Deloitte.

Quality.
Commitment.
Excellence.

ATM Security: The Need for Providence

Private and confidential
July 2023

ATM Security: The Need for Providence

ATMs are becoming an attractive target for cybercriminals since they handle financial transactions and store sensitive customer information as well as legal tender in the form of cash. With evolving features and technology, ATMs are becoming more complex, and serve numerous banking related functions, thus becoming a high-priority target for hackers and cyber vandals.

Some alarming stats specific to ATM frauds are:

- As per the RBI data, 65,893 frauds related to 'Card/Internet/ATM/Debit Card, Credit Card and Internet Banking' have taken place in 2021-22.
- As per the NCRB report, state reporting highest number of cases related to ATM frauds were around 652. The country recorded almost two thousand cases related to ATM frauds that year.

Some of the techniques being used are card shimming[1], card skimming[2] , card trapping[3] jamming of keyboard[4] , hidden cameras, replicating digital signatures to name a few, to get access to the customer's account.

In order to control ATM frauds and sensitise everyone, RBI has issued advisories, advising banks to conduct an ATM security ecosystem assessment due the rise in fraudulent cases.

RBI mandate and advisories on ATM security*

RBI mandates modernising ATM estates, futureproofing them against physical security attacks, and providing consumers with an improved experience.

RBI regularly disseminates information about the frauds/cybercrimes and issue advisories to the Regulated Entities (REs)

***RBI Advisories on ATM Security**

Advisory dated 21st June 2018

Advisory dated 29th October 2021

Advisory dated 31st December 2019

Advisory dated 14th June 2019

Advisory dated 19th May 2022

Threats hovering around the banking ATM ecosystem

Some common cyber threats to the ATM ecosystem are:

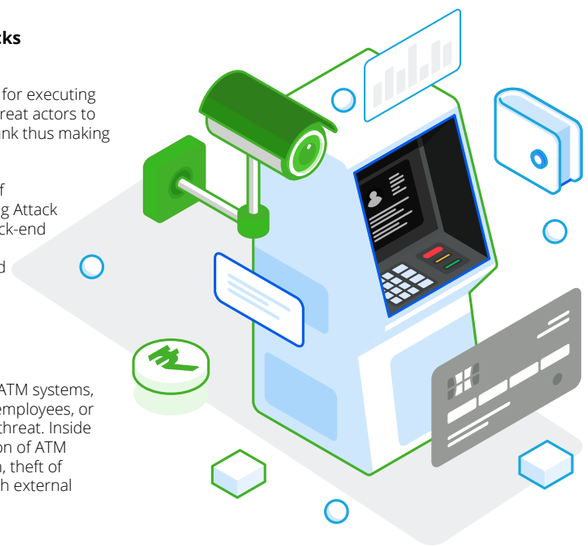
Malware might be camouflaged

ATM machines often get infected with malicious software specifically designed to target ATMs. These malwares might infect the machines through various means, such as compromised software updates or physical access to the ATM's ports. ATM malware can manipulate the system to dispense cash without authorisation and collect sensitive banking information of customer like PIN, CVV etc. It is also called as **jackpotting malware.**

Network-based attacks

ATMs depend on banking network for executing financial transactions. This lures threat actors to attack network infrastructure of bank thus making them vulnerable.

These attacks can be in the form of Man-in-the-Middle attack or Sniffing Attack and can lead to compromise of back-end systems, data theft, transaction manipulation or even unauthorised access of customer account.



Repercussions of partially patched ATM systems

Failure to apply critical security patches and the latest updates to ATM's computer operating system and ATM application and software can leave the machines vulnerable to known exploits and cyberattacks. Outdated software may have known vulnerabilities that can be exploited by attackers.

Insider threat

Insiders with authorised access to ATM systems, such as third-party vendors, bank employees, or contractors, can pose a significant threat. Inside activity may involve the manipulation of ATM software and security configuration, theft of customer data, or collaboration with external threat actors.

