Investigadores en ciberseguridad han revelado detalles sobre una nueva plataforma de *spyware* móvil denominada ZeroDayRAT, que se promociona en Telegram como una herramienta para obtener datos sensibles y permitir vigilancia en tiempo real en dispositivos Android e iOS.

> *«El desarrollador gestiona canales específicos para ventas, atención al cliente y actualizaciones periódicas, ofreciendo a los compradores un único punto de acceso a un panel de espionaje completamente funcional»,* afirmó Daniel Kelley, investigador de seguridad en iVerify. *«La plataforma va más allá de la recopilación de datos convencional e incorpora vigilancia en vivo y robo financiero directo.»*

ZeroDayRAT está diseñada para funcionar en versiones de Android 5 a 16 y en iOS hasta la versión 26. Se estima que el malware se distribuye mediante ingeniería social o a través de tiendas de aplicaciones falsas. Los archivos maliciosos se generan con un *builder* que se entrega a los compradores junto con un panel en línea que pueden instalar en su propio servidor.

Una vez que el dispositivo es comprometido, el operador puede visualizar todos los detalles —modelo, ubicación, sistema operativo, estado de la batería, SIM, operador móvil, uso de aplicaciones, notificaciones y vista previa de SMS recientes— desde un panel autogestionado. Estos datos permiten al atacante perfilar a la víctima y conocer con quién se comunica y qué aplicaciones utiliza con mayor frecuencia.

El panel también extrae las coordenadas GPS actuales y las representa en Google Maps, además de almacenar el historial completo de ubicaciones visitadas, convirtiendo efectivamente la herramienta en un sistema de espionaje integral.

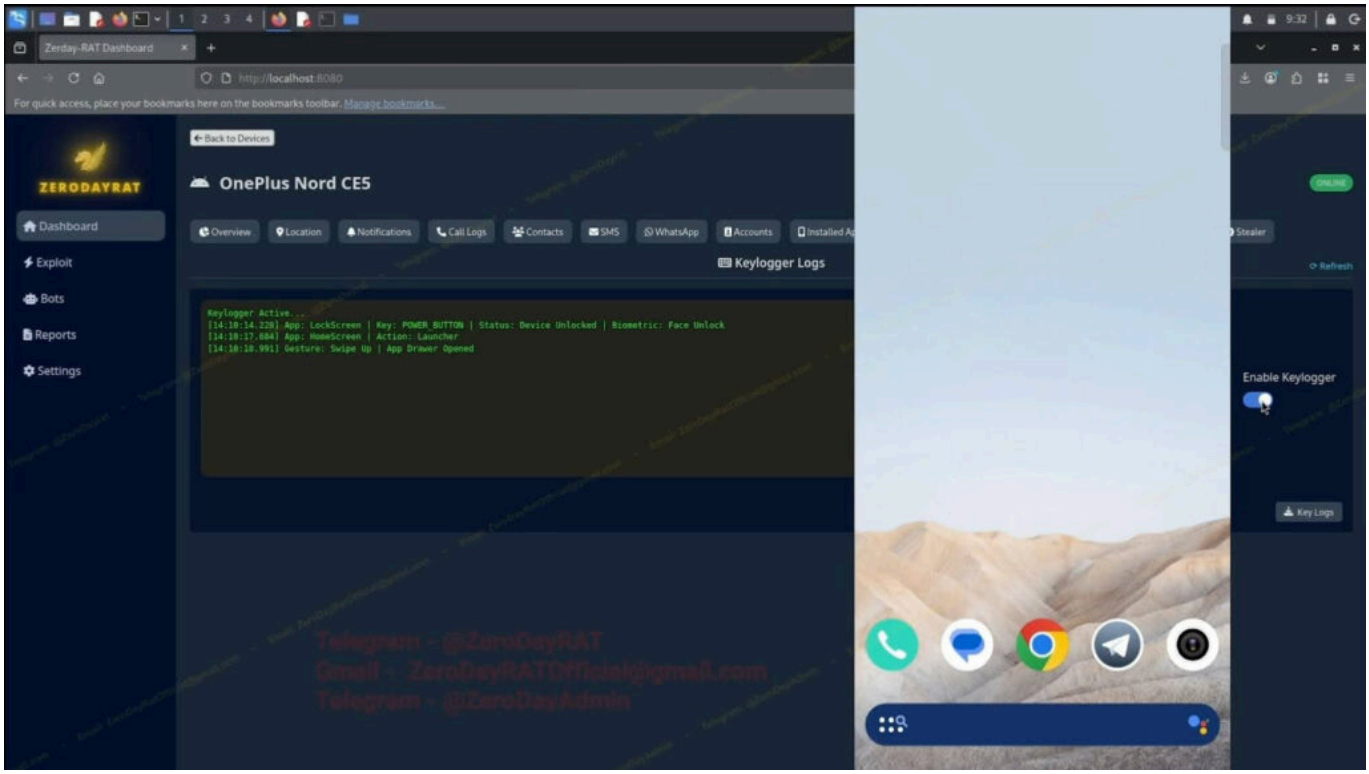
> *«Una de las secciones más preocupantes es la pestaña de cuentas»,* añadió Kelley. *«Se enumeran todas las cuentas registradas en el dispositivo: Google, WhatsApp, Instagram, Facebook, Telegram, Amazon, Flipkart, PhonePe, Paytm, Spotify y otras*

