Registra México 11,695 ataques de nuevo malware bancario

Por Franco Becerra B. y G.

México registró 11 mil 695 ataques relacionados con un nuevo malware bancario denominado 'JanelaRAT'

En 2025, México registró 11 mil 695 ataques relacionados con un nuevo malware bancario denominado "JanelaRAT", una versión que permite secuestrar sesiones bancarias en tiempo real, de acuerdo con la telemetría de la compañía de ciberseguridad Kaspersky.

JanelaRAT es un troyano de acceso remoto y una variante fuertemente modificada del antiguo BX RAT de 2014, que apunta principalmente a usuarios en América Latina, especialmente en sectores bancarios, fintech y de criptomonedas.

La compañía reportó que sus investigadores detectaron y analizaron una nueva versión de JanelaRAT donde en línea con intrusiones y campañas previas, los principales objetivos de los actores detrás de esta amenaza son usuarios bancarios en América Latina, con especial enfoque en clientes de instituciones financieras en Brasil y México.

Con esta nueva versión del malware, explicó Kaspersky, los atacantes manipulan al usuario para que interactúe con una pantalla superpuesta personalizada sobre la interfaz real de banca en línea, lo que les permite iniciar el secuestro de la sesión bancaria.

El malware utiliza una cadena de infección de múltiples etapas que comienza con correos de phishing que contienen scripts maliciosos en VBS dentro de archivos comprimidos, los cuales son abiertos por los usuarios.

Según la telemetría de Kaspersky, en 2025 también se registraron 14 mil 739 ataques en Brasil.

"JanelaRAT sigue siendo una amenaza activa y en evolución, con intrusiones que mantienen características consistentes pese a las modificaciones continuas. Hemos seguido su evolución durante algún tiempo, observando variaciones tanto en el malware como en su cadena de infección, incluyendo variantes específicas por país.

"Esta nueva versión representa un avance significativo en las capacidades de los atacantes, al combinar múltiples canales de comunicación, monitoreo completo de la víctima, superposiciones interactivas, inyección de entradas y funciones robustas de control remoto. Además, está diseñado para minimizar su visibilidad y adaptar su comportamiento ante la detección de software antifraude", comentó María Isabel Manjarrez, Investigadora de Seguridad para América Latina en el Equipo Global de Investigación y Análisis de Kaspersky.

La nueva versión de JanelaRAT implementa una táctica interactiva diseñada para capturar credenciales bancarias y evadir la autenticación multifactor. Cuando detecta una ventana bancaria, el malware despliega una pantalla completa con una imagen enviada por los atacantes que imita interfaces legítimas de bancos o del sistema.

Luego, bloquea la interacción de la víctima mediante cuadros de diálogo controlados por los atacantes. Las acciones dentro de estos cuadros corresponden a operaciones específicas, como la captura de contraseñas o de tokens de autenticación (MFA), entre otras.

Entre los engaños utilizados se incluyen pantallas falsas de carga, simulaciones de actualizaciones de Windows en pantalla completa y otros elementos similares, relató Kaspersky.

Para mantenerse protegido frente a este tipo de amenazas, Kaspersky recomienda ser cauteloso al abrir o descargar archivos recibidos por mensajería o correo electrónico, ya que pueden contener malware.

También, prestar atención a notificaciones por correo electrónico, ya que los ciberdelincuentes suelen suplantar tiendas en línea o bancos para inducir a hacer clic en enlaces maliciosos.