ATM SECURITY LANDSCAPE AND FORECAST: AN IN-DEPTH ANALYSIS

AURIGA
the banking e-volution

"Banks must remain alert to attacks on their ATMs. These can cause not only large financial losses, but also irreparable damage to their reputation. Implementing robust cybersecurity measures and proactively managing threats is essential to protect access to banking services and customer trust in a financial institution".

Néstor Santolaya Bea
Cybersecurity Product Expert, Auriga

Summary

1 Introduction

ATMs are the most visible face of banks and, often the most vulnerable, suffering attacks such as theft, damage, or computer viruses.

The range of threats ATMs face can be classified into two broad categories:

- Physical Attacks
- Fraud Attacks

Or, in other words: attacks against the ATM itself or the people involved with the ATM (Safe Vault, replenishment tasks); or those attacks on the PC stored inside the ATM or any of its peripherals. While the physical attacks often attract attention due to their dramatic nature, it is those f**raud attempts on ATMs that are more frequent and present a greater financial risk**.

Understanding the difference between both is crucial for designing and implementing a comprehensive and effective protection strategy that addresses both physical and cyber vulnerabilities.

In the following pages, we will explore the differences between them, the most common attack methods, and how financial institutions can protect themselves.

2 ATM attacks: classification

Physical Attacks

Their main characteristic is that they involve the use of physical force on, or even destruction of the ATM.

But, despite their spectacular nature, this type of attack only accounts for a small proportion - 5% - of the total losses related to crimes against ATMs worldwide, according to the European Association for Secure Transactions.

Types of physical attacks

- **Raids** or use of heavy machinery to destroy and access the ATM.
- **Explosions** using gas or solid explosives to break open the ATM.
- **Theft** of the entire ATM itself to access the cash and/or software.
- **Access to the safe** deposit box using tools and equipment**.**
- **Assault on armoured vans** that transport cash to or from the ATM.

How to avoid it?

To address this risk, institutions invest heavily in physical security measures such as **reinforced ATM structures**, advanced locking mechanisms, surveillance systems, or packets of ink or glue that render-stolen money unusable.

Fraud attempts

Fraud attempts are responsible for most financial losses associated with ATMs: on average, more than €500 per ATM per year across Europe.

There are two types of ATM fraud attempts to defend against: hardware (black box) attacks, where malicious hardware accessories, generally known as a 'black box,' are connected to the ATM and used to bypass security measures causing, for instance, the cash dispenser to release money without legitimate authorisation; and software attacks, where malware is key to this type of threat.

Types of fraud attacks

- **Skimming:** This involves capturing card details and PIN numbers.
- **Jackpotting:** The ATM dispenser is instructed to dispense cash in an unauthorised manner.
- **Network attacks:** The communication systems between the ATM and the bank's core systems are intercepted and manipulated.
- **Card retention:** The card is retained within the device and, later, the criminals recover it to use it fraudulently. Another version of this attack is to make the ATM retain the money that the user tries to withdraw, and for the criminal to then return to recover it later.
- **Shimming:** Devices are inserted into the card reader to read the information from the chip without being detected.

"Banks must remain alert to attacks on their ATMs. These can cause not only large financial losses, but also irreparable damage to their reputation. Implementing robust cybersecurity measures and proactively managing threats is essential to protect access to banking services and customer trust in a financial institution".

Néstor Santolaya Bea
Cybersecurity Product Expert, Auriga

What is malware?

Malware is any type of computer software that is used with the intention of damaging the device or conducting fraudulent activities. In the case of malware specially designed to attack ATMs, the difference is that one of its main targets is the XFS (eXtended Financial Services) layer, something that other generic malicious codes do not have access to.

It is by attacking the XFS that cyber criminals can execute different functions, from stealing or intercepting data (such as card details or PIN numbers) to manipulating ATM functions to dispense money without authorisation.

How to avoid?
To address the vulnerabilities associated with fraud attacks, continuous vigilance and proactive security measures are required by banks and ATM operators.
They must enforce strict software update policies, adopt a **Zero-Trust approach** to ATM security, conduct regular security audits, and implement operating system hardening techniques.

This proactive approach helps maintain the integrity and security of customers' financial transactions, ensuring ongoing defence against existing and future cyber threats.

In the next few pages, we will look at more details about banking-specific malware and how it works.