Lack of physical security

ATMs are often vulnerable to physical attacks which include theft, ram-raiding, or explosive attacks. Criminals may attempt to break into the ATM to steal cash or gain access to the system for further exploitation.

Social engineering

Social engineering techniques, such as phishing or vishing (voice phishing), can trick ATM users or bank employees into revealing sensitive information like PINs or passwords. These tactics are often used to gain unauthorised access to customer accounts or to gather information for future attacks.

Cash-out attacks

Criminals may compromise an ATM network to perform coordinated cash-out attacks. Cash out attacks involve infecting multiple ATMs with malware and orchestrating simultaneous withdrawals of large amounts of cash, usually during non-business hours.

These threats give birth to requirement of implementing comprehensive security measures, such as strong access controls, regular software updates, encryption, physical security measures, and user education, to protect the ATM ecosystem and maintain the trust and safety of customers.

[1] A shimmer is a thin board discreetly inserted into a card reader which reads data from the magnetic stripe, without interfering with the normal bank card service.

[2] A hidden device is installed in an ATM machine, which reads the information from payment cards during the ATM transaction.

[3] Card trap is the placement of a device.

[4] In this, the fraudsters block important buttons on the ATM keypad (Cancel, Enter, etc.) to prevent the transaction from succeeding.

Source: https://atmeye.com/blog/what-is-atm-fraud/

How Deloitte can help

Security Assessment - The assessment of ATM Channel including review of physical security, network architecture, logical access control, ATM terminal, card management, vulnerability management, vendor management, settlement and reconciliation processes

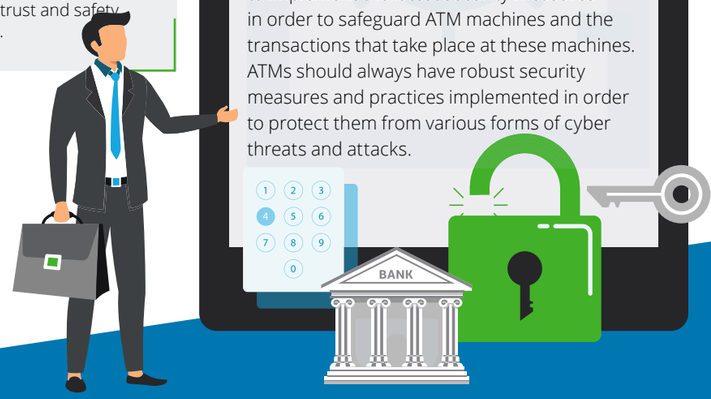
Forensic Review - Proactive/reactive forensic review pertaining to the ATM HDD's involved, to identify the presence, nature of the malware, source of attack, potential reason for propagation of infection to the extent possible

Technical Advisory - Recommendations and measures for creating a robust ATM ecosystem as per RBI guidelines

Our value proposition

- Availability of professional and experienced team members
- Experience in providing ATM ecosystem review with leading tools and technologies
- Experience in working with various public/private sectors and co-operative banks in India

Security of ATM machines is a critical aspect of the banking industry to ensure the safety of customer money, customer transactions, and protection against fraudulent activities. Banks and ATM service providers are bound to implement the latest security measures in order to safeguard ATM machines and the transactions that take place at these machines. ATMs should always have robust security measures and practices implemented in order to protect them from various forms of cyber threats and attacks.



Contact Us

Nikhil Bedi
Partner and Leader - Forensic
Financial Advisory
Deloitte India
Email: nikhilbedi@deloitte.com

Jayant Saran
Partner - Forensic
Financial Advisory
Deloitte India
Email: jsaran@deloitte.com

Sachin Yadav
Partner - Forensic
Financial Advisory
Deloitte India
Email: sachyadav@deloitte.com

Lakshmi Allamsetty
Executive Director
Risk Advisory
Deloitte India
Email: lallamsetty@deloitte.com

Contributor

Shailesh Kand

Deloitte.