Special Report – Cyber-attacks on the Indian banking sector

Introduction

State Bank of India, India’s largest bank, on October 19th, stated that it had blocked close to six lakh debit cards following a malware-related security breach in a non-SBI ATM network. Several other banks, such as Axis Bank, HDFC Bank and ICICI Bank also admitted to being victims of similar cyber attacks. Due to the massive data breach, Indian banks have decided to either replace or request users to change the security codes of as many as 3.2 million debit cards. However, in certain cases banks have decided blocked the cards or issue fresh ones.

What happened?

Card data of 3.2 million customers was stolen between May 25th and July 10th from a network of Yes Bank ATMs managed by Hitachi Payment Services. However, it was only in early September that banks and payments services providers became aware of the extent of the breach. As per some reports, the malware infection took about six weeks to detect, compromising transactions that took place during this period. Banks came across fraudulent transactions, in which debit cards were used in China and the US for customers who were present in India. In addition, cardholders also detected similar transactions. Subsequently, banks lodged complaint to the National Payments Corporation of India (NPCI), which has oversight over retail payments systems in India. Fraudulent withdrawals have been reported from 19 banks so far.

NPCI investigations found a malware-induced security breach in the systems of Hitachi Payment Services, which provides ATMs, point of sale and other services in India. The investigation alleged that the security breach occurred in the ATMs of a particular private bank.

Of the 3.2 million cards involved, over 2.6 million belonged to MasterCard and Visa, and the remaining were from the RuPay, according to the NPCI. Visa and MasterCard have stated that their own networks were not compromised. Both YES Bank and Hitachi claim there was no breach or compromise at their end. The breach, according to initial investigations, has mainly affected the magnetic strip ATM cards.

What is the impact?

This is one of the biggest data breaches in the country.
- Around 3.2 million cards issued by Indian banks are to be replaced, or their holders asked to change their PINs.
- According to NPCI investigations, 90 ATMs have been compromised, and at least 641 customers across 19 banks have lost Rs 1.3 crore.
- SBI will replace about 6,25,000 debit cards as a precaution, and customers will be compensated for losses, estimated to be around Rs 10 lakhs to Rs 12 lakhs.

The number of cards affected by the breach may seem small, as it the impact is on about 0.5% of the 712.39 million cards issued by Indian banks till August 2016. However, the potential losses could still be significant, if a large number of them are exposed to this fraud. However, at the present juncture, there is no way of knowing the exact extent of the damage caused, until the investigations are completed.

What is a malware attack?

Malware is malicious software including viruses, worms, Trojans, ransomware, spyware and other programmes that damages computer systems at ATMs or bank servers, and allows fraudsters to access confidential debit card data. In the recent data breach, swiping a card at an allegedly compromised ATM allowed the data on the card to be transmitted to the fraudsters, who then misused it for fraudulent transactions.

What is being done now?

The affected banks, NPCI, Visa, MasterCard, and Hitachi Payment Services have called for a forensic probe by SISA Information Security. In addition, the Indian Government has sought a detailed report from banks and RBI on the debit card fraud. The council of Payment Card Industry Data Security Standard (PCIDSS), an international body that sets data security standards, has also ordered a forensic audit of the data breach, which is expected to be concluded by the end of October.

As per the initial report of CERT-In, submitted on October 19th, CERT-In, in July 2016, had sent an alert on planned cyber attacks on banks’ information infrastructure. Later, on August 12th and 24th, it had alerted banks about backdoor Trojans that steal credentials of users and also stated about advanced targeted attacks, along with the indicators of compromise for the banks to take action.

Some banks are looking to refund money to customers or other banks. State Bank of India would replace the cards affected by the malware. Meanwhile, Axis Bank has said that while some cards have been replaced, several customers have been asked to change their security codes as well.

Meanwhile, RBI has advised banks to review funds in their bank’s (overseas) nostro accounts, and carry out hourly reconciliation of payment emails by comparing outward messages with SWIFT confirmations. In addition, the RBI has revised its rules for payment companies to incorporate a provision to impose a penalty ranging between Rs 5 lakh to Rs 1 crore for non-compliance or contravention of the Payments Act.

