En una señal de que los hackers siguen encontrando formas de evitar las protecciones de seguridad de Google Play Store, los investigadores detectaron un troyano cuentagotas de Android previamente no documentado que se encuentra actualmente en desarrollo.

> *«Este nuevo malware intenta abusar de los dispositivos utilizando una técnica novedosa, nunca antes vista en el malware de Android, para propagar el extremadamente peligroso troyano bancario Xenomorph, lo que permite a los ciberdelincuentes realizar fraudes en dispositivos de las víctimas»,* dijo Han Sahin, de ThreatFabric.

Nombrada como BugDrop por la compañía de seguridad holandesa, la aplicación cuentagotas está diseñada explícitamente para derrotar las nuevas funciones introducidas en la siguiente versión de Android, que tiene como objetivo dificultar que el malware solicite privilegios de Servicios de Accesibilidad a las víctimas.

ThreatFabric atribuyó el cuentagotas a un grupo de ciberdelincuentes conocido como *«Hadoken Security»,* que también está detrás de la creación y distribución de las familias de malware para Android Xenomorph y Gymdrop.

Los troyanos bancarios generalmente se implementan en dispositivos Android por medio de aplicaciones cuentagotas inocuas que se hacen pasar por aplicaciones de productividad y utilidades que, una vez instaladas, engañan a los usuarios para que otorguen permisos invasivos.

Particularmente, la API de accesibilidad, que permite que las aplicaciones lean el contenido de la pantalla y realicen acciones en nombre del usuario, ha sido objeto de fuertes abusos, lo que permite a los operadores de malware capturar datos confidenciales, como credenciales e información financiera.

Esto se logra mediante lo que se denomina ataques de superposición, en los que el troyano inyecta un formulario de inicio de sesión similar a un falso que se recupera de un servidor

remoto cuando la víctima abre una aplicación deseada, como una billetera de criptomonedas.

Debido a que la mayoría de estas aplicaciones maliciosas están descargadas, algo que solo es posible si el usuario ha permitido la instalación desde fuentes desconocidas, Google, con Android 13, dio el paso de bloquear el acceso a la API de accesibilidad a las aplicaciones instaladas desde fuera de una tienda de aplicaciones.

Pero eso no ha impedido que los atacantes intenten eludir esta configