SEGURIDAD EN CAJEROS AUTOMÁTICOS: UN RETO FÍSICO Y VIRTUAL

AURIGA
the banking e-volution

"Los bancos deben permanecer alerta ante los ataques a sus ATMs. Este tipo de incidentes puede causar no solo grandes pérdidas financieras, sino también un daño irreparable a su reputación. Implementar medidas de ciberseguridad robustas y realizar una gestión proactiva de las amenazas es esencial para proteger el acceso a los servicios bancarios y la confianza del cliente en la entidad financiera ".

Néstor Santolaya Bea
Cybersecurity Product expert de Auriga Iberia

Sumario

1 Introducción

Los cajeros automáticos o **ATM son la cara más visible de los bancos** y, muchas veces, también la más vulnerable, ya que pueden sufrir ataques como robos, destrozos o virus informáticos.

El rango de amenazas al que se enfrentan puede ser clasificado en dos grandes categorías:

- Ataques contra la propiedad
- Intentos de fraude

O, lo que es lo mismo: ataques de fuerza contra la propiedad del banco (ATM, caja fuerte, efectivo) frente a ataques al servicio que ofrece (datos del cliente, efectivo). Y, aunque los ataques físicos suelen llevarse la atención por su naturaleza dramática, **los intentos de fraude son más frecuentes y presentan un mayor riesgo financiero**.

Entender la diferencia entre ambos es crucial para diseñar e implementar una estrategia de protección completa y eficaz que aborde tanto las vulnerabilidades físicas como las cibernéticas.

A lo largo de las siguientes páginas exploraremos las diferencias entre ambos, las modalidades de ataque más frecuentes y cómo las entidades financieras pueden protegerse.

2 Tipos de ataques a cajeros

Ataques contra la propiedad

Su principal característica es que implican el uso de la fuerza física o la destrucción.

Pero, a pesar de su espectacularidad, este tipo de ataques supone solo una pequeña proporción (un 5% " según la **Asociación Europea para las Transacciones Seguras** " de las pérdidas totales relacionadas con crímenes contra cajeros en todo el mundo).

Tipos de ataques

Las modalidades de ataques contra la propiedad utilizadas más frecuentemente son:

- **Alunizajes** o uso de vehículos para destruir y acceder al cajero.
- **Explosiones** utilizando gas o explosivos sólidos para abrir el cajero.
- **Robo del propio cajero** al completo para poder acceder al efectivo y/o al software que hay en su interior.
- **Acceso a la caja de seguridad** mediante herramientas y equipos.
- **Asalto a furgones blindados** que transportan el efectivo desde o hacia el cajero.

Cómo evitarlos

Para hacerle frente a este riesgo, las instituciones realizan grandes inversiones en medidas de seguridad física como pueden ser **el refuerzo de las estructuras del ATM**, mecanismos de bloqueo avanzados, sistemas de vigilancia o paquetes de tinta o pegamento que hacen que el dinero robado sea inutilizable.

Intentos de fraude

Los intentos de fraude son responsables de la mayor parte de las pérdidas económicas asociadas con los cajeros automáticos: de media, más de 500€ por cajero al año en toda Europa.

A su vez, se pueden categorizar en 2 tipos, los de Hardware (Black box), donde se utilizan accesorios de hardware maliciosos conocidos en general como 'caja negra' que una vez conectados al ATM eluden las medidas de seguridad y consiguen que, por ejemplo, el dispensador de efectivo expulse dinero sin autorización legítima y por otro lado los de Software, donde el malware es la clave en este tipo de amenazas.

Tipos de ataques

Algunos ataques de fraude comunes en ATMs son

- **Skimming:** Consiste en la colocación en el cajero de algún tipo de dispositivo capaz de capturar los detalles de las tarjetas y los números PIN.
- **Jackpotting:** Se infecta el software del ATM para hacer que dispense efectivo de manera no autorizada.
- **Ataques de red:** Se interceptan y manipulan los sistemas de comunicación entre el cajero y los sistemas *core* del banco.
- **Retención de la tarjeta:** Se retiene la tarjeta dentro del dispositivo y, más tarde, los malhechores la recuperan para utilizarla de manera fraudulenta. Otra modalidad es, directamente, la retención del dinero que el usuario intenta extraer.
- **Shimming:** Se insertan dispositivos en el lector de tarjetas para leer la información del chip sin ser detectados.

