FBI FLASH

ACTIONABLE CYBER INTELLIGENCE

19 FEBRUARY 2026

FLASH Number
FLASH-20260219-001

Increase in Malware Enabled ATM Jackpotting Incidents Across United States

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate indicators of compromise (IOCs) and technical details associated with malware enabled ATM jackpotting. Threat actors exploit physical and software vulnerabilities in ATMs and deploy malware to dispense cash without a legitimate transaction. The FBI has observed an increase in ATM jackpotting incidents across the United States. Out of 1,900 ATM jackpotting incidents reported since 2020, over 700 of them with more than $20 million in losses occurred in 2025 alone. This FLASH is being provided to encourage organizations to implement the recommended mitigation steps and to outline the information requested from the public.

Technical Details

Overview

Threat actors are deploying ATM jackpotting malware, including the Ploutus family malware, to infect ATMs and force them to dispense cash. Ploutus malware exploits the eXtensions for Financial Services (XFS), the layer of software that instructs an ATM what to physically do. When a legitimate transaction occurs, the ATM application sends instructions through XFS for bank authorization. If a threat actor can issue their own commands to XFS, they can bypass bank authorization entirely and instruct the ATM to dispense cash on demand. As a result, Ploutus allows threat actors to force an ATM to dispense cash without using a bank card, customer account, or bank authorization. Once Ploutus is installed on an ATM, it gives threat actors direct control over the machine, allowing them to trigger cash withdrawals. Ploutus attacks the ATM itself rather than customer accounts, enabling fast cash-out operations that can occur in minutes and are often difficult to detect until after the money is withdrawn.

Common Methods of Infection

After gaining access to ATMs, most often by opening an ATM face with widely available generic keys, ATM jackpotting threat actors have used several main methods to deploy malware:

- Threat actors remove the ATM’s hard drive, connect it to their computer, copy the malware to the hard drive, return the hard drive to the ATM, and reboot the ATM.
- Threat actors remove the ATM’s hard drive, replace it with a foreign hard drive or other external device with preloaded malware, and reboot the ATM.

Malware Functionality

The malware interacts directly with the ATM hardware, bypassing any communications or security of the original ATM software. The malware does not require connection to an actual bank customer account to dispense cash. The malware can be used across ATMs of different manufacturers with very little adjustment to the code as the Windows operating system is exploited during the compromise.

Indicators of Compromise (IOCs)

Disclaimer: The FBI recommends organizations investigate and vet indicators prior to taking action.

Digital Indicators (as observed on affected ATMs running Windows OS)

- Executable files not expected on the hard drive, including, but not limited to, the following:
  - Newage.exe
  - Color.exe
  - Levantaito.exe
  - NCRApp.exe
  - sdelete.exe
  - Promo.exe
  - WinMonitor.exe
  - WinMonitorCheck.exe
  - Anydesk1.exe
  - Identified MD5s:
    - 2C2D16658D8DA6B389934273EF8F8E22
    - 5F177B84F3D92AB5711BE446125FDBE3
    - 61EECEB5F9186A0BC01DC82798CD6C5F
    - FDA82030AE92313E94B9339EA1FC107C
    - C04A7CB926CCBF829D0A36A91EBF91BD
- Associated Files and Scripts:
  - C.dat
  - Restaurar.bat
  - Restauraropteva.bat
  - Logcontrol.txt
  - Logc.txt
  - Borrar_beta.txt
- New directories, including, but not limited to, the following:
  - Anydesk1.exe Anydesk1.exe

  - C:\<ATM_Manufacture>\exe\p
  - C:\Users\SSAuto1\AppData\Local\P\

- Remote connection applications, such as TeamViewer or AnyDesk, if unauthorized; or application logs showing connections from unexpected IP addresses.

Persistence Mechanisms

- Abnormal autoruns:
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

- Custom services:
  - Custom service entries under:
    - HKLM\SYSTEM\CurrentControlSet\Services\
  - Services pointing to non-standard install paths
  - Services running under SYSTEM without vendor signature
  - Services running with generic or deceptive names:
    - ATM Service
    - Dispenser Service
    - DIEBOLDP IP addresses.

Physical Interaction Indicators

- USB insertion events:
  - Event ID 2003 -
    - May appear with the insertion of USB storage device, or peripheral
  - Event ID 6416 -
    - The Security log records the detection of a newly connected external device when external storage auditing is enabled. This event can indicate the attachment of removable media such as USB storage devices, but does not confirm file access or execution
  - Event ID 4663 -
    - The Security log may record file access or modification activity involving removable media, provided object access auditing is enabled and appropriate system access control lists (SACLs) are configured on the target files or directories

- Detection of:
  - USB keyboards
  - USB hubs
  - Flash drives

- Physical Indicators
  - ATM door open alerts outside of planned maintenance schedule
  - Low/No cash indicators outside of expected use schedule
  - Unauthorized devices plugged into the ATM
  - Removal of hard drives from ATMs
  - ATM unexpectedly out of service

A key validation step during ATM incident response is confirming whether file hashes match the organization's verified baseline. Each ATM should be deployed from a controlled "gold image" containing cryptographically verified executables, libraries, and configuration files approved by the vendor and the institution. Any deviation from these baseline hashes, particularly the presence of unsigned or newly introduced binaries, should be treated as a potential compromise. Maintaining and routinely validating system integrity against a gold image is one of the most effective defenses against ATM-targeted malware, as jackpotting threats often rely on locally introduced files that bypass traditional network-based detection.