3 ATM malware

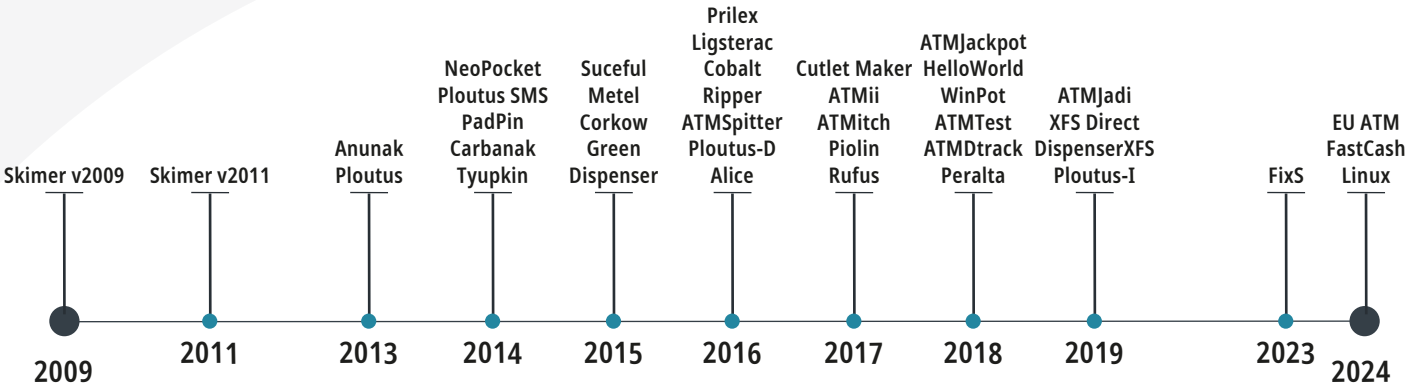
History of malware
The development of ATM-specific malware has kept pace with the security measures implemented by banks. Initially, the malware was made up of simple lines of code, but over time, they have transformed into highly sophisticated programmes capable of infecting ATMs from different providers at the same time, resulting in substantial financial losses for banks. They have even become easy to use by non-technical people, which contributes to their indiscriminate expansion.

Losses to financial institutions resulting from some types of malware over the last two decades are in the billions and affect all types of entities and in any location. The first sample of ATM-specific malware was detected in 2009, shortly after the global financial crisis of 2008.

However, it was not until four years later, in 2013, that there was a noticeable increase in attacks on ATMs. Since then, more than thirty new variants of ATM malware families were identified, each with new or improved features to bypass security measures, extract cash, and avoid detection by security software.

There are currently around fifty active variants identified.

FASTcash malware alone is suspected of having stolen $2 billion from banks in Asia and Africa. The various Ploutus variants, meanwhile, have cost banks in Latin America, Europe, and the United States a total of more than $450 million.



How does ATM-specific malware operate?

When designed to infect ATMs, malware has several specific features that enable it to execute sophisticated attacks on these devices.

Its success depends on malware's ability to adapt, evade defences, and operate stealthily within ATMs and the supporting ATM infrastructure. Let's look at these features in detail:

MULTIVENDOR SUPPORT:

ATM malware is carefully designed to be able to operate across different hardware and software configurations from different manufacturers. This adaptability allows the malware to execute sophisticated attacks on a wide variety of ATM systems.

UNAUTHORISED CASH AND DATA CAPTURE:

Malware captures customer card data, including magnetic stripe or chip data, and intercept PIN entries by keystroke logging (skimming). In addition, it can issue commands directly to the ATM's cash dispenser, allowing unauthorised cash withdrawals (jackpotting).

COMMUNICATION AND CONTROL:

Some malware can communicate with remote servers by compromising ATMs remotely. By using remote access tools (RAT), criminals can execute commands and access critical data to completely control the device and the entire ATM network as well.

OVERCOMING SECURITY:

ATM malware employs sophisticated mechanisms designed to evade detection and overcome security measures implemented by financial institutions, such as antivirus software, firewalls, and intrusion detection systems. This capability facilitates prolonged exploitation and unauthorised activity without triggering alarms or detection mechanisms.

STEALTH & PERSISTANCE:

Malware designed to attack ATM systems uses anti-forensic tactics to delete or alter records, covering its tracks and complicating investigative efforts. It camouflages itself within the ATM's own software infrastructure, masquerading as legitimate code to evade detection. In addition, this kind of malware can be persistent across system reboots and updates.

The life cycle of a malware attack

In the security field, understanding the lifecycle phases of fraud attacks is essential to developing effective defence strategies and enabling security professionals to develop proactive measures.

Research and Development Phase

Attackers prepare by gathering as much information as possible about the targeted ATMs. This includes identifying model-specific vulnerabilities and configurations used that they could exploit for malicious purposes. To achieve this, attackers use stolen intellectual property such as unencrypted ATM disks or software images, which will serve as a basis for reverse engineering processes that allow them to analyse and exploit the vulnerabilities.

Infection Phase

Malware distribution mechanisms are varied and may involve physical access to the ATM hardware or remote access through network vulnerabilities:

Physical Infiltration

This method involves direct access to the ATM hardware or peripherals. Attackers can introduce malware using CD or USB drives, modify images of stolen hard drives, or connect to the ATM back-end. Ploutus is one of the most well-known malware systems that can be distributed using one of these methods. Others such as Skimer, Ligsterac, Padpin, Tyupkin, Alice and FiXS operate in the same way.

Network Infiltration

The infection occurs remotely, taking advantage of vulnerabilities in the ATM's network infrastructure or in the bank's general systems. Legitimate remote connection tools or authorised software distribution systems are used to spread the malware. This method is fast and efficient in infecting multiple ATMs connected to the same network. Anunak, Carbanak, Cobalt, Ripper, ATMii, ATMSpitter, Dtrack, ATMDtrack and ATMJaDi are some of the remote connection systems used for malware distribution.

Attack Phase

Attackers consolidate control over compromised systems and execute a sequence of manoeuvres to achieve their illicit objectives — such as jackpotting (where cash is dispensed illegally) or skimming, which involves capturing sensitive data from users' cards — and then cover their tracks to evade detection. This phase can also occur physically or remotely. Physical activation may involve the manipulation of numeric keypads or the use of wireless keyboards and mice, while remote activation may involve sending remote commands to the ATM or exploiting legitimate credit card data obtained from compromised SWIFT servers.

The implementation of robust security protocols, continuous monitoring systems, and subsequent forensic practices are essential to mitigate risks and safeguard the integrity of ATM operations.

How far ATM malware can go

As we've already explained, there are many and varied families of ATM malware in existence, each with its own special additional characteristics to suit specific situations. These can be categorised into five main areas:

Data capture and theft:
These can include logging keystrokes to steal PINs and other sensitive data, gaining access to browser data that may contain session tokens, and monitoring system processes and files for valuable information.

System and hardware manipulation:
Some can trick ATM hardware into bypassing security mechanisms by spoofing hardware, disabling, or manipulating sensors to avoid detection, and controlling the card reader to retain or eject credit cards.

Network and service disruption:
These can cause the ATM network to be overloaded by, for example, a denial-of-service attack. This can cut off network connectivity to isolate it and create unauthorised web services for remote control of ATMs or extract sensitive data linked to ATM systems.

Security evasion and data erasure:
Many malware families go beyond basic obfuscation by removing evidence of their activities and are specifically designed to erase data to prevent recovery and even alter or delete the Master Boot Record (MBR), to obstruct effective forensic analysis.

Other functionalities:
These can include disabling alarms to avoid alerting security personnel, enabling remote control for real-time manipulation of the ATM, stealing ATM operator credentials to access the ATM, and encrypting data transmitted by the malware to prevent detection by network monitoring tools.

4 How to protect ATMs

Protecting ATMs under the traditional model

The traditional approach to protecting ATMs against threats encompasses several key strategies.

Encrypting the hard drive to ensure that the information on it cannot be modified outside the operating system. All information thus remains unreadable to anyone without the decryption key. This ensures that customer data, transaction records and other sensitive information are stored securely and inaccessible to unauthorised persons or attackers attempting to gain physical access to the ATM.

Applying hardware restrictions: This involves protecting the physical components of the machine to prevent tampering or unauthorised access, including disabling or blocking unused USB ports and other physical interfaces that could be used to introduce malicious devices or for unauthorised access.

Implementing antivirus and firewall software: This is to protect the systems themselves, and to safeguard the integrity of the ATM network and connections.

Specific solutions such as Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) systems improve security in this traditional approach. Additionally, the execution of malicious software should be limited by whitelisting techniques.

Always update! Frequent updates to the operating system and hardware are necessary to prevent zero-day attacks and avoid vulnerabilities that can be exploited by cybercriminals.

Continuous monitoring: It is important to monitor and record all operations performed on the ATM to detect any suspicious activity and allow a real-time response. Intrusion detection systems (IDS) further improve security by continuously monitoring network traffic and system logs for indicators of suspicious activity.

Zero-Trust ATM Protection

Zero-Trust Protection represents a **change in thinking from the traditional security approach**, aiming to mitigate the vulnerabilities and limitations inherent in conventional ATM protection strategies.

This approach limits access and any type of action to any unauthorised person, minimising the risk of unauthorised access to any point in the processes or systems.

Never trust the Software Distribution System: Frequent system updates, necessary to prevent zero-day attacks, depend on the software distribution system, which has historically been a significant vulnerability in ATM malware infections at the network level. In addition, the required availability of ATMs does not always allow them to be continuously updated with the latest policies, critical patches, and operating system updates.

> *"While traditional methods are based on perimeter defences and trust assumptions, Zero-Trust takes a fundamentally sceptical stance, assuming that every aspect of the ATM environment could potentially be compromised".*
>
> **Néstor Santolaya Bea**
> Cybersecurity Product Expert, Auriga

Never trust anyone with physical access to the ATM: Zero-Trust extends hardware protection beyond traditional measures by requiring rigorous certification of all ATM hardware components, ensuring that only devices that meet strict security criteria are authorised to operate, regardless of the physical ports they connect to.

Protect the ATM like an industrial device: On the software side, Zero-Trust is addressed by transforming the ATM operating system from a general-purpose IT (information technology) environment to a purpose-built OT (operational technology) system. This strategic shift significantly reduces the attack surface by strictly limiting software operations to only those essential to the ATM's functionality, effectively isolating critical processes. This not only protects the integrity of the file system, ensuring strict control over the processes that can access and modify files, but also facilitates the implementation of a rigorous application whitelist.

Be wary of anything that does not serve the ATM's operation: In the Zero-Trust model, the emphasis is not on maintaining an exhaustive database of malware hashes, as traditional approaches typically do, but instead focuses on strong access controls to detect and mitigate threats in real time. This proactive stance not only provides effective protection against new and unknown malware, but also protects against the misuse of legitimate tools unnecessary for ATM operations that are often exploited in ATM-related attacks.

5 How can Auriga help?

Financial institutions face a wide variety of challenges in making ATMs available 24 hours a day and ensuring maximum security. To do so, they need to develop a cybersecurity programme that understands the business context, the technical infrastructure supporting critical functions, and related cybersecurity threats. Auriga provides the necessary tool to ensure ATM protection against not only the known malware, but also for the new ATM malware families that are yet to come.

Lookwise Device Manager: The tailored ATM solution

Lookwise Device Manager (LDM) is the centralised and modular solution specifically designed for ATM network security.

The solution provides a **comprehensive set of features** to ensure the protection and monitoring of a bank or independent ATM operator's critical devices.

It adds an additional layer of control that allows users to execute customised remote actions to investigate or react to potential incidents.

In addition, this remote management also makes it possible to **protect and correct any deviations detected on the ATM from the default software image** in a previously established laboratory environment.

By implementing an effective operational technology cybersecurity strategy, it is possible to protect critical devices and comply with regulations at the same time without impacting operations.

The LDM security model:

- Protects the software image of the device, monitoring and correcting its deviations and ensuring the reduction of attack vectors by converting the operating system into a special-purpose operational technology (OT) type system. In addition, 100% of encrypted hard drives maintain the integrity of the software.

- Integrates seamlessly with ATM maintenance tasks, allowing for the monitoring and approval of software and hardware modifications, in accordance with the Zero-Trust principle applied to the maintenance team.

- Ensures software distribution and update tasks, certifying not only the distribution system, but also each distributed package, in accordance with the Zero-Trust concept applied to the distribution system.

- Securely centralises the ATM's daily tasks, saving costs and reducing vulnerability windows to a minimum by not having to relax protection to carry them out, since the status of the ATM can be monitored and there is a real-time response capacity to any attack.

LDM centralises the security of the network of devices, thus guaranteeing efficient control. In addition, by concentrating security operations on a single platform, a minimal impact on device performance is achieved. In this way, centralised control is maintained over software and hardware changes with integrated visibility and management of the network status and an increase in overall availability.

By implementing LDM, banks and other ATM operators can achieve a 98.4% uptime optimisation of their entire ATM network.

lookwise
DEVICE MANAGER

AURIGA
the banking e-volution

Building 3, 566 Chiswick High Road
London W4 5YA - United Kingdom
london@aurigaspa.com
www.aurigaspa.com