FiXS

La nueva amenaza de ciberseguridad para cajeros automáticos

LOS ATAQUES DE *JACKPOTTING*, CIBERAMENAZA QUE CONSISTE EN ACCEDER FÍSICAMENTE AL CAJERO PARA ROBAR EL EFECTIVO EN SU INTERIOR, LLEVAN CAUSANDO GRANDES PÉRDIDAS ECONÓMICAS A LAS ORGANIZACIONES BANCARIAS DESDE HACE AÑOS. ESTE 2023 PARECE QUE LOS CIBERDELINCUENTES VUELVEN CON FUERZAS RENOVADAS USANDO **UNA NUEVA VARIANTE DE MALWARE LLAMADA FIXS**, QUE YA ESTÁ CAUSANDO ESTRAGOS EN LATINOAMÉRICA, ESPECIALMENTE EN PAÍSES COMO MÉXICO, SEGÚN UN INFORME DE LA EMPRESA DE CIBERSEGURIDAD METABASEQ.

FiXS: Nuevo malware, viejas técnicas

FiXS es una variante de malware ATM nueva, descubierta a finales de febrero de 2023, pero las técnicas y tácticas que utiliza no son diferentes de las de otras familias de malware ya conocidas como **Ploutus, Tyupkin, Alice, Ripper o Cobalt**.

Como la mayoría de ellas, FiXS obtiene acceso ilegítimo al middleware XFS (servicios financieros extendidos) que controla los dispositivos de hardware de los ATM y de este modo **envía órdenes directamente al dispensador del cajero** para extraer efectivo sin necesidad de pasar por el proceso de autorización de la transacción.

El hecho de atacar la capa XFS hace que FiXS sea una amenaza para múltiples proveedores y modelos de cajeros automáticos.

Cómo es el malware FiXS

FiXS se disfraza con el nombre de un ejecutable común del sistema: **conhost.exe**, que se encarga de extraer el malware (FiXS.exe) y copiarlo en el sistema de archivos del cajero automático en un directorio temporal.

Desde ahí, FiXS.exe hace uso de la biblioteca MSXFS.dll para interactuar con la API de los servicios financieros extendidos (XFS), desde donde puede enviar órdenes a los dispositivos de hardware, como el dispensador.

La interacción con FiXS **se realiza a través de un teclado conectado**, que permite al atacante iniciar la interfaz gráfica de usuario (GUI), ver la información de las unidades de efectivo y enviar comandos de dispensación.

Modus Operandi del ataque

De la infección a la ejecución

El ciclo de vida del ataque incluye varias fases, desde la preparación hasta la infección, la persistencia y la ejecución final para lograr el botín. La accesibilidad física al cajero automático es un factor clave para el ataque.

Este tipo de ciberataques suele empezar por una etapa de **preparación**, en que los ciberdelincuentes roban un disco duro de un cajero automático de producción, que contiene el stack de software completo utilizado por la institución financiera, lo analizan y lo someten a ingeniería inversa para preparar un ataque dirigido.

Después proceden a la **infección** mediante el acceso físico al dispositivo a través de teclados externos y memorias USB para introducir el malware, algo que se puede hacer online, accediendo al sistema operativo y copiando el malware, o bien offline, arrancando desde un USB externo para luego montar el disco duro del cajero automático y copiar el malware.

Es importante que el malware sea persistente para que se ejecute automáticamente al iniciarse el cajero automático, lo que logran reemplazando los ejecutables legítimos del sistema o configurando la ejecución automática en el momento del inicio.

De este modo, el malware se ejecutará en segundo plano esperando un código de activación y con pleno acceso al middleware XFS para enviar comandos al dispensador.

Aquí, ya estarían listos para pasar a la **ejecución**, es decir, la extracción ilegítima del efectivo, que puede ser realizada por otros actores, las llamadas “mulas de dinero”, que acceden físicamente al cajero y pueden ingresar un código de activación que despierta el malware activando una interfaz gráfica de usuario (GUI). Otros métodos de activación pueden ser el propio pinpad, el uso de tarjetas falsificadas o incluso conectar un dispositivo móvil y recibir un SMS.

Finalmente, una vez que se completa el "reintegro", algunas familias de malware brindan un mecanismo de **limpieza/desinstalación** para eliminar cualquier rastro del ataque.

Windows XP / 7 / 10

Todos son vulnerables

Algunas fuentes afirman que los cajeros automáticos que ejecutan sistemas operativos obsoletos como Windows XP o Windows 7 son más vulnerables porque el sistema operativo ya no es compatible y no hay nuevos parches de seguridad. Sin embargo, si bien migrar a Windows 10 y mantener los parches actualizados siempre es una buena práctica, lo cierto es que **los cajeros automáticos con Windows 10 son tan vulnerables como los que ejecutan Windows 7 o XP**.
La razón es que el malware para cajeros automáticos está muy dirigido y no explota las vulnerabilidades del sistema operativo, sino **las vulnerabilidades de diseño del stack de software** de cajeros automáticos, como la falta de autenticación en la capa XFS.

ZERO TRUST

La aproximación correcta a la seguridad del ATM

Toda organización que opera una red de cajeros automáticos es un objetivo potencial para los ataques de Jackpotting y, por lo tanto, la aplicación de contramedidas de ciberseguridad robustas y eficientes se convierte en una necesidad básica.