Significantly, RBI has reportedly instructed banks to upgrade the role of the CISO (chief information security officer) from an ‘operational level’ to a ‘strategic level’. The country’s central bank has also instructed banks to implement a security policy enlisting their strategy on combating cyber threats, and spelling out tangible cyber hygiene measures, which are approved by their respective boards.
Analysis

A bank runs multiple servers that store enormous amount of information and details of various operations such as credit cards, ATMs, real time gross settlements, ATMs and SWIFT (the global financial messaging service banks use to move funds), among others. Over the past few years, banks have been fighting cyber attacks like ‘distributed denial of service’ (or DDoS), considered the most common type of cyber attack on financial institutions, worldwide. According to cyber experts, several of these attacks are the work of Chinese or East European hackers.

One such major breach this year was the one on Bangladesh Bank. Earlier this year, around $81 million was stolen from the Bangladesh Central Bank’s account with the Federal Reserve Bank of New York, in one of the biggest-ever cyber heists. The attack on Bangladesh Bank was done through a Trojan Horse, and instructions were issued via the SWIFT network.

Indian banks, when compared to say US banks, have created additional layers of security for users of debit and credit cards. In the US, it is easier to use a credit card but in India there are another levels of security such as OTP (One Time Password) or another system of validation. However, despite the security levels, malware attacks, such as the recent one to Indian banks, remain a high possibility.

The recent attack on Indian banks however, is not the first to hit the Indian banking sector. In one instance, in early August, a Pakistan hacker reportedly defaced the website of a large public sector bank by inserting a malicious page and trying to block some of the bank’s e-payment services. A month prior, in July, another state-run bank’s offshore account was breached in a cyber attack, however, the money trail was traced and the movement of funds was blocked. Separately, software viruses were also found in three personal computers at the Bombay Stock Exchange, which were then identified, separated, and quarantined immediately.

The RBI had already, earlier this year, instructed banks to upgrade their debit cards into chip-based EMV cards, which have added layers of security. The RBI also had issued instructions on a cyber security framework to be implemented in banks, which required banks to have a board-approved cyber security policy.

While most banks have insisted on the fact that there has not been any reported financial loss from the recent attacks, cyber security experts believe that the level of preparedness for cyber crime in India is still basic and companies need to improve their response and detection capabilities. A recent survey by Assocham and PwC found that frauds in the financial sector caused $20 billion in direct losses, annually.

Banks need to assess their own readiness to mount a real cyber defence and incident response to cyber attacks. The only option banks have is to mitigate the effects of cyber attacks as there is no full proof solution to stop such attacks.
Recommendations

- In respect to the current data breach, banks have instructed consumers to use ATMs associated only with their banks.
- Always keep the PIN number secure and regularly change your PIN.
- Activate SMS alert for your debit card transactions and also regularly check your SMS alerts and bank statements for any unusual transactions.
- Ensure bank has your current mobile number so as to get alerts for transactions.
- Always be alert for any strangers around the ATM.
- Check for any visible additional devices attached to the ATM.
- Inform the bank immediately in case the debit card is lost or stolen, or if an unknown transaction is made on the card.
- Do not write the PIN number on the card or disclose it to anyone.
- Recommended not to use public WiFi for financial transactions.
- Do not take help from strangers or let anyone else handle your card.

-------------------------------End of the Report-------------------------------

©2016 All rights reserved. The information contained herein is the Intellectual Property of MitKat Advisory Services Pvt. Ltd. Any unauthorized use of this content, in any form, violates our rights.

Disclaimer: This report is based on analysis of open source information. Recipients must monitor local environmental conditions to ensure security and business continuity. MitKat Advisory Services makes no representation or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties or usefulness for any particular purpose of this document.

MitKat Advisory Services Private Limited

Mumbai
511 Ascot Centre
Sahar Air Road
Andheri (E),
Mumbai - 400099
+91 22 2839 1243

Delhi NCR
Suite# 009, 4th Floor
Time Square
Sushant Lok – 1
Gurgaon – 122002
+91 124 455 9200

Bengaluru
# 127, 2nd Cross
6th Block
Koramangala
Bangalore – 560095
+91 (80) 2550 3300

Singapore
101 Cecil Street #23-12
Tong Eng Building
Singapore (069533)
+65 9222 5030