Information Requested

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office at www.fbi.gov/contact-us/field-offices or the FBI Internet Crime Complaint Center at www.ic3.gov. If reporting an incident of jackpotting, please provide the following information:

Bank Information

- Bank name, branch, location, and contact information

ATM Information

- Manufacturer make and model
- Vendor name and contact information
- Available logging

Recommended Mitigations:

The FBI recommends a targeted audit policy focused on removable storage usage, controlled file access, and process creation providing high-fidelity detection of ATM jackpotting activity with minimal system overhead. When combined with gold image integrity validation, this approach enables early identification of physical intrusion and malware staging events that would otherwise evade network-based monitoring. The application of the following mitigations could limit potential adversarial use of the Ploutus malware family and reduce the risk of ATM jackpotting:

Physical Security

- Threat sensors on devices and vestibules
    - Installing vibration, temperature change, and other sensors to alert security personnel to suspicious activity
- Locks and keypads
    - Changing the standard locks on ATM devices to prevent the use of keys available for purchase online
    - Installing keypads on devices that set off alarms if a code is not entered when the maintenance hatch is opened
- Physical barriers
    - Installing additional keyed barriers that prevent the cashbox and maintenance hatch from being accessed
- Security cameras and footage
    - Ensuring security cameras cover necessary areas and preserve security footage recordings in the event of an incident

Hardware Security

- Automatic shutdown
    - Configuring security settings to take preventative action on the ATM when an established combination of IOCs for ATM Jackpotting is detected. Once a combination is identified for example, the ATM should enter an automatic shutdown or out of service status to prevent distribution of cash
- Device whitelisting
    - Whitelisting hardware devices could prevent connection of unauthorized devices, such as phones and hard drives

- Firmware Checks
  - Firmware integrity checks using digital signatures use the Trusted Platform Module 1.2 (ISO/IEC 11889-1:2009) to apply integrity checks at boot up time

- Disk encryption
  - Enabling hard drive encryption could prevent introduction of malware to an unplugged hard drive
  - Apply hardware level permissions between devices

- Track components
  - Track components using Software Bill of Materials and Hardware Bill of Materials for software and hardware integrity

- Memory integrity
  - Enabling memory integrity in Windows security settings

Logging

- If jackpotting risk exists, explicitly enable the following:
  - Audit Removable Storage
  - Audit Object Access (targeted SACLs only)

- Maintain logs
  - Maintaining logging and, if available, centrally storing it, could allow security personnel to detect suspicious activity quickly
  - Enabling removable media detection
    - Enable *Audit Removable Storage* under *Object Access* which is found in *Advanced Audit Policy Configuration*. This will trigger Event ID 6416 when a USB storage device is connected
    - Explore enabling *Audit File System* which results in Event ID 4663 and ONLY with SACLs applied to:
      - ATM Application Directory.... Audit RWX
      - Vendor middleware directories.... Audit WX
      - C:\users\Public\..... Audit WX
      - Any writeable service paths.... Audit WX
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit
    - ProcessCreationIncludeCmdLine_Enabled = 1
      - Results in Event ID 4688
      - Detection of unexpected executables
      - Correlation with USB insertion

      - Expands 4688 record to include the Process Command Line field
      - Audit Process creation must be enabled
      - Note: sensitive data passed in command line will be recorded Any writeable service paths.... Audit WX

  - Enabling *Audit Process Creation* under *Detailed Tracking*
    - Results in Event ID: 4688
      - Detection of unexpected executables.... Audit WX

  - Enable *Audit Security System Extension* and *Audit System Integrity* under *System*
    - Generating Event ID 1102, Security log cleared
    - Generating Event ID 4719, Audit Policy changed

- Preserve logs
  - Long periods of log retention could allow for greater insight if a suspicious event were to occur

- Log device state
  - Tracking the state of the ATM could further improve the security personnel’s ability to quickly detect suspicious activity

Possible logged attack example:

Step	Event
USB inserted	6416
Malware copied	4663
Malware executed	4688
Service installed	4697
Logs cleared	1102

Auditing

- Audit ATM devices
  - Security personnel should audit ATM devices to ensure all available security mechanisms are properly enabled

- Change default credentials
  - Changing default credentials can significantly impact the ability of subjects to get access to elevated permissions on the ATM devices

- Pre-production assessment
  - An audit of the device's updates and security implementations on a test device in a pre-production environment could ensure they are operating in an expected way

Network Security

- IP whitelisting
    - Whitelisting IP addresses could prevent the attackers from connecting to the ATM devices remotely

Endpoint Detection and Response

- Antimalware/Antivirus
    - Antimalware and antivirus software could assist in preventing the deployment of malware on ATM devices

- Software whitelisting

    Whitelisting software could give more granular control over what software is allowed to run on the ATM, which could further assist in preventing the deployment of malware

Threat Intelligence

- Maintenance schedule
    - Familiarization with software updates and physical maintenance schedules could allow security personnel to easily identify unusual activity

- Industry groups
    - Information sharing in the industry could keep security personnel updated about the threat landscape, including possible attack vectors and the need for relevant defenses

- Threat readiness and training
    - Training employees on the specifics of ATM jackpotting could result in better reporting and quicker responses to the threat

Reporting Notice

If you identify suspicious activity within your enterprise or have information related to the contents of this document, please contact your local FBI field office immediately at **www.fbi.gov/contact-us/field-offices**. The FBI also encourages you to report suspicious or criminal activity to the FBI Internet Crime Complaint Center at **www.ic3.gov**. When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Individual indicators included in this document should always be evaluated in light of your complete information security situation. Some indicators, particularly those of a nondeterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise.

Your organization has no obligation to provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistent with applicable state and federal law.

Administrative Note

The information in this document is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI.

Your feedback regarding this product is critical.

Please take a moment to complete the survey at the link below. Input can be submitted anonymously and should be specific to your experience with our written products.

https://www.ic3.gov/PIFSurvey

This survey is for feedback on contact and value only. Reporting of technical information regarding FLASH reports must be submitted through your local FBI field office.