Los bancos y las instituciones financieras en países de América Latina como Brasil y México han seguido siendo objetivo de una familia de malware conocida como JanelaRAT.

JanelaRAT, una versión modificada de BX RAT, está diseñado para robar datos financieros y de criptomonedas vinculados a entidades específicas, además de rastrear el uso del mouse, registrar pulsaciones de teclado, capturar pantallas y recolectar metadatos del sistema.

«Una de las diferencias clave entre estos troyanos es que JanelaRAT utiliza un mecanismo personalizado de detección de barras de título para identificar los sitios web deseados en los navegadores de las víctimas y ejecutar acciones maliciosas,» señaló Kaspersky en un informe publicado hoy. *«Los actores de amenaza detrás de las campañas de JanelaRAT actualizan constantemente la cadena de infección y las versiones del malware agregando nuevas funcionalidades.»*

Los datos de telemetría recopilados por la empresa rusa de ciberseguridad indican que se registraron hasta 14,739 ataques en Brasil en 2025 y 11,695 en México. Por ahora, no se sabe cuántos de estos incidentes terminaron en compromisos exitosos.

Detectado por primera vez en estado activo por Zscaler en junio de 2023, JanelaRAT ha utilizado archivos ZIP que contienen un script de Visual Basic (VBScript) para descargar un segundo archivo ZIP, el cual incluye un ejecutable legítimo y una carga útil en formato DLL. La fase final emplea la técnica de carga lateral de DLL para ejecutar el troyano.

En un análisis posterior publicado en julio de 2025, KPMG indicó que el malware se distribuye mediante instaladores MSI falsos que se hacen pasar por software legítimo alojado en plataformas confiables como GitLab. Los ataques relacionados con este malware han tenido como principales objetivos a Chile, Colombia y México.

«Tras su ejecución, el instalador inicia un proceso de infección de múltiples etapas mediante scripts de orquestación escritos en Go, PowerShell y batch,» señaló KPMG en ese momento. *«Estos scripts descomprimen un archivo ZIP que contiene el ejecutable del RAT, una extensión maliciosa del navegador basada en Chromium y componentes adicionales de*

soporte.»

Estos scripts también están diseñados para detectar navegadores basados en Chromium instalados y modificar de forma sigilosa sus parámetros de inicio (como el interruptor de línea de comandos «–load-extension») para instalar la extensión maliciosa. Posteriormente, este complemento recopila información del sistema, cookies, historial de navegación, extensiones instaladas y metadatos de pestañas, además de ejecutar acciones específicas según coincidencias en patrones de URL.

La cadena de ataque más reciente documentada por Kaspersky muestra que se utilizan correos de phishing disfrazados de facturas pendientes para engañar a las víctimas y hacer que descarguen un archivo PDF mediante un enlace, lo que finalmente conduce a la descarga de un archivo ZIP que inicia la cadena de ataque mencionada, incluyendo la carga lateral de DLL para instalar JanelaRAT.

Al menos desde mayo de 2024, las campañas de JanelaRAT han pasado de usar scripts de Visual Basic a instaladores MSI, los cuales actúan como descargadores del malware utilizando la técnica de carga lateral de DLL y establecen persistencia en el sistema creando un acceso directo de Windows (LNK) en la carpeta de inicio que apunta al ejecutable.

Una vez en ejecución, el malware establece comunicación con un servidor de comando y control (C2) mediante un socket TCP para registrar la infección exitosa y monitorear la actividad de la víctima con el fin de interceptar interacciones bancarias sensibles.

El objetivo principal de JanelaRAT es obtener el título de la ventana activa y compararlo con una lista predefinida de instituciones financieras. Si encuentra coincidencias, el malware espera 12 segundos antes de abrir un canal dedicado con el C2 y ejecutar tareas maliciosas recibidas del servidor. Algunos de los comandos que puede ejecutar incluyen:

- Enviar capturas de pantalla al servidor C2
- Recortar regiones específicas de la pantalla y exfiltrar imágenes
- Mostrar imágenes en pantalla completa (por ejemplo, «Configurando actualizaciones

de Windows, por favor espere») e imitar interfaces bancarias mediante superposiciones falsas para robar credenciales
- Registrar pulsaciones de teclado
- Simular acciones del teclado como DOWN, UP y TAB para navegar
- Mover el cursor y simular clics
- Forzar el apagado del sistema
- Ejecutar comandos mediante «cmd.exe» y scripts o comandos de PowerShell
- Manipular el Administrador de tareas de Windows para ocultar su ventana
- Detectar la presencia de sistemas antifraude
- Enviar metadatos del sistema
- Identificar entornos sandbox y herramientas de automatización

«El malware determina si la máquina de la víctima ha estado inactiva durante más de 10 minutos calculando el tiempo transcurrido desde la última interacción del usuario,» explicó Kaspersky. *«Si el periodo de inactividad supera los 10 minutos, el malware notifica al C2 enviando el mensaje correspondiente. Cuando el usuario vuelve a interactuar, también lo reporta al atacante. Esto permite rastrear la presencia y la rutina del usuario para programar posibles operaciones remotas.»*

«Esta variante representa un avance significativo en las capacidades del actor, al combinar múltiples canales de comunicación, monitoreo integral de la víctima, superposiciones interactivas, inyección de entradas y sólidas funciones de control remoto. El malware está específicamente diseñado para minimizar su visibilidad ante el usuario y adaptar su comportamiento cuando detecta software antifraude.»