Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

# ATM Jackpotting Attacks on the Rise

## SUMMARY

ATM malware is increasingly being used to commit a crime known as "jackpotting," in which attackers install malware that forces ATMs to dispense large amounts of cash on command.

## TAKE ACTION NOW

- Secure the hood with a pick-resistant key and alarm.
- Ensure network communications use TLS 1.2e encryption.
- Keep all components (operating system, firmware, software, etc.) up to date.
- Change all default passwords.

## CRITICAL ACTIONS & MITIGATION STEPS

- **Secure the Hood**
  - Use specially designed, pick-resistant keys to limit access and prevent the use of universal keys.
  - Install an alarm on the top hat of the ATM to alert you of a physical breach before a cash dispense occurs.
  - Include battery backup in case of power outages.
- **Secure the Basic Input/Output System (BIOS)**
  - Configure BIOS to boot only from the primary hard disk. Remove all other bootable devices from the boot order.
  - Password-protect all BIOS operations with unique, non-default credentials.
- **Establish a Strong Password Policy**
  - Change all default passwords. Each ATM should have unique credentials.
  - Require complex passwords that are updated every 90 days
- **Encrypt Communications**
  - Migrate existing systems to a secure TLS version, currently TLS 1.2e.
- **Install and Maintain a Firewall**
  - Configure firewalls to allow only authorized incoming and outgoing connections required for ATM operation.

    - Apply settings on a per-program basis rather than per port.
- **Remove Unused Services and Applications**
    - Apply the principle: "If you don't use it, disable it" to reduce attack surfaces.
- **Deploy Effective Anti-Malware Mechanisms**
    - Use white-listing solutions that offer protection against known and unknown threats, including memory protection and zero-day attack detection.
- **Establish a Regular Patching Process**
    - Keep all ATM software updated with the latest security patches to prevent exploitation of known vulnerabilities.
- **Harden the Windows Operating System (OS)**
    - Disable Windows AutoPlay.
    - Use locked-down user accounts for ATM applications with least-privilege access and no interactive desktop access.
    - Use keyboard disablers to prevent unauthorized input.
    - Apply file, folder, and registry permissions to restrict access to only what's necessary.
    - Use Group Policies to limit functionality to only what's needed for secure ATM operation.
- **Deploy Full Hard Drive Encryption** Full disk encryption protects against offline attacks by rendering the contents unreadable if:
    - The ATM is booted from removable media
    - The hard drive is removed and accessed externally
    - The ATM core is removed
- **Secure ATM Core-Dispenser Communication**
    - Encrypt communications between the ATM core and dispenser to prevent black box attacks.
    - Only authenticated commands from the ATM software stack should be processed.
- **Perform Annual Penetration Testing**
    - Engage a third-party security provider to perform a comprehensive penetration test annually.
    - Testing should simulate various attack scenarios to uncover vulnerabilities, misconfigurations, and weaknesses, helping you strengthen your ATM's overall security posture.

## JOIN US FOR AN IMPORTANT LET'S TALK FRAUD WEBINAR

Register now for a special Let's Talk Fraud **tomorrow, June 17th** where we will be discussing how to protect your ATMs against fraud.

## RISK MITIGATION RESOURCES

- White Paper: Armor Your ATMs
- Helpful links:
    - Sign up for our **Let's Talk Fraud** quarterly webinars
    - View additional risk resources

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net



LinkedIn