"Los bancos deben permanecer alerta ante los ataques a sus ATMs. Este tipo de incidentes puede causar no solo grandes pérdidas financieras, sino también un daño irreparable a su reputación. Implementar medidas de ciberseguridad robustas y realizar una gestión proactiva de las amenazas es esencial para proteger el acceso a los servicios bancarios y la confianza del cliente en la entidad financiera".

Néstor Santolaya Bea
Cybersecurity Product expert de Auriga Iberia

¿Qué es malware?

Como ya sabemos, denominamos malware a cualquier tipo de software informático que se use con intención de dañar el dispositivo o realizar actividades fraudulentas. En el caso de los malwares especialmente diseñados para la banca, la diferencia es que uno de sus principales objetivos es la capa XFS (eXtended Financial Services), algo a lo que no tienen acceso otros códigos maliciosos genéricos. Es desde ahí desde donde suelen ejecutar distintas funciones, desde el robo o interceptación de datos (como detalles de tarjetas o números PIN) hasta la manipulación de las funciones del cajero para dispensar dinero sin una autorización.

Cómo evitarlos

Para abordar las vulnerabilidades asociadas con los ataques de software se requiere una vigilancia continua y medidas de seguridad proactivas.

Las instituciones financieras deben aplicar estrictas políticas de actualización de software, adoptar un **enfoque de confianza cero** para la seguridad de los cajeros automáticos, realizar auditorías de seguridad periódicas e implementar técnicas de fortalecimiento del sistema operativo.

Este enfoque proactivo ayuda a mantener la integridad y la seguridad de las transacciones financieras de los clientes, lo que garantiza una defensa permanente contra las amenazas cibernéticas existentes y futuras.

En las próximas páginas veremos más detalles sobre el malware específico para la banca y cómo funciona.

3 El malware en cajeros

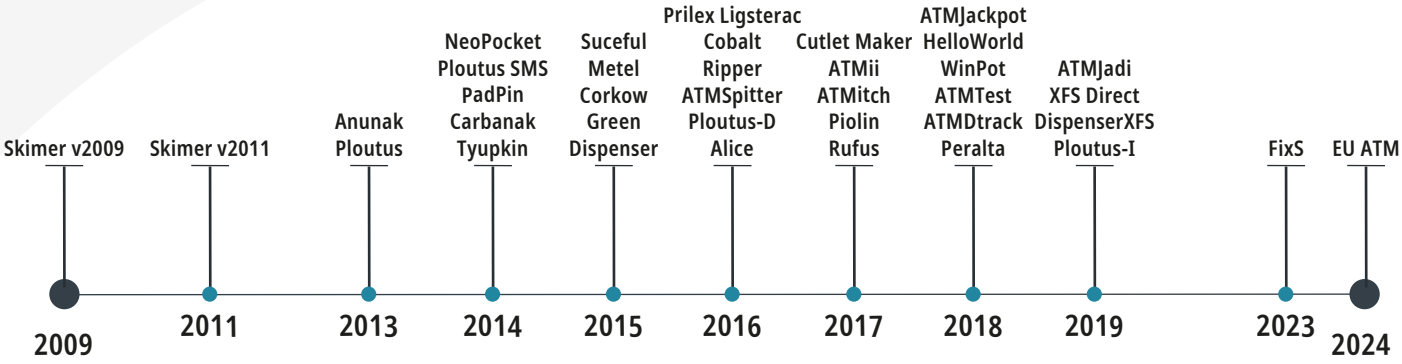
Historia del malware

El desarrollo de malware específico para cajeros automáticos ha evolucionado al mismo ritmo que lo hacían las medidas de seguridad implementadas por los bancos. Inicialmente estos malwares eran simples fragmentos de código, pero con el tiempo se han transformado en programas altamente sofisticados capaces de infectar cajeros de distintos proveedores al mismo tiempo, resultando en sustanciales pérdidas financieras para los bancos. Incluso se han vuelto fáciles de usar por personas sin conocimientos técnicos, lo que contribuye a su expansión indiscriminada.

