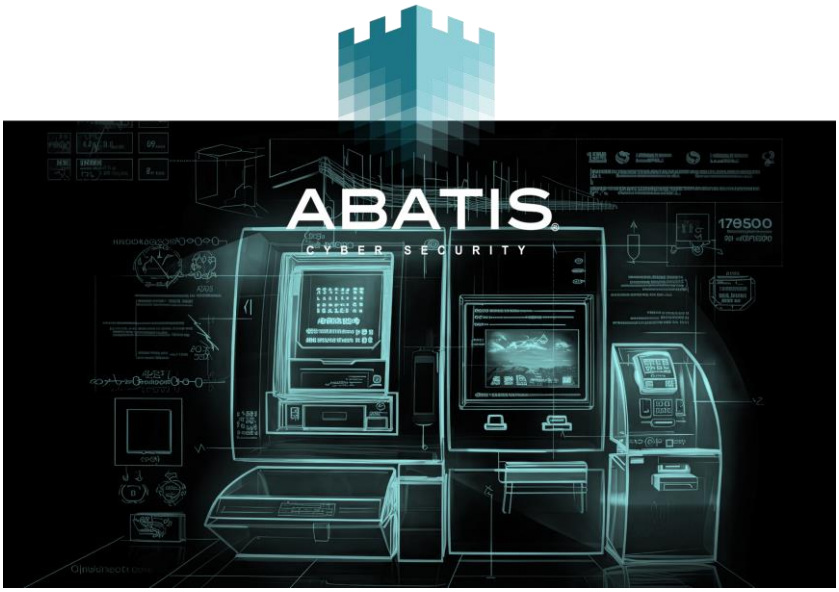

Securing Automatic Teller Machine (ATM) Networks in 2025

FS-ISAC | AFFILIATE

ABSTRACT

This white paper delves into the modern attack strategies targeting ATMs, showcasing real-world incidents that underscore the urgency of the issue.

Alexander Rogan, CEO

Platinum High Integrity Technologies Limited | Kemp House, 152 - 160 City Road, London, EC1V 2NX.

alexander.rogan@platinum-hit.com | www.platinum-hit.com

Contents

Addressing Modern Cyber Threats and Legacy Challenges

Introduction

The security of Automatic Teller machines (ATM) networks is an urgent priority for financial institutions globally. While traditional threats like skimming and card cloning have been effectively countered over the years, today's attacks have evolved, becoming more sophisticated and exploiting outdated vulnerabilities and gaps in existing security measures.

This white paper delves into modern attack strategies targeting ATMs, showcasing real-world incidents that underscore the urgency of the issue. It also highlights legacy systems' significant challenges and the constantly changing regulatory landscape. By presenting comprehensive strategies for enhancing endpoint security, this paper aims to equip institutions with the tools necessary to build a resilient and secure ATM network.

A Brief History of ATM Cyber Attacks

- **Early Attacks**
  Initial threats focused on physical security, such as skimming devices used to steal magnetic stripe data and PINs.

- **Logical Attacks**
  Malware like Ploutus and Black Box introduced software-based compromises, bypassing physical safeguards to manipulate ATM hardware.

- **Hybrid Attacks**
  Modern attackers combine physical tampering with network-based exploits. For example, they may replace ATM hardware to install malware that communicates with remote servers for command and control.

- **Insider Threats**
  Employees or contractors with privileged access may exploit their roles to deploy malware, manipulate systems, or steal sensitive data.

Notable Real-World ATM Attacks

Carbanak Cybercrime Group (2013–2018)

Summary - Phishing campaigns infiltrated bank networks, allowing remote control of ATMs. Losses exceeded $1 billion.

Implications - Highlighted the dangers of phishing and weak internal network protections.

$45 Million ATM Cash-Out Scheme (2012–2013)

Summary - Attackers manipulated backend systems to eliminate withdrawal limits, enabling mass cashouts.

Implications - Exposed vulnerabilities in card management and backend processes.

Ploutus.D Jackpotting Attacks (2018)

Summary - Attackers physically accessed ATMs to install malware that dispensed cash on demand.

Implications - Demonstrated risks from physical access and unsecured legacy systems.

Cryptojacking on ATMs (2023)

Summary - Attackers exploited unpatched systems to install cryptocurrency mining software, significantly degrading ATM performance.

Implications - Highlighted non-traditional attacks leveraging ATM resources for financial gain.

Emerging Threats in ATM Cybersecurity

Broadening Attack Methodologies

- **Hybrid Attacks**
  Combine physical tampering with remote exploitation.

- **AI-Powered Attacks**
  Automate phishing, adapt malware in real-time and evade traditional defences.

- **Ransomware Targeting ATM Networks**
  Lockdown ATM operations until a ransom is paid.

- **Cryptojacking**
  Exploits ATM systems for unauthorised cryptocurrency mining, often using vulnerabilities in legacy operating systems.

ATM Network Vulnerabilities

- **Unencrypted Data Transmission**
  Legacy systems like Windows XP transmit sensitive transaction data without encryption, leaving it exposed to interception and theft.

- **Weak Encryption Protocols**
  Modern attackers easily compromise older protocols like SMBv1 and 128-bit RC4 encryption, allowing lateral movement within ATM networks and data exfiltration.

- **Flat Network Architectures**
  Many ATM networks lack segmentation, enabling attackers who gain access to one ATM to propagate malware across the network.

- **Unpatched Vulnerabilities**
  Modern operating systems like Windows 10 can harbour vulnerabilities (e.g., SMBv1 exploit EternalBlue), often unpatched in ATM environments due to operational constraints.