Disponibilidad vs Seguridad

Los cajeros automáticos son dispositivos críticos que prestan servicios esenciales para los ciudadanos. Su principal objetivo es **garantizar la disponibilidad y fiabilidad del servicio**, de forma continua y sin interrupciones.
Sin embargo, desde el punto de vista de la seguridad, la falta de políticas proactivas de actualización, sumada a la accesibilidad física de estos dispositivos, crea un entorno vulnerable que hace que los cajeros sean muy difíciles de proteger con las tecnologías de seguridad tradicionales.

Modelo de protección “Zero Trust”

Uno de los términos más de moda en las comunidades especializadas en ciberseguridad es "*Zero Trust*", que se basa en la suposición de que su infraestructura se verá comprometida y en el concepto de "**nunca confiar, siempre verificar**".

Cuando hablamos de dispositivos críticos, como cajeros automáticos o dispositivos de autoservicio asistido (ASST), el modelo *Zero Trust* debe estar en el centro de cualquier estrategia de ciberseguridad. **Consiste en realizar una serie de suposiciones sospechosas sobre la vulnerabilidad de la infraestructura** que gestiona los dispositivos como, por ejemplo, que puede ser manipulado, que el sistema de distribución de software puede ser utilizado para desplegar malware, que el técnico de mantenimiento o el usuario final mismo pueden ser atacantes o que nuestro disco duro puede ser robado para realizar actividades de ingeniería inversa.

El valor de la estrategia *Zero Trust* radica en su capacidad para permitir que las instituciones financieras aseguren la banca de autoservicio digital sin confiar en la supuesta seguridad del software convencional. Esta desconfianza es importante porque los atacantes cibernéticos secuestrarán herramientas y software legítimos para lanzar un ataque.

Desde el punto de vista de Auriga, los puntos clave para diseñar un sólido modelo de protección de cajeros automáticos serían:

- **Reducción drástica de la superficie de ataque**: para que el acceso al software, hardware y comunicaciones se verifique continuamente y solo se conceda al conjunto mínimo de recursos legítimos y estrictamente necesarios para el correcto funcionamiento del dispositivo.

- **Control estricto de cambios en el cajero automático**: para bloquear cualquier intento de cambio de software o hardware que no haya sido autorizado explícitamente.

LOOKWISE DEVICE MANAGER

La solución adecuada

Lookwise Device Manager (LDM) es la solución de Auriga para la ciberseguridad de los cajeros automáticos, basada en el enfoque *Zero Trust*. Ha sido diseñada en base al conocimiento de la infraestructura de cajeros automáticos y las tácticas y técnicas del atacante, y proporciona el modelo de protección en capas más completo para proteger un cajero automático en todas las etapas del ciclo de vida del ataque.

Primero realiza un **cifrado de disco duro** (para evitar la "ingeniería inversa" en caso de robo del mismo), de forma que el atacante no tenga acceso a las diferentes capas del stack de software. **En el caso de FiXS, esto impediría el acceso a la biblioteca MSXFS.dll**. Ese cifrado también evita manipulación del sistema de archivos "fuera de línea", por lo que, en el caso de FiXS, impediría los intentos de copiar el malware en el sistema de archivos del cajero automático.

La solución también garantiza la **integridad del sistema de archivos** (para evitar la manipulación del sistema de archivos "en línea") -en el caso de FiXS, esto bloquearía los intentos de copiar el malware conhost.exe y FiXS.exe en el sistema de archivos ATM-, y la **protección de hardware (para evitar la conexión de dispositivos HW "no fiables")**, que evitará que un atacante conecte dispositivos externos para interactuar con el sistema operativo. En el caso de FiXS esto bloquearía la conexión del teclado que se utiliza para interactuar con el Sistema Operativo.

LDM También garantiza la **integridad del registro de Windows para evitar la "persistencia" del malware**, ya que los ciberdelincuentes suelen modificar las claves del registro de Windows para permitir que el malware se inicie en el momento del arranque, como sucede en el caso de FiXS.

Por último, su **lista blanca de software** evitaría la ejecución de software "no fiable", ya que el sistema verifica cualquier ejecución (path&hash) y el acceso a bibliotecas críticas lo que, en el caso de FiXS, consistiría en bloquear la ejecución de conhost.exe o FiXS.exe y también los intentos de vincular dinámicamente la biblioteca MSXFS.dll del sistema.

Asímismo, es importante **su protección Firewall (para evitar la comunicación con paneles externos de "comando y control")**. Muchas familias de malware utilizan funciones de devolución de llamada para comunicarse con paneles externos de "comando y control" para recibir órdenes. La protección de firewall de LDM evitará que un proceso malicioso se comunique con un sistema externo no autorizado. En el caso de FiXS no hay evidencia de la existencia de un panel de "Comando y Control".

LDM ha sido diseñado para integrarse perfectamente con los procedimientos operativos clave de los cajeros automáticos y para garantizar que cualquier cambio realizado en el cajero automático (software y hardware) esté totalmente controlado y protegido.

THE # NEXTGENBANK

AURIGA
the banking e-volution

Auriga Iberia, S.L.
Paseo Santxiki, 2 Bajo A1 31192
Aranguren, Navarra, España
pamplona@aurigaspa.com

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

www.aurigaspa.com