Las pérdidas en instituciones financieras a manos de algún tipo de malware a lo largo de las dos últimas décadas son milmillonarias, y afectan a todo tipo de entidades y en cualquier localización. La primera muestra de malware específico para cajeros automáticos se detectó en 2009, poco después de la crisis financiera mundial de 2008.

Sin embargo, no fue hasta cuatro años después, en 2013, cuando se produjo un aumento patente de los ataques a cajeros automáticos. A partir de entonces ‘y en los cinco años posteriores,’ se identificaron más de 30 nuevas variantes de familias de malware para cajeros, cada una de las cuales presentaba características nuevas o mejoradas para eludir las medidas de seguridad, extraer efectivo y evitar la detección por parte del software de seguridad. Actualmente hay identificadas alrededor de 50 variantes en activo.

Se sospecha que solo el malware Fastcash permitió el robo de 2.000 millones de dólares de bancos en Asia y África. Las distintas variantes de Ploutus, por su parte, han hecho perder un total de más de 450 millones de dólares a bancos en América Latina, Europa y Estados Unidos.



Una radiografía del malware específico para cajeros

El malware diseñado para infectar cajeros automáticos tiene varias características específicas que le permiten ejecutar ataques sofisticados a estos dispositivos. Su éxito depende de su capacidad para adaptarse, evadir las defensas y operar de manera sigilosa dentro de las infraestructuras. Veamos en detalle cuáles son esas características:

Compatibilidad con múltiples proveedores

El malware para cajeros automáticos está diseñado meticulosamente para poder funcionar en distintas configuraciones de hardware y software de diferentes fabricantes. Esta adaptabilidad permite que el malware ejecute ataques sofisticados en una amplia variedad de sistemas de cajeros automáticos.

Extracción no autorizada de datos y efectivo

Está diseñado para capturar datos de las tarjetas de los clientes, incluidos los datos de la banda magnética o el chip, e interceptar las entradas de PIN mediante el registro de pulsaciones de teclas (skimming). Además, puede emitir comandos directamente al dispensador de efectivo del cajero automático, lo que permite extraer efectivo de manera no autorizada (jackpotting).

Comunicación y control: Puede comunicarse con servidores remotos comprometiendo los cajeros a distancia. Al utilizar herramientas de acceso remoto (RAT), los malhechores pueden ejecutar comandos y acceder a datos críticos hasta controlar totalmente el dispositivo y, tal vez también toda la red de cajeros.

Evasión de la seguridad

El malware para cajeros automáticos cuenta con mecanismos sofisticados destinados a evadir la detección y superar las medidas de seguridad implementadas por las instituciones financieras, como el software antivirus, los cortafuegos y los sistemas de detección de intrusiones. Esta capacidad facilita la explotación prolongada y las actividades no autorizadas sin activar alarmas ni mecanismos de detección.

Sigilo y persistencia

El malware diseñado para atacar sistemas de ATMs emplea tácticas antiforenses para eliminar o alterar registros, cubriendo sus huellas y complicando los esfuerzos de investigación. Se camufla dentro de la propia infraestructura de software del cajero haciéndose pasar por código legítimo para evadir la detección. Además, puede ser persistente ante reinicios y actualizaciones del sistema.

El ciclo de vida de un ataque de malware

En el ámbito de la seguridad, comprender las fases del ciclo de vida de los ataques de fraude es esencial para desarrollar estrategias de defensa eficaces y permitir a los profesionales de seguridad desarrollar medidas proactivas.

Fase de investigación y desarrollo

Los atacantes se preparan recopilando toda la información posible sobre los cajeros automáticos objetivo. Esto incluye la identificación de vulnerabilidades específicas de cada modelo y las configuraciones utilizadas que podrían explotar con fines maliciosos. Para lograrlo, pueden utilizar propiedad intelectual robada como discos de cajeros automáticos sin cifrar o imágenes de software, que les servirá como base para los procesos de ingeniería inversa que les permitan analizar y explotar las vulnerabilidades.