Evolution of Attack Vectors

- **Network-Based Attacks**
  Attackers infiltrate bank networks using phishing, credential theft, or exploiting vulnerabilities, moving laterally to compromise multiple ATMs.

- **Supply Chain Attacks**
  Malware is introduced through compromised vendor updates or maintenance services.

Implications for Financial Institutions

- **Financial Losses**
  Direct theft, regulatory fines, and reputational damage.

- **Operational Disruptions**
  Forensic investigations and mitigation efforts can lead to prolonged ATM downtime.

- **Regulatory Pressure**
  Heightened scrutiny from financial regulators demanding compliance with security standards like PCI DSS and GDPR.

Abatis Mitigation for Modern ATM Malware Families

ATM Attack	Deployment Method	Abatis Mitigation
Ploutus	USB installation or network exploitation.	Prevents unauthorised binaries from executing and enforces OS integrity.
Tyupkin	Installed via physical access, activated with input codes.	Blocks unauthorised file writes and script execution, preventing activation.
GreenDispenser	Uses false UI screens to facilitate cash withdrawals.	Ensures UI integrity and blocks unauthorised code execution.

Ransomware Targeting ATMs

- **Deployment Method**
  Encrypts ATM systems or locks operations.

- **Abatis Mitigation**
  Prevents ransomware payloads from executing and ensures system immutability.

Legacy System Vulnerabilities

Windows XP and Windows 7

- **Unencrypted Data:** Sensitive data is transmitted without encryption, making intercepting easy.

- **Outdated Protocols:** SMBv1 and weak encryption algorithms allow attackers to exploit networks.

Windows 10 and Beyond:

While more secure, unpatched vulnerabilities and compatibility issues with legacy hardware create risks.

Microsoft ending support for Windows 10 in **October 2025** forces banks into an expensive upgrade cycle.

Vendor Lock-In - Financial institutions are trapped in Microsoft's perpetual upgrade model, prioritising compliance over security improvements.

Expanding on Network Segmentation

Effective network segmentation can significantly reduce the attack surface:

- **Virtual Local Area Networks (VLANs):** Isolate ATMs from other systems on the bank's network.
- **Firewalls and IDS:** Deploy firewalls or intrusion detection systems at key network junctions to monitor and block suspicious activity.
- **Least Privilege Access:** Ensure only authorised users and applications can access ATM networks.

Building Resilient ATM Networks

Key Strategies

- **Proactive Endpoint Security:**
  Deploy technologies like Abatis to prevent malware execution and enforce system integrity.
- **Modern Encryption Protocols:**
  Replace outdated protocols with AES-256 or TLS 1.2/1.3 to secure data transmissions.
- **Network Segmentation:**
  Divide ATM networks into segments to limit the scope of potential breaches.
- **Legacy System Security:**
  Utilise Abatis to extend the secure lifecycle of older systems, reducing forced upgrades' cost and operational burden.

Addressing Regulatory Challenges

Evolving Requirements

- **PCI DSS Updates**
  Requires stronger encryption protocols, regular vulnerability scans, and secure software development practices.
- **GDPR and Data Privacy**
  Ensures sensitive data remains protected during ATM transactions.

- **DORA (Digital Operational Resilience Act)**
  Focuses on ensuring operational resilience across EU financial institutions.

Regional Variations

- **Europe**
  Emphasises data privacy and breach reporting.

- **United States**
  Focuses on operational resilience and critical infrastructure protection.

How Abatis Helps

Abatis delivers compliance-ready solutions that guarantee data integrity, eliminate malware threats, and enhance the security of legacy systems. Trust us to safeguard your operations and ensure peace of mind.

Future-Proofing ATM Security

Blockchain Technology

Blockchain technology features immutable transaction logs that enhance security by providing a tamper-proof record of all ATM activities. It also secures communication between ATMs and central servers through cryptographic protocols.

Quantum Encryption

To safeguard against future threats from quantum computing, adopting long-term solutions like post-quantum encryption is essential.

Abatis' exceptional flexibility ensures effortless integration with cutting-edge encryption technologies, making it a smart choice for securing your data.

The Business Model Trap

Microsoft's mandated upgrade cycles, exemplified by the impending cessation of support for Windows 10 in October 2025, highlight the issue of vendor lock-in. Financial institutions encounter significant expenses in their efforts to remain compliant while failing to adequately address fundamental vulnerabilities.

Abatis offers an alternative solution that enables secure operations across legacy and contemporary systems while reducing reliance on costly upgrades.

Call to Action

Financial institutions must take immediate action and adopt proactive and resilient cybersecurity solutions to safeguard ATM networks amid an increasingly complex threat landscape. The following steps are critical:

- **Evaluate Current Security Measures:**
  Conduct a comprehensive review of ATM networks, including operating systems, hardware, and network segmentation, to identify vulnerabilities.

- **Implement Proactive Solutions Like Abatis:**
  The transition from reactive to proactive endpoint protection ensures system integrity, prevents unauthorised changes, and blocks malware execution at the kernel level.

- **Future-Proof Security Strategies:**
  Explore emerging technologies such as blockchain for transaction logging and quantum encryption for long-term resilience against sophisticated threats.

- **Enhance Compliance Frameworks:**
  Align with evolving global regulations like PCI DSS, GDPR, and DORA to ensure robust data protection and operational resilience.

- **Invest in Employee Training and Insider Risk Management:**
  Educate staff on phishing risks, insider threats, and the importance of secure network practices to minimise human error.

- **Engage With Us:**
  Abatis is uniquely positioned to help financial institutions secure their ATM networks while reducing costs and breaking free from vendor lock-in cycles.

Contact us today for a consultation or to find out how our patented technology can secure the future of your operations.