



Rafael Navajo

Director Desarrollo de Negocio

GMV Secure e-Solutions

Combatir el fraude en los cajeros automáticos

P

ODER disponer de nuestro dinero las 24 horas del día desde cualquier parte del mundo es una comodidad con la que podemos contar hoy gracias a la función de los cajeros automáticos o ATMs (por sus iniciales en inglés, Automated Teller Machine). Hace más de cuatro décadas, sin embargo, esa posibilidad no existía en el mundo financiero y la gente sólo podía disponer de su dinero en los bancos en su horario de apertura. En 1967, en la localidad de Enfield al norte de Londres, se inauguró el primer cajero automático. Inicialmente los directivos de los bancos temieron que estos terminales automáticos tuviesen un impacto negativo en la relación con el cliente, pero pronto se dieron cuenta de las ventajas de la automatización.

El fenómeno de los cajeros automáticos ha ido creciendo de forma imparable desde que surgió, hasta alcanzar la cifra de más de 2 millones de unidades en el mundo, con grandes ventajas tanto para el consumidor como para la entidad bancaria, aunque desde sus inicios, su seguridad, ha sido un problema de difícil solución.

Debido a la valiosa información que estos dispositivos manejan y a la propia gestión y almacenamiento de efectivo, no hay duda que un cajero automático es un elemento muy atractivo para los criminales. Actualmente nos encontramos con un incremento en los ataques a las redes de cajeros automáticos de manera organizada y altamente sofisticada, convirtiéndose en un gran problema, provocando importantes pérdidas de dinero tanto a las entidades como a los clientes. Según

datos aportados por EAST (European ATM Security Team), los bancos de 22 países europeos perdieron en conjunto 485 millones de euros en sólo un año debido al fraude en cajeros.

Los ataques básicos a un cajero se pueden clasificar en dos tipos: ataques a la infraestructura TI de los cajeros (y de las redes que emplean para procesar transacciones) y ataques físicos en cajeros automáticos. Hoy en día, el fraude en los cajeros tiende por un lado hacia técnicas que persiguen el robo de los datos de las tarjetas de crédito, con el fin de suplantar la identidad de la persona, y por otro lado hacia el ataque a las infraestructuras de las sucursales bancarias, para hacerse con el control remoto del cajero.

El sistema de fraude más común es conocido como "skimming", y sucede cuando los datos de la banda magnética de la tarjeta se capturan en el cajero automático, a través de un lector de tarjetas modificado conocido como un dispositivo de duplicado. La información capturada es utilizada para falsificar tarjetas para su posterior uso fraudulento.

Este punto débil se está tratando de solventar con la introducción de tarjetas inteligentes EMV (también conocido como tarjetas con chip). La implantación de EMV reduce el fraude al disminuir las posibilidades de obtener datos de la banda y el 90% de los cajeros automáticos europeos son ahora compatibles con EMV.

De esta forma, el fraude en cajeros parece que tiende hacia el ataque de las infraestructuras

tecnológicas. Los criminales se están dando cuenta que es más rentable explotar las vulnerabilidades de la infraestructura TI del cajero, ya sea infectando al ATM con algún tipo de software malicioso, pudiendo tomar el control remoto del cajero, o incluso obtener dinero en efectivo directamente del mismo o bien por ejemplo aprovechando alguna vulnerabilidad del software. La detección de este tipo de fraude es mucho más compleja, dado que al no existir manipulación física del ATM en el momento de efectuar el fraude, la entidad bancaria, si no dispone de las herramientas necesarias, puede tardar mucho tiempo en identificar la causa del problema, siendo más difícil la identificación del criminal.

Los cajeros actuales son bastante vulnerables, ya que muchos de ellos emplean sistemas operativos como Microsoft Windows (más del 75%) para su funcionamiento común, (más del 85% de los incidentes de seguridad se producen en sistemas Windows), y utilizan redes IP como mecanismo de comunicación, lo que conlleva un aumento de riesgos de seguridad asociados a las vulnerabilidades existentes en este tipo de sistemas abiertos, siendo susceptibles de quedar infectados con software malicioso.

Para mitigar estos riesgos de una manera sencilla y eficaz, ya existen en el mercado productos de seguridad especialmente diseñados para sistemas de autoservicio, que permiten administrar de forma centralizada cuáles son las aplicaciones que se ejecutan en el sistema, a qué recursos locales o remotos acceden, con qué otros sistemas se comunican y

qué dispositivos pueden acceder. Mediante este férreo control, aseguran en el cajero un entorno de alta seguridad que evita que se puedan explotar vulnerabilidades, infectar los ATMs con por virus, troyanos, gusanos y otros “malwares” especialmente diseñados para atacar la infraestructura de autoservicio financiero, así como la

introducción y ejecución de software malicioso con acceso a recursos sensibles del cajero.

Cada uno de los cajeros en los que se instalan estos dispositivos, disponen de una lista de control de acceso (ACL, Access Control List) que define exhaustivamente los procesos, recursos del sistema (archivos y librerías), comunicaciones permitidas y dispositivos con acceso al ATM. Cualquier otro elemento que no aparezca en esta lista queda automáticamente bloqueado. El nivel de detalle de estas listas de control permite definir exactamente qué puede y qué no puede hacer el cajero. También dispone de un servidor central desde el que se gestiona y monitoriza la red de cajeros. La comunicación entre los cajeros y el servidor es cifrada extremo a extremo y permite realizar la gestión remota del entorno de seguridad del cajero, así como recibir en tiempo real cualquier tipo de evento de seguridad detectado en un cajero.

Afortunadamente, estos productos crean en el cajero automático un entorno de ejecución y de comunicaciones seguro, cumpliendo los más altos niveles de calidad y fiabilidad con un mínimo consumo de recursos. También cabe destacar que puede ser gestionado y monitorizado de forma centralizada. Dichos productos garantizan la seguridad integral, centralizan la información y avisan no sólo de las operaciones efectuadas sino también de los intentos de acceso no autorizados. Ahora sólo queda esperar que cada vez más entidades lo instalen en sus ATMs, ya que su propia seguridad está en juego. ●

“
**Para mitigar estos
 riesgos de una manera
 sencilla y eficaz, existen
 en el mercado productos
 de seguridad
 especialmente diseñados
 para sistemas de
 autoservicio**
 ”