

La Guía de Malware de Auriga analiza las 50 variantes que más han afectado a la banca en las últimas décadas.

La compañía de software para la banca ha recopilado las distintas variedades de código malicioso en la Guía de Malware para la Banca, donde define y explica cada una de ellas.

Madrid, 16 de junio de 2025

En un momento en que el fraude, los ciber robos y las alertas por ataques digitales masivos están a la orden del día, en el sector bancario los cajeros automáticos son un elemento especialmente vulnerable.

El malware o software malicioso es una de las principales amenazas para estos dispositivos y, por ende, para toda la ciberseguridad de las entidades, ya que a través de él no solo se pueden robar grandes cantidades de dinero, sino también datos de los clientes e información valiosa de sus procesos y funcionamiento.

Se considera malware a cualquier código diseñado para eludir medidas de seguridad, modificar procesos o replicarse de forma autónoma con distintos propósitos.

Para los responsables de tecnología, las agencias de cumplimiento de la ley y las instituciones financieras es importante conocer a fondo esta amenaza como primer paso para fortalecer sus defensas y mitigar los riesgos. Pensando en ellos, la Unidad de Negocio de Ciberseguridad de [Auriga](#), compañía de software para el sector de pagos y banca omnicanal y experta en ciberseguridad en dispositivos específicos, ha elaborado la primera [Guía de Malware para la Banca](#), una referencia completa de 50 variantes de malware que pueden afectar a cajeros automáticos con sus características, métodos de infección, procedimientos de activación, contexto histórico, nombres y eventos notables de cada una de ellas.

Estas son, según la Guía, las más destacadas:

- ▶ **El primer malware específico para cajeros:** Skimer, descubierto en Rusia en 2009.
- ▶ **El malware de mayor impacto en el mundo:** Se estima que los ataques coordinados con Carbanak, Anunak y Cobalt acumulan más de 1000 millones de dólares en pérdidas para las entidades financieras, siendo el malware que mayor impacto ha tenido en las finanzas globales en los últimos 15 años.
- ▶ **El malware que ha infectado más cajeros:** Ploutus, comprometiendo más de 75.000 cajeros en todo el mundo.
- ▶ **La familia de malware más recientemente detectada:** Hasta que se demuestre la existencia real de AU ATM Malware (mayo 2024), FixS se considera la última familia de malware específica de ATMs detectada, en este caso en México, en febrero de 2023.
- ▶ **La variante más reciente detectada:** FastCash, con una nueva variante descubierta en octubre de 2024.
- ▶ **El malware con más variantes conocidas:** Ploutus, con múltiples versiones.
- ▶ **El malware más peligroso para el ATM:** Por su impacto inmediato y directo, y debido a su capacidad para dispensar grandes sumas de dinero, Tyupkin puede considerarse la familia de malware más peligrosa para los ataques físicos.



- ▶ **El malware más difícil de detectar:**
Por su nivel de infiltración y porque es necesario un sistema antifraude muy sofisticado para su detección, Metel puede considerarse el que puede operar durante más tiempo sin que se detecte su presencia.
- ▶ **El malware más fácil de usar:**
Por su sencilla interfaz y porque automatiza muchas de las tareas involucradas en el ataque, Cutlet Maker es probablemente el más sencillo de usar por los criminales.

“ A día de hoy, la mejor protección de un cajero automático frente a este tipo de software se basa en reducir la superficie de ataque a la mínima expresión mediante un enfoque de confianza cero. Dada la evolución de la programación, las variantes pueden ser numerosas y, muchas veces, difíciles de detectar, por eso vigilar, entender cómo operan los malhechores y estar preparados para atajar este problema es fundamental. Esperamos que esta guía resulte útil para sentar las bases de la ciberseguridad en evolución”

Néstor Santolaya Bea, cybersecurity product expert de Auriga y autor de la Guía de Malware para la Banca

Acerca de Auriga

Auriga es un proveedor líder de software y soluciones tecnológicas para la banca y el sector de pagos, y especialista en soluciones omnicanal innovadoras 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 mientras al mismo tiempo que reducen los costes y protegen los dispositivos críticos de ciberataques, logrando una ventaja competitiva a largo plazo. Auriga es una compañía global, con presencia en Italia, Reino Unido, España, Bélgica, Polonia y México, y está expandiéndose en Europa occidental y oriental, Latinoamérica y Asia-Pacífico.

Más información sobre Auriga:

<https://www.aurigaspa.com/es/>

Para más información:

Jesús Martínez - jesus.martinez@alephcom.es
Esther Gago - esther.gago@alephcom.es
Aleph Comunicación - Tel.: 91 386 69 99

Alison Correa
Communica
acorrea@communika.com.mx

Contacto Auriga:

Antonella Comes
Chief Marketing Officer
antonella.comes@aurigaspa.com