cards linked to real customer accounts.

# SWITCH application used by cosmos

Cosmos Bank used a switch application from the Indian payment services provider, "**Hitachi Payment Services**".

The switch application is an essential component of the bank's infrastructure as it handles transactions by facilitating communication between the bank's core banking system and various payment gateways, such as the **National Payments Corporation of India (NPCI).**

# WHO MADE THE MISTAKE ?

| SWITCH APPLICATION PROVIDERS | COSMOS BANK |
| --- | --- |
| • **updates and security**<br>• **application security**<br>• **security support** | • **security practices**<br>• **monitoring and auditing**<br>• **compliance and awareness to employees** |

# how was the injection made to the software?

howsoever the bank tries to hide under the cover of hitachi payment services the injection could only be made for the faults of banking services there wasnt any proper ingress and egress systems to handle the date entering and exiting the bank there wasnt any switch or prevention system in network layer .It could only be possible by :

- phishing attacks
- exploiting vulnerabilities
- social engineering
- insider threats
- remote access control

all these processes could have only be made if the employees wasnt aware enough

# why was these integrations made after attack?

## KNOW YOUR CUSTOMER (KYC) AND ANTI MONEY LAUNDERING (AML)

The Bank is complying with all the guidelines related to KYC & AML issued by RBI from time to time. Accordingly the KYC/AML Policy is formulated. The Bank has submitted all the statutory reports within prescribed time limit to FIU-IND.

The Bank has 2 Centralized Account Opening Cells for opening current and savings account. Account opening form with KYC documents are scanned through Document Management System (DMS) to maintain permanent e-record documents at these Account Opening Cells.

32/100

page 31 of the 2018 annual report provided by cosmos bank when KYC was a must information to be gathered from customer the policy issued by RBI in 2005

The 'Know Your Customer' guidelines were issued in February 2005 revisiting the earlier guidelines issued in January 2004 in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). 1 Jul 2015

# why was policy that wasnt followed not reviewd by RBI

# changes made by the bank after the attack

- Security posture
- Endpoint security
- Atm whitelisting
- Spam mail filtering
- Cyber security framework

# How could it be prevented in 2024?

there were multiple ways to prevent it if the attack was made in 2024 enlisting:

- cloud framework and security
- policy changes
- frequent updates of software
- AI based threat detection
- Spam mail alert
- Email detection

# conclusion

I felt personally this was a lower percentage of mistake rather than failure of proper awareness of the bank and its IT departments , all of them should have been warned and given proper information on how to deal with mails that are not from their companies .Their negligence  on cyber threat and mandatory policy update led to such failures.

I feel standing in 2024 where the human pshycology is more tipped towards the eye candy leading to  such disasters there are jobs spreading all over the world but no one to spread awareness. What  would happen ? How much it can affect me ? people tend to forget such serious questions .I feel there is more to aware people bout securing than making security changes.