Fase de infección

Los mecanismos de distribución del malware son variados y pueden implicar el acceso físico al hardware del cajero automático o remoto a través de vulnerabilidades de la red:

Físico

Este método implica el acceso directo al hardware o los periféricos del cajero. Los atacantes pueden introducir el malware mediante unidades de CD o USB, modificar imágenes de discos duros robados o explotar vulnerabilidades utilizando dispositivos como computadoras de placa única o teléfonos móviles conectados al back-end del cajero. Ploutus es una de las familias de malware más conocidas que puede ser distribuida con uno de estos métodos. Otros como Skimer, Ligsterac, Padpin, Tyupkin, Alice y FiXS también utilizan este método.

Red

La infección se produce de forma remota, aprovechando las vulnerabilidades de la infraestructura de red del cajero o de los sistemas generales del banco. Para propagar el malware se utilizan herramientas de conexión remota legítimas o sistemas de distribución de software autorizados. Este método es rápido y eficiente para infectar varios ATM conectados a la misma red. Anunak, Carbanak, Cobalt, Ripper, ATMii, ATMSpitter, Dtrack, ATMDtrack y ATMJaDi son algunos de los ejemplos de malware que se distribuyen mediante este sistema.

Fase de ataque

Los atacantes consolidan su control sobre los sistemas comprometidos y ejecutan una secuencia de maniobras para lograr sus objetivos ilícitos —como el jackpotting (donde se dispensa dinero en efectivo de manera ilícita) o el skimming, que implica capturar datos confidenciales de las tarjetas de los usuarios—; y, después, eliminan el rastro para cubrir sus huellas y evadir la detección. Esta fase también puede desarrollarse de manera física o remota. La activación física puede implicar la manipulación de teclados numéricos o el uso de teclados y ratones inalámbricos, mientras que la remota supone explotar los datos legítimos de tarjetas de crédito obtenidos de servidores SWIFT comprometidos.

La implementación de protocolos de seguridad sólidos, sistemas de monitorización contínua y prácticas forenses posteriores son esenciales para mitigar los riesgos y salvaguardar la integridad de las operaciones de los cajeros.

Hasta dónde puede llegar el malware en cajeros automáticos

Como ya hemos explicado, son muchas y variadas las familias de malware para cajeros automáticos existentes, cada una de ellas con sus propias características especiales adicionales para adaptarse a situaciones específicas. Estas capacidades únicas se pueden clasificar en cinco áreas principales:

Captura y robo de datos: Pueden incluir el registro de pulsaciones de teclas para robar PIN y otros datos confidenciales, obtener acceso a datos del navegador que pueden contener tokens de sesión y supervisar los procesos y archivos del sistema en busca de información valiosa.

Manipulación del sistema y del hardware: Algunos tienen la capacidad de engañar al hardware del cajero automático para que eluda los mecanismos de seguridad mediante la suplantación de hardware, la desactivación o manipulación de sensores para evitar la detección, y el control del lector de tarjetas para retener o expulsar las tarjetas de crédito.

Interrupción de la red y del servicio: Pueden provocar la sobrecarga de la red del cajero automático para un ataque de denegación de servicio, el corte de la conectividad de red para aislarlo y la creación de servicios web no autorizados para el control remoto o la exfiltración de datos.

Evasión de seguridad y borrado de datos: Muchas familias de malware van más allá de la ofuscación básica al eliminar evidencia de sus actividades, y están diseñados específicamente para borrar datos que eviten la recuperación e incluso alterar o eliminar el Registro de Arranque Maestro (MBR), lo que complica enormemente el análisis forense.

Otras funcionalidades: Pueden incluir la desactivación de alarmas para evitar alertar al personal de seguridad, habilitar el control remoto para la manipulación en tiempo real del cajero automático, robar credenciales del operador del cajero automático para acceder a él y cifrar los datos transmitidos por el malware para evitar que las herramientas de monitorización de la red los detecten.