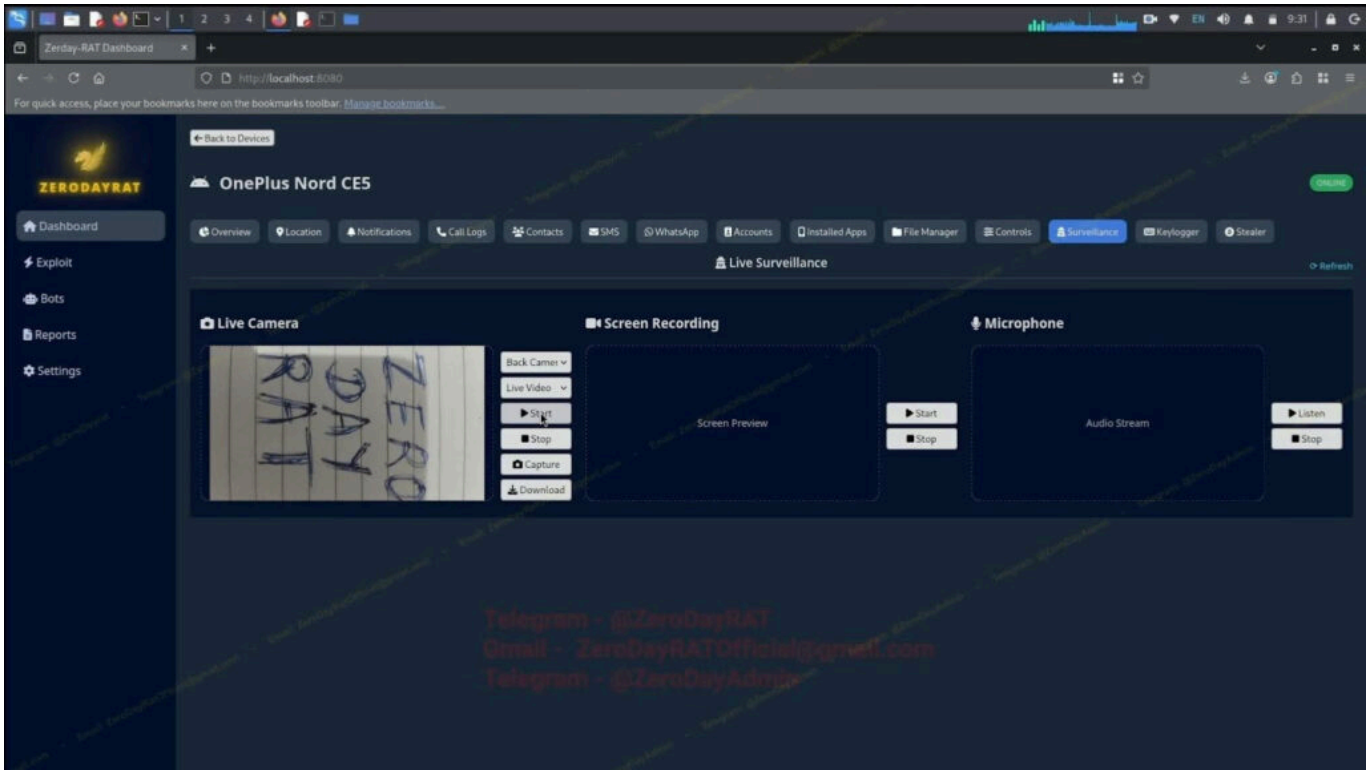
> *más, cada una con su nombre de usuario o correo electrónico asociado.»*

Entre otras funciones, ZeroDayRAT puede registrar pulsaciones de teclas, recopilar mensajes SMS —incluidos códigos OTP para eludir la autenticación en dos factores— y ejecutar acciones directas como activar la cámara en vivo o el micrófono para supervisar remotamente a la víctima.

Para facilitar el robo financiero, el malware integra un módulo *stealer* que analiza aplicaciones de billetera digital como MetaMask, Trust Wallet, Binance y Coinbase, y sustituye las direcciones copiadas en el portapapeles para redirigir las transacciones hacia una billetera controlada por el atacante.

También incorpora un módulo especializado en el robo bancario orientado a plataformas de pago móvil como Apple Pay, Google Pay y PayPal, además de PhonePe, una aplicación india de pagos digitales que permite transferencias instantáneas mediante la Interfaz Unificada de Pagos (UPI).


Zerday-RAT Dashboard
http://localhost:8080
ZERODAYRAT
Dashboard
Exploit
Bots
Reports
Settings
Back to Devices
OnePlus Nord CE5
Overview
Location
Notifications
Call Logs
Contacts
SMS
WhatsApp
Accounts
Keylogger Logs
Enable Keylogger
Key Logs
Refresh



> *«En conjunto, se trata de un kit completo de compromiso móvil, algo que antes requería inversión estatal o el desarrollo de exploits a medida, y que ahora se comercializa en Telegram»*, señaló Kelley. *«Un solo comprador obtiene acceso total a la ubicación, mensajes, finanzas, cámara, micrófono y pulsaciones de teclado del objetivo desde una simple pestaña del navegador. Su compatibilidad multiplataforma y el desarrollo activo lo convierten en una amenaza creciente tanto para individuos como para organizaciones.»*

El malware ZeroDayRAT guarda similitudes con muchas otras amenazas que han atacado a usuarios de dispositivos móviles mediante *phishing* o infiltración en tiendas oficiales de aplicaciones. En los últimos años, actores maliciosos han logrado evadir en repetidas ocasiones las medidas de seguridad implementadas por Apple y Google para inducir a los usuarios a instalar aplicaciones dañinas.

Los ataques dirigidos a iOS suelen aprovechar la capacidad de aprovisionamiento empresarial que permite instalar aplicaciones sin publicarlas en la App Store. Al comercializar herramientas que combinan espionaje, vigilancia y robo de información, los delincuentes reducen la barrera de entrada para hackers menos experimentados y evidencian la creciente sofisticación y persistencia de las amenazas móviles.

La aparición de esta plataforma comercial de *spyware* coincide con diversas campañas recientes de malware y estafas móviles —

Un troyano de acceso remoto (RAT) para Android utilizó Hugging Face para alojar y distribuir archivos APK maliciosos. La cadena de infección comienza cuando los usuarios descargan una aplicación aparentemente inofensiva que actúa como *dropper* (por ejemplo, TrustBastion), la cual solicita instalar una actualización que descarga el APK malicioso. Posteriormente, el malware pide permisos de accesibilidad y acceso a controles sensibles para habilitar vigilancia y robo de credenciales.

Un RAT para Android llamado Arsink emplea Google Apps Script para exfiltrar archivos y contenido multimedia hacia Google Drive, además de usar Firebase y Telegram como infraestructura C2. Se distribuye mediante enlaces en Telegram, Discord y MediaFire, suplantando marcas populares, y ha afectado principalmente a usuarios en Egipto, Indonesia, Irak, Yemen y Turquía.

Una aplicación llamada All Document Reader, publicada en Google Play, fue señalada por actuar como instalador del troyano bancario Anatsa (también conocido como TeaBot o Toddler). Antes de su eliminación, superó las 50.000 descargas.

El troyano bancario deVixor ha atacado activamente a usuarios iraníes a través de sitios de *phishing* que imitan negocios automotrices legítimos. Además de recolectar información confidencial, incluye un módulo de *ransomware* activado remotamente que puede bloquear dispositivos y exigir pagos en criptomonedas.

Una campaña denominada ShadowRemit utilizó aplicaciones Android falsas y páginas que

imitaban Google Play para promover transferencias internacionales no autorizadas. *«Se instruye a las víctimas para que envíen pagos a cuentas beneficiarias y proporcionen capturas de pantalla como prueba de verificación»,* indicó CTM360. *«Este método puede eludir los canales regulados de remesas y coincide con patrones de cuentas mula.»*

Otra campaña en India explotó la confianza en servicios gubernamentales y plataformas digitales oficiales para distribuir APK maliciosos vía WhatsApp, desplegando malware capaz de robar datos, mantener control persistente y ejecutar minería de criptomonedas.

Los operadores del troyano Triada utilizaron páginas de *phishing* que simulaban actualizaciones del navegador Chrome para engañar a usuarios y distribuir APK maliciosos alojados en GitHub.

Una estafa orientada a WhatsApp recurrió a videollamadas en las que el atacante se hacía pasar por representante bancario o soporte de Meta, solicitando compartir la pantalla e instalar aplicaciones legítimas de acceso remoto como AnyDesk o TeamViewer para sustraer información sensible.

Una campaña de *spyware* en Android empleó tácticas de estafa romántica en Pakistán para distribuir una aplicación maliciosa de citas llamada GhostChat, diseñada para exfiltrar datos. Los actores también estarían detrás de ataques ClickFix y GhostPairing para comprometer dispositivos y cuentas de WhatsApp.

Una nueva familia de troyanos de fraude por clic denominada Phantom utiliza TensorFlow.js para detectar e interactuar automáticamente con anuncios en WebView ocultos. También puede transmitir video en vivo mediante WebRTC para permitir a los atacantes interactuar remotamente con el navegador virtual.

El malware NFCShare se difundió mediante una campaña de *phishing* que suplantaba a Deutsche Bank, induciendo a instalar un archivo “deutsche.apk” que leía datos NFC y los enviaba a un servidor remoto. Comparte características con familias como NGate, ZNFC, SuperCard X, PhantomCard y RelayNFC.

En un informe publicado el mes pasado, Group-IB señaló un aumento significativo del malware Android con tecnología NFC para pagos sin contacto, promocionado en comunidades de ciberdelincuencia chinas en Telegram. Esta técnica también se conoce como Ghost Tap.

> *«Al menos 355.000 dólares en transacciones ilegítimas se registraron de un solo proveedor de POS entre noviembre de 2024 y agosto de 2025»,* indicó la empresa. *«En otro escenario, billeteras móviles precargadas con tarjetas comprometidas son utilizadas por mulas en todo el mundo para realizar compras.»*

Group-IB identificó tres proveedores principales de aplicaciones NFC relay para Android: TX-NFC, X-NFC y NFU Pay, siendo TX-NFC el que acumuló más de 25.000 suscriptores en Telegram desde enero de 2025.

El objetivo final de estos ataques es inducir a las víctimas a instalar malware con capacidades NFC y acercar sus tarjetas físicas al teléfono, permitiendo que los datos de la transacción sean capturados y retransmitidos al dispositivo del ciberdelincuente a través de un servidor controlado por este. Esto se complementa con una aplicación instalada en el dispositivo de la mula para completar pagos o retirar fondos como si la tarjeta estuviera físicamente presente.

Al calificar las estafas *tap-to-pay* como una amenaza en expansión, Group-IB indicó que detectó un incremento constante de artefactos de malware entre mayo de 2024 y diciembre de 2025. *«Al mismo tiempo, surgen nuevas familias y variantes, mientras las anteriores continúan activas»,* concluyó. *«Esto demuestra la difusión de esta tecnología entre los estafadores.»*