Se han difundido cuatro troyanos bancarios diferentes a través de la tienda oficial de Google Play entre agosto y noviembre de 2021, lo que resultó en más de 300,000 infecciones por medio de varias aplicaciones de cuentagotas que se hicieron pasar por aplicaciones de utilidad aparentemente inofensivas para tomar el control total de los dispositivos infectados.

Diseñado para entregar Anatsa (también conocido como TeaBot), Alien, ERMAC e Hydra, la compañía de seguridad cibernética ThreatFabric, dijo que las campañas de malware no solo son más refinadas, sino que también están diseñadas para tener una pequeña huella maliciosa, lo que garantiza de forma efectiva que las cargas útiles se instalen solo en dispositivos de teléfonos inteligentes de regiones específicas y evitando que el malware se descargue durante el proceso de publicación.

Una vez instalados, estos troyanos bancarios pueden desviar subrepticiamente contraseñas de usuario y códigos de autenticación de dos factores basados en SMS, pulsaciones de teclas, capturas de pantalla e incluso, agotar las cuentas bancarias de los usuarios sin su conocimiento mediante el uso de una herramienta llamada Automatic Transfer System (ATS). Desde entonces, las aplicaciones que fueron eliminadas de Play Store son:

- Autenticador de dos factores (com.flowdivion)
- Protection Guard (com.protectionguard.app)
- QR CreatorScanner (com.ready.qrscanner.mix)
- Master Scanner Live (com.multifunction.combine.qr)
- QR SCanner 2021 (com.qr.code.generate)
- Escáner QR (com.qr.barqr.scangen)
- Escáner de documentos PDF gratuito (com.doscanner.mobile)
- Escáner de documentos PDF – Escanear a PDF (com.xaviermucher.docscannerpro2)
- Crypto Tracker (cryptolistapp.app.com.cryptotracker)
- Gimnasio y entregador físico (com.gym.trainer.jeux)

Aunque Google a inicios del mes instituyó limitaciones para restringir el uso de permisos de accesibilidad que permiten que las aplicaciones maliciosas capturen información confidencial de dispositivos Android, los operadores de dichas aplicaciones están refinando cada vez más

sus tácticas por otros medios, incluso cuando se ven obligados a elegir la forma más tradicional de instalar aplicaciones por medio de app store.

La principal de las técnicas es una llamada control de versiones, en la que las versiones limpias de las aplicaciones se cargan primero y las funcionalidades maliciosas se introducen gradualmente en forma de actualizaciones posteriores de la aplicación.

Otra táctica consiste en diseñar sitios web de comando y control (C2) similares que coincidan con el tema de la aplicación de cuentagotas para pasar por alto los métodos de detección convencionales.

ThreatFabric descubrió seis cuentagotas Anatsa en Play Store desde junio de 2021, con las aplicaciones programadas para descargar una *«actualización»* seguida de la solicitud a los usuarios para otorgar privilegios y permisos del Servicio de Accesibilidad para instalar aplicaciones de fuentes externas desconocidas.

Brunhilda, un actor de amenazas que fue descubierto distribuyendo un troyano de acceso remoto llamado Vultur en julio de 2021, aprovechó las aplicaciones troyanizadas disfrazadas de las aplicaciones creadoras de códigos QR para eliminar el malware Hydra y ERMAC dirigido a usuarios en Estados Unidos, un mercado que antes no era el objetivo de las dos familias de malware.

Finalmente, se descubrió que una aplicación de cuentagotas de entregamiento físico con más de 10,000 instalaciones, denominada GymDrop, ofrecía la carga útil del troyano bancario Alien, enmascarada como un *«nuevo paquete de ejercicios de entrenamiento»*, incluso cuando su sitio web para desarrolladores supuestamente legítimo se duplicó como el servidor C2 para buscar la configuración necesaria para descargar el malware.

> *«Para hacerse aún más difíciles de detectar, los actores detrás de dichas aplicaciones de cuentagotas solo activan manualmente la instalación del troyano bancario en un dispositivo infectado en caso de que deseen más víctimas en una*

> *región específica del mundo. Esto hace que la detección automatizada sea una estrategia mucho más difícil de adoptar por cualquier organización»,* dijeron los investigadores.