4 Cómo proteger los ATMs

La protección de los ATMs según el modelo tradicional

El enfoque tradicional para proteger los cajeros automáticos contra amenazas abarca varias estrategias clave:

Cifrado del disco duro para garantizar que la información que contiene no pueda modificarse fuera del sistema operativo. De este modo, toda la información permanece codificada e ilegible para cualquier persona que no cuente con la clave de descifrado. Esto garantiza que los datos de los clientes, los registros de transacciones y otra información confidencial se almacenen de forma segura y sean inaccesibles para personas no autorizadas o atacantes que intenten obtener acceso físico al cajero automático.

Aplicación de restricciones al hardware: Implica proteger los componentes físicos de la máquina para evitar la manipulación o el acceso no autorizado, lo que incluye deshabilitar o bloquear puertos USB no utilizados y otras interfaces físicas que podrían usarse para introducir dispositivos maliciosos o para el acceso no autorizado.

Implementación de un software antivirus y cortafuegos: Por un lado para proteger los sistemas en sí, por el otro para salvaguardar la integridad de la red y las conexiones del cajero.

Soluciones específicas como los sistemas *Endpoint Detection and Response (EDR) o Extended Detection and Response (XDR)* para mejorar la seguridad en este enfoque tradicional. Además, la ejecución de software peligroso debe limitarse mediante técnicas de listas blancas.

Actualización, ¡siempre!: Las actualizaciones frecuentes del sistema operativo y del hardware son necesarias para evitar ataques de día cero y evitar vulnerabilidades que puedan ser explotadas por parte de cibercriminales.

Monitorización continua: Es importante supervisar y registrar todas las operaciones realizadas en el cajero automático para detectar cualquier actividad sospechosa y permitir una respuesta en tiempo real. Los sistemas de detección de intrusiones (IDS) mejoran aún más la seguridad al monitorizar continuamente el tráfico de la red y los registros del sistema en busca de indicadores.

La protección de los ATMs según el modelo Zero Trust

La Protección Zero Trust (de Confianza Cero) representa **un cambio de paradigma con respecto al enfoque de seguridad tradicional,** que apunta a mitigar las vulnerabilidades y limitaciones inherentes a las estrategias de protección de cajeros automáticos convencionales.

En este enfoque se limita el acceso y cualquier tipo de actuación a cualquier persona no autorizada, lo que minimiza el riesgo de acceso no autorizado a cualquier punto de los procesos o de los sistemas.

Nunca confíes en el sistema de distribución de SW: Las actualizaciones frecuentes del sistema, necesarias para prevenir ataques de día cero, dependen del sistema de distribución de software, que históricamente ha sido una vulnerabilidad destacada en las infecciones de malware de cajeros automáticos a nivel de red. Además, la disponibilidad requerida de los cajeros automáticos no siempre permite que se actualicen de manera continua con las últimas políticas, parches críticos y actualizaciones del sistema operativo.

> *"Mientras que los métodos tradicionales se basan en defensas perimetrales y suposiciones de confianza, Zero-Trust adopta una postura fundamentalmente escéptica, asumiendo que cada aspecto del entorno del cajero automático podría verse potencialmente comprometido".*
>
> **Néstor Santolaya Bea**
> Cybersecurity Product expert de Auriga Iberia

Nunca confíes en nadie con accesso fisico al ATM: Zero Trust extiende la protección de hardware más allá de las medidas tradicionales al exigir una certificación rigurosa de todos los componentes de hardware del cajero automático, lo que garantiza que sólo los dispositivos que cumplen con estrictos criterios de seguridad estén autorizados para operar, independientemente de los puertos físicos a los que se conecten.

Protege el ATM como un dispositivo industrial: En cuanto al software, Zero Trust se aborda transformando el sistema operativo del cajero automático de un entorno IT (*information technology*, por sus siglas en inglés) de propósito general a un sistema OT (*operational technology*) de tecnología operativa específico. Este cambio estratégico reduce significativamente la superficie de ataque al limitar estrictamente las operaciones de software solo a aquellas esenciales para la funcionalidad del cajero automático, aislando de manera efectiva los procesos críticos. Así no solo se

protege la integridad del sistema de archivos, asegurando un control estricto sobre los procesos que pueden acceder y modificar archivos, sino que también se favorece la implementación de una rigurosa lista blanca de aplicaciones.

