Investigadores en ciberseguridad han revelado el funcionamiento interno de un malware para Android llamado AntiDot, que ha comprometido a más de 3,775 dispositivos en el marco de 273 campañas distintas.

> *"Operado por el actor de amenazas LARVA-398, motivado por fines económicos, AntiDot se comercializa activamente como un servicio de malware (MaaS) en foros clandestinos, y ha sido vinculado con una amplia variedad de campañas móviles,"* explicó PRODAFT en un informe.

AntiDot se promociona como una solución *"todo en uno",* con funciones para grabar la pantalla del dispositivo mediante el abuso de los servicios de accesibilidad de Android, interceptar mensajes SMS y extraer información confidencial de aplicaciones de terceros.

Se sospecha que este botnet para Android se distribuye mediante redes de publicidad maliciosa o a través de campañas de phishing altamente dirigidas, adaptadas según el idioma y la ubicación geográfica de las víctimas.

La primera documentación pública de AntiDot apareció en mayo de 2024, cuando se detectó que se disfrazaba como actualizaciones de Google Play para robar información.

Al igual que otros troyanos en Android, cuenta con una gama de funcionalidades que incluyen ataques por superposición de pantalla, registro de pulsaciones y control remoto del dispositivo a través de la API MediaProjection. Además, establece una conexión WebSocket para comunicación en tiempo real entre el servidor externo y el dispositivo infectado.

En diciembre de 2024, Zimperium reveló detalles sobre una campaña de phishing móvil que distribuía una versión actualizada de AntiDot conocida como AppLite Banker, usando señuelos relacionados con ofertas de trabajo.

Los hallazgos más recientes de la empresa suiza de ciberseguridad indican que hay al menos 11 servidores C2 activos, que gestionan un mínimo de 3,775 dispositivos infectados

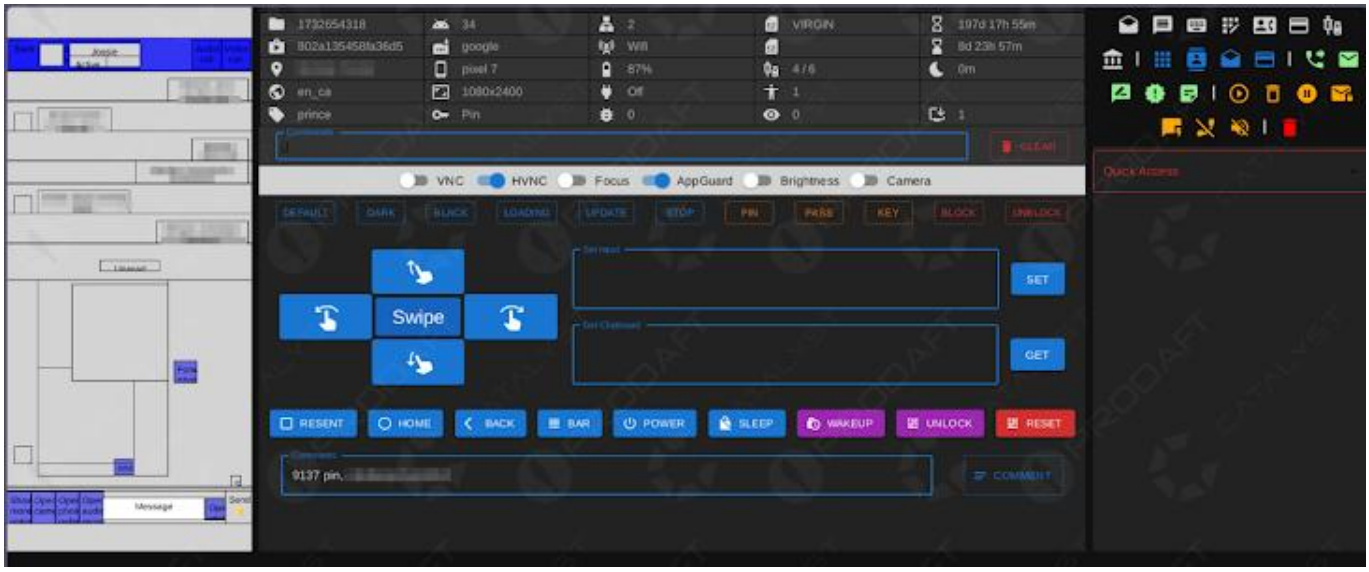
distribuidos en 273 campañas diferentes.

Desarrollado en Java, AntiDot se encuentra fuertemente ofuscado utilizando un empacador comercial, lo cual dificulta su detección y análisis. Según PRODAFT, se entrega a través de un proceso en tres etapas, comenzando con un archivo APK.

> *"Al inspeccionar el archivo AndroidManifest, se observa que muchos nombres de clase no aparecen en el APK original,"* indicó la empresa. *"Estas clases ausentes se cargan dinámicamente durante la instalación mediante el empacador, e incluyen código malicioso extraído desde un archivo cifrado. Todo el mecanismo está diseñado específicamente para evadir el software antivirus."*

Al ejecutarse, AntiDot muestra una falsa barra de actualización y solicita permisos de accesibilidad. Una vez concedidos, descomprime y carga un archivo DEX que contiene las funciones del botnet.

Una función clave del malware es su capacidad para detectar nuevas aplicaciones abiertas por el usuario y mostrar una pantalla falsa de inicio de sesión desde el servidor C2 cuando se abren apps de criptomonedas o de pagos que interesan a los operadores.



También abusa de los servicios de accesibilidad para recolectar información detallada sobre lo que aparece en pantalla, y se configura como la aplicación predeterminada para SMS, lo que le permite interceptar mensajes entrantes y salientes. Adicionalmente, puede monitorizar llamadas telefónicas, bloquear números específicos o redirigirlas, abriendo nuevas vías para el fraude.

Otra capacidad importante del malware es su habilidad para vigilar en tiempo real las notificaciones que aparecen en la barra de estado, pudiendo silenciarlas o descartarlas para evitar que el usuario detecte actividad sospechosa.

PRODAFT también detalló que el panel C2 que permite controlar remotamente los dispositivos infectados está construido con MeteorJS, un framework JavaScript de código abierto para comunicación en tiempo real. El panel tiene seis pestañas principales:

- Bots: muestra la lista de dispositivos comprometidos junto con sus detalles.
- Injects: enumera las aplicaciones objetivo para los ataques por superposición y permite ver las plantillas usadas.
- Analytic: contiene el listado de apps instaladas en los dispositivos de las víctimas, útil para identificar nuevas aplicaciones populares a atacar.

- Settings: permite modificar la configuración principal, incluyendo la actualización de los ataques por inyección.
- Gates: gestiona los puntos de conexión de la infraestructura de bots.
- Help: proporciona recursos de soporte para el uso del malware.

> *"AntiDot representa una plataforma MaaS escalable y difícil de detectar, diseñada para el lucro financiero mediante el control continuo de dispositivos móviles, especialmente en regiones específicas por idioma o localización,"* señaló la empresa. *"El malware también utiliza inyecciones con WebView y ataques por superposición para robar credenciales, constituyendo una amenaza seria a la privacidad del usuario y la seguridad del dispositivo."*

El regreso de GodFather

Este descubrimiento coincide con el anuncio de Zimperium zLabs, que ha identificado una evolución avanzada del troyano bancario para Android conocido como GodFather, el cual ahora emplea virtualización local en el dispositivo para manipular aplicaciones legítimas de banca y criptomonedas y ejecutar fraudes en tiempo real.

> *"El núcleo de esta nueva técnica radica en la capacidad del malware de crear un entorno virtual completo e independiente dentro del dispositivo de la víctima. En lugar de imitar solo la pantalla de inicio de sesión, el malware instala una aplicación 'host' maliciosa que incorpora un framework de virtualización,"* explicaron los investigadores Fernando Ortega y Vishnu Pratapagiri.
>
> *"Dicho host descarga y ejecuta una copia real de la aplicación bancaria o de criptomonedas dentro de su entorno aislado controlado."*

Cuando el usuario abre la aplicación, es redirigido a la versión virtualizada, desde donde los

atacantes pueden observar todas sus acciones. Además, esta nueva versión de GodFather incluye mecanismos para evitar el análisis estático, como la manipulación de archivos ZIP y la inclusión de permisos irrelevantes en el archivo AndroidManifest.

Al igual que AntiDot, GodFather también se apoya en los servicios de accesibilidad para recopilar información y controlar el dispositivo comprometido. Si bien Google ha aplicado restricciones que impiden a las aplicaciones instaladas por fuera de Play Store activar estos servicios en Android 13, los atacantes pueden evadir esta medida mediante un enfoque de instalación por sesiones.

Este método de instalación por sesión es utilizado por tiendas de aplicaciones, apps de mensajería, correo y navegadores para manejar archivos APK.

Una pieza central del funcionamiento de este malware es su sistema de virtualización. En la primera fase, recopila la lista de aplicaciones instaladas y verifica si alguna coincide con las apps que tiene predefinidas como objetivos.

Si se detecta una coincidencia, el malware extrae información relevante de esas aplicaciones y luego instala una copia dentro de un entorno virtual gestionado por la propia app dropper. Así, cuando la víctima intenta abrir la aplicación bancaria real, GodFather intercepta la acción y redirige al usuario hacia la instancia virtualizada.

Cabe destacar que funcionalidades de virtualización similares ya habían sido identificadas anteriormente en otro malware para Android conocido como FjordPhantom, documentado por Promon en diciembre de 2023. Este enfoque representa un cambio de paradigma en las amenazas móviles, ya que supera las técnicas tradicionales de superposición de pantalla para robar credenciales e información confidencial.

> *“Aunque esta campaña de GodFather tiene un alcance global, afectando a casi 500 aplicaciones distintas, nuestro análisis indica que este sofisticado ataque de virtualización se enfoca actualmente en una docena de instituciones financieras en*

> *Turquía,"* informó la empresa.
>
> *"Una capacidad especialmente preocupante que presenta este malware es la posibilidad de robar las credenciales de desbloqueo del dispositivo, ya sea mediante patrón, PIN o contraseña. Esto representa un riesgo crítico para la privacidad del usuario y la seguridad del dispositivo."*

La empresa de seguridad móvil también advirtió que el uso indebido de los servicios de accesibilidad es una de las múltiples vías mediante las cuales las apps maliciosas logran escalar privilegios en Android, obteniendo permisos que exceden lo necesario para su funcionamiento. Esto incluye el mal uso de permisos otorgados por fabricantes (OEM) y la explotación de vulnerabilidades en aplicaciones preinstaladas que los usuarios no pueden eliminar.

> *"Evitar la escalada de privilegios y proteger el ecosistema Android contra apps maliciosas o con excesivos privilegios requiere más que concientización del usuario o parches reactivos — se necesita una defensa proactiva, escalable e inteligente,"* explicó el investigador en seguridad Ziv Zeira.

En una declaración, Google señaló que no ha detectado ninguna aplicación con este malware en Google Play, y que los usuarios de Android están protegidos contra esta amenaza gracias a Google Play Protect.

> *"Los usuarios de Android están protegidos automáticamente contra versiones conocidas de este malware mediante Google Play Protect, que viene activado por defecto en dispositivos con servicios de Google Play,"* indicó un portavoz. *"Google Play Protect puede alertar a los usuarios o bloquear apps que exhiban comportamientos maliciosos, incluso si estas provienen de fuentes externas a la*

> *tienda oficial."*

SuperCard X apunta a usuarios rusos

Estos hallazgos se suman a los primeros reportes de ataques dirigidos a usuarios en Rusia mediante SuperCard X, un nuevo malware para Android que puede llevar a cabo ataques de retransmisión NFC con el fin de realizar transacciones fraudulentas.

Según la empresa rusa de ciberseguridad F6, SuperCard X es una modificación maliciosa de una herramienta legítima llamada NFCGate, la cual permite capturar o manipular el tráfico NFC. El objetivo del malware es interceptar datos de tráfico NFC y también información de tarjetas bancarias mediante comandos enviados al chip EMV.

> *"Esta aplicación permite a los atacantes robar datos de tarjetas bancarias interceptando el tráfico NFC, para luego sustraer dinero de las cuentas de los usuarios,"* explicó el investigador Alexander Koposov en un informe publicado esta semana.

Los primeros ataques con SuperCard X fueron detectados a inicios de este año en Italia, donde se utilizó la tecnología NFC para retransmitir datos de tarjetas físicas hacia dispositivos controlados por atacantes, con los cuales realizaban retiros fraudulentos en cajeros automáticos o autorizaban pagos en terminales PoS.

Esta plataforma MaaS de habla china, que se promociona en Telegram como capaz de atacar clientes de bancos importantes en EE. UU., Australia y Europa, comparte una gran cantidad de código con NGate, otro malware Android que también ha sido vinculado al uso malicioso de NFCGate, en este caso en la República Checa.

Todas estas campañas tienen en común el uso de técnicas de smishing, es decir, mensajes de texto engañosos que convencen a la víctima de instalar un archivo APK bajo el pretexto

de ser una app útil.

Aplicaciones maliciosas en tiendas oficiales

Aunque la mayoría de los malwares mencionados hasta ahora requieren que los usuarios instalen manualmente las apps desde fuentes externas, nuevas investigaciones han descubierto aplicaciones maliciosas presentes en tiendas oficiales como Google Play Store y Apple App Store. Estas apps pueden recolectar datos personales e incluso robar frases semilla de billeteras de criptomonedas, con el objetivo de vaciar los fondos de las víctimas.

Una de las aplicaciones detectadas, llamada RapiPlata, se estima que fue descargada unas 150,000 veces tanto en dispositivos Android como iOS, lo cual demuestra la magnitud del problema. Este software pertenece a la categoría conocida como SpyLoan, que engaña a los usuarios ofreciendo préstamos con bajos intereses, pero en realidad los somete a extorsión, chantaje y robo de datos.

> *"RapiPlata apunta principalmente a usuarios en Colombia, ofreciendo préstamos rápidos,"* explicó Check Point. *"Más allá de sus prácticas abusivas de crédito, la aplicación realiza un extenso robo de datos. Tenía acceso a información sensible como mensajes SMS, registros de llamadas, eventos de calendario y aplicaciones instaladas — e incluso subía esta información a sus servidores."*

Por otro lado, las apps diseñadas para robar frases semilla de billeteras de criptomonedas fueron distribuidas mediante cuentas de desarrolladores comprometidas, sirviendo páginas de phishing a través de WebView para capturar las claves de recuperación.

Aunque dichas aplicaciones ya fueron eliminadas de las tiendas oficiales, el riesgo persiste, ya que pueden seguir circulando en tiendas de terceros. Se recomienda a los usuarios tener especial precaución al descargar aplicaciones relacionadas con finanzas o préstamos.