**NOTA DE PRENSA**

# El malware FiXS ataca a cajeros automáticos en Latinoamérica, ¿cómo se puede prevenir?

Un nuevo malware bautizado FiXS fue reportado a fines de febrero y está atacando a los cajeros automáticos de la región latinoamericana, mayormente en México, con el objetivo de vaciar cajeros por completo. En este marco, Auriga, proveedor internacional de soluciones tecnológicas para la banca omnicanal, aconseja implementar sistemas de seguridad que partan del enfoque de confianza cero para los cajeros automáticos ante la nueva amenaza.

Si bien FiXS es una variante de malware ATM nueva, según reportó la empresa Metabase Q, 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.

FiXS está diseñado para ser operado por el atacante y, a su vez, puede controlar los dispositivos de un cajero automático desde un teclado conectado de manera externa.
Se disfraza con el nombre de un ejecutable común del sistema, que se encarga de extraer el malware y copiarlo en el sistema de archivos del cajero automático en un directorio temporal.
Desde ahí, FiXS 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.

*"Dado el reciente aumento de brechas y ataques que ha experimentado este sector, en Auriga queremos subrayar la importancia de implementar sistemas de seguridad dedicados y centralizados",* afirma Juan Ramón Aramendía, Head of Cybersecurity Product Engineering de Auriga.

**Las 4 etapas del ataque de FiXS**
En primer lugar, 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, incluyendo el desarrollo del malware (como es el caso de FiXS).
Una vez completada la fase de I+D, proceden a la **infección** de cajeros cargados con efectivo, mediante el acceso físico al dispositivo a través de teclados externos y memorias USB para introducir 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 la extracción ilegítima del efectivo, que puede ser realizada por otros actores 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 la conexión de un dispositivo móvil y el recibimiento de 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.

*"Todos los cajeros automáticos son vulnerables"* - subraya Aramendía -*"Pese a que lo recomendable es una actualización constante de los sistemas operativos, en este caso, 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.

**¿Cómo pueden los bancos hacer frente a este tipo de malware?**

Auriga ha desarrollado la plataforma **Lookwise Device Manager (LDM)** para garantizar un alto nivel de seguridad en los sistemas y en la información del sistema financiero, basada en el enfoque Zero Trust. Se trata de una plataforma modular que puede proteger y monitorear los dispositivos críticos y, al mismo tiempo, cuenta con una capa de control adicional para facilitar la ejecución de acciones personalizadas y remotas, y así reaccionar ante posibles incidentes.

De esta manera, LDM realiza un cifrado de disco duro 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, evitaría la manipulación del sistema de archivos fuera de línea y, por tanto, bloquearía los intentos de copiar el malware en el sistema de archivos del cajero automático.

Esta solución también garantiza la integridad del sistema de archivos, bloqueando los intentos de copiar el malware en línea en el sistema de archivos del ATM, y la protección de hardware para evitar la conexión de

dispositivos no fiables, impidiendo la conexión del teclado utilizado para interactuar con el sistema operativo. A su vez, LDM también protege la integridad del registro de Windows para evitar la persistencia del malware.

En el caso de los dispositivos críticos, como los cajeros automáticos, adoptar el modelo Zero Trust es menester para cualquier estrategia de ciberseguridad, ya que implica realizar una serie de suposiciones sospechosas sobre la vulnerabilidad de la infraestructura que gestiona los dispositivos, ante la posibilidad de que, por ejemplo, sea manipulado, de que el sistema de distribución de software sea utilizado para desplegar malware, de que el técnico de mantenimiento o el usuario final mismo puedan ser atacantes o de que el disco duro pueda ser robado para realizar actividades de ingeniería inversa.

En suma, las soluciones que mejor podrán hacer frente a amenazas como FiXS son aquellas que estén formuladas desde el enfoque Zero Trust. Esta perspectiva es de los temas más actuales en ciberseguridad e implica tanto la presunción de que la infraestructura se verá comprometida, como la aplicación concreta del concepto de “nunca confiar, siempre verificar”.

**Acerca de Auriga**

Auriga es un proveedor líder de soluciones de software y tecnología para la banca y el sector de pagos, y especialista en soluciones innovadoras omnicanal para la banca y otras instituciones financieras. Sus soluciones, desplegadas en más del 74% de los cajeros automáticos de Italia, se basan en una moderna arquitectura tecnológica y mejoran el time-to-market para nuevos servicios al mismo tiempo que reducen los costes, protegiendo los dispositivos críticos de ciberataques y logrando una ventaja competitiva a largo plazo. Auriga es una compañía global, con presencia directa en Italia, Reino Unido, España, Bélgica y México, y está ampliando sus operaciones en Europa occidental y oriental, Latinoamérica y Asia-Pacífico.

Más información sobre Auriga: https://www.aurigaspa.com/es/

**Contacto para medios en LatAm**
EntercommLA/Audacia
Yanira Franco - M. 55 1812 8155
yanira@audacia.com.mx
Claudia Medellín - M 55 1938 9631
claudia@audacia.com.mx

**Para más información en España**:
Jesús Martínez jesus.martinez@alephcom.es
Esther Gago esther.gago@alephcom.es
Aleph Comunicación
Tel.: 91 386 69 99

**Contacto Auriga:**
Antonella Comes
Chief Marketing Officer
antonella.comes@aurigaspa.com