Desconfía de todo aquello que no sirva a la operación del ATM: En el modelo Zero Trust, el énfasis no está en mantener una base de datos exhaustiva de *hashes* de malware, como suelen hacer los enfoques tradicionales, sino que se centra en controles de acceso sólidos para detectar y mitigar amenazas en tiempo real. Esta postura proactiva no solo proporciona una protección eficaz contra malware nuevo y desconocido, sino que también protege contra el uso indebido de herramientas legítimas innecesarias para las operaciones de cajeros automáticos que suelen explotarse en ataques relacionados con los cajeros automáticos.

5 Cómo puede ayudar Auriga

Las instituciones financieras se enfrentan a una gran variedad de desafíos para hacer que los cajeros automáticos —como dispositivos críticos que son— estén disponibles las 24 horas del día y garantizar la máxima seguridad. Para ello, necesitan elaborar un programa de ciberseguridad que comprenda el contexto comercial, la infraestructura técnica que respalda las funciones críticas y las amenazas de seguridad cibernética relacionadas.

Lookwise Device Manager: la solución a medida para los ATMs

LDM es la solución centralizada y modular de Auriga, específicamente diseñada para la seguridad de la red de cajeros automáticos.

Esta solución proporciona un **conjunto integral de funciones** para garantizar la protección y monitorización de sus dispositivos críticos. Agrega una capa de control adicional que permite a los usuarios ejecutar acciones remotas personalizadas para investigar o reaccionar ante posibles incidentes. Además, esta gestión remota también permite **proteger y corregir cualquier desviación que se detecte en el ATM** respecto a la imagen de software predeterminada en un entorno de laboratorio previamente.

Al implementar una estrategia efectiva de ciberseguridad de tecnología operacional, es posible proteger los dispositivos críticos sin afectar las operaciones y cumplir con las regulaciones al mismo tiempo.

El modelo de seguridad, de este modo, permite:

- Proteger la imagen de software del dispositivo, monitorizando y corrigiendo sus desviaciones y asegurando la reducción de vectores de ataque al haber convertido el sistema operativo en un sistema de propósito específico de tipo tecnología operativa (OT). Además, el 100% de los discos duros encriptados ayuda a preservar la integridad del software.

- Integrarse de forma fluida con las labores de mantenimiento del ATM, permitiendo supervisar y aprobar las modificaciones realizadas tanto de software como de hardware, de acuerdo al principio de Zero Trust aplicado al equipo de mantenimiento.

- Asegurar las labores de distribución y actualización de software, certificando no solo el sistema de distribución, sino también cada paquete distribuido, de acuerdo al concepto Zero Trust aplicado al sistema de distribución.

- Centralizar de forma segura las labores cotidianas del cajero, ahorrando costes y reduciendo las ventanas de vulnerabilidad al mínimo al no tener que relajar la protección para realizarlas, ya que se puede monitorizar el estado del mismo y tener capacidad de respuesta en tiempo real ante cualquier ataque.

LDM centraliza la seguridad de la red de dispositivos garantizando así un control eficiente. Además, al concentrar las operaciones de seguridad en una sola plataforma, se logra un impacto mínimo en el rendimiento de los dispositivos. De esta manera se mantiene un control centralizado sobre los cambios de software y hardware con una visibilidad y gestión integradas del estado de la red y un aumento de la disponibilidad general.

Mediante la implementación de LDM la banca puede conseguir una optimización del 98,4% en el tiempo activo de toda su red de ATMs.

lookwise
DEVICE MANAGER

AURIGA
the banking e-volution

Auriga Iberia S.L.
Calle Villalar, 7 Planta 00, Puerta Iz
28001 Madrid - España
madrid@aurigaspa.com

Auriga Latin America, S.de R.L.de C.V.
Córdoba 83 Colonia Roma, 06700,
Ciudad de México, México
mexicocity@aurigaspa.com