Un nuevo malware para Android llamado Albiriox ha sido promocionado bajo un modelo de malware-como-servicio (MaaS), ofreciendo un "espectro completo" de funciones para facilitar fraudes directamente en el dispositivo (ODF), manipulación de pantalla e interacción en tiempo real con equipos infectados.

El malware incluye una lista incrustada de más de 400 aplicaciones, entre ellas plataformas bancarias, de tecnología financiera, procesadores de pagos, casas de cambio de criptomonedas, billeteras digitales y servicios de trading.

Los investigadores de Cleafy, Federico Valentini, Alessandro Strino, Gianluca Scotti y Simone Mattia, explicaron que *"el malware utiliza aplicaciones dropper distribuidas mediante señuelos de ingeniería social, combinadas con técnicas de empaquetado para evadir la detección estática y entregar su carga maliciosa"*.

Se cree que Albiriox fue promocionado inicialmente en una fase de reclutamiento limitada a finales de septiembre de 2025, antes de pasar a ofrecerse como MaaS un mes después. Hay evidencia que sugiere que los actores detrás de la amenaza son de habla rusa, basándose en su actividad en foros criminales, patrones lingüísticos e infraestructura utilizada.

A los clientes potenciales se les proporciona acceso a un generador personalizado que, según sus desarrolladores, se integra con un servicio externo de cifrado llamado Golden Crypt para evadir soluciones antivirus y de seguridad móvil. Actualmente se ofrece por una suscripción mensual de 720 dólares.

El objetivo final de los ataques es tomar el control de los dispositivos móviles y ejecutar acciones fraudulentas sin ser detectados. Al menos una campaña inicial se dirigió específicamente a víctimas en Austria mediante señuelos en alemán y mensajes SMS con enlaces acortados que redirigían a páginas falsas de Google Play con aplicaciones como PENNY Angebote & Coupons.

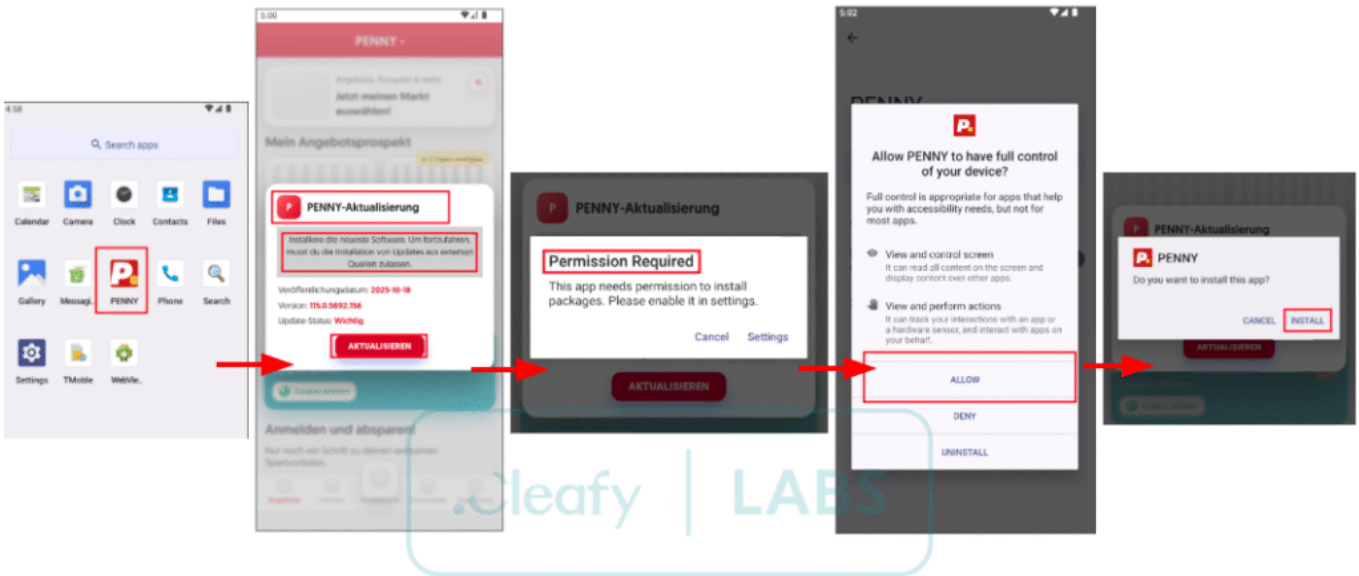
Los usuarios desprevenidos que hacían clic en el botón *"Install"* en la página falsa eran infectados con un APK dropper. Una vez instalado y ejecutado, la aplicación solicitaba

permisos para instalar otras apps haciéndose pasar por una actualización de software, lo que permitía desplegar el malware principal.

Albiriox utiliza una conexión de socket TCP sin cifrado para su comando y control (C2), permitiendo a los atacantes enviar órdenes para manipular el dispositivo de forma remota mediante VNC, extraer información sensible, mostrar pantallas negras o en blanco y ajustar el volumen para mejorar el sigilo operativo.

También instala un módulo de acceso remoto basado en VNC para permitir a los actores interactuar directamente con los teléfonos comprometidos. Una de sus variantes usa los servicios de accesibilidad de Android para mostrar todos los elementos de la interfaz del dispositivo.

Los investigadores explicaron que *"este mecanismo de transmisión basado en accesibilidad está diseñado intencionalmente para evadir las limitaciones impuestas por la protección FLAG_SECURE de Android"*.



Añadieron que *"dado que muchas aplicaciones bancarias y de criptomonedas bloquean la grabación o captura de pantalla cuando esa bandera está activa, aprovechar los servicios de accesibilidad permite al malware obtener una vista completa de la interfaz sin activar las protecciones asociadas con las técnicas directas de captura de pantalla"*.

Al igual que otros troyanos bancarios para Android, Albiriox admite ataques de superposición contra una lista predefinida de aplicaciones objetivo para robar credenciales. Además, puede mostrar pantallas que simulan actualizaciones del sistema o pantallas negras para ocultar actividades maliciosas ejecutadas en segundo plano.

Cleafy también observó un método de distribución alterno que redirige a los usuarios a un sitio falso que se hace pasar por PENNY, donde se les pide ingresar su número telefónico para recibir un enlace de descarga por WhatsApp. La página solo acepta números austriacos. Los números ingresados se envían a un bot de Telegram.

Cleafy señaló que *"Albiriox exhibe todas las características centrales del malware moderno de fraude en el dispositivo (ODF), incluyendo control remoto mediante VNC, automatización basada en accesibilidad, superposiciones dirigidas y recolección dinámica de credenciales"*. Añadieron que *"estas capacidades permiten a los atacantes evitar los mecanismos tradicionales de autenticación y detección de fraude al operar directamente dentro de la sesión legítima de la víctima"*.

La revelación coincide con la aparición de otra herramienta MaaS para Android llamada RadzaRat, que se hace pasar por una app legítima de gestión de archivos, pero que despliega amplias funciones de espionaje y control remoto tras su instalación. El RAT fue anunciado en un foro clandestino el 8 de noviembre de 2025.

La investigadora de Certo, Sophia Taylor, comentó que *"el desarrollador del malware, bajo el alias 'Heron44', ha posicionado la herramienta como una solución de acceso remoto accesible que requiere un conocimiento técnico mínimo para implementarse y utilizarse"*. Añadió que *"la estrategia de distribución refleja una inquietante democratización de las herramientas de ciberdelincuencia"*.

La función principal de RadzaRat es la capacidad de gestionar de forma remota el sistema de archivos, permitiendo a los atacantes navegar directorios, buscar archivos específicos y descargar datos del dispositivo comprometido. También abusa de los servicios de accesibilidad para registrar pulsaciones de teclas y utiliza Telegram para su C2.

Para mantenerse activo, el malware recurre a los permisos RECEIVE_BOOT_COMPLETED y RECEIVE_LOCKED_BOOT_COMPLETED, además de un componente BootReceiver, asegurando su ejecución automática tras reinicios del dispositivo. También solicita el permiso REQUEST_IGNORE_BATTERY_OPTIMIZATIONS para evitar que la optimización de batería limite su actividad en segundo plano.

Certo advirtió que *"su disfraz como un gestor de archivos funcional, combinado con amplias capacidades de vigilancia y exfiltración de datos, lo convierte en una amenaza significativa para usuarios y organizaciones por igual"*.

Los hallazgos surgen mientras páginas falsas de Google Play promocionan una app llamada *"GPT Trade"* (*"com.jxtfkrsl.bjtgsb"*), que distribuye el malware BTMOB y un módulo de persistencia llamado UASecurity Miner. BTMOB, documentado por primera vez por Cyble en febrero de 2025, es conocido por abusar de los servicios de accesibilidad para desbloquear dispositivos, registrar teclas, automatizar el robo de credenciales mediante inyecciones y permitir control remoto.

Las campañas de ingeniería social con contenido para adultos también han impulsado una red sofisticada de distribución de malware Android que entrega un APK malicioso extremadamente ofuscado que solicita permisos sensibles para superposiciones de phishing, captura de pantalla, instalación de más malware y manipulación del sistema de archivos.

Palo Alto Networks Unit 42 explicó que *"emplea una arquitectura resistente y de múltiples etapas con sitios señuelo frontales que usan ofuscación y cifrado de nivel comercial para esconderse y conectarse dinámicamente con una infraestructura backend separada"*. Añadieron que *"los sitios señuelo utilizan mensajes de carga engañosos y una serie de verificaciones, incluido el tiempo de carga de una imagen de prueba, para evadir la detección*

y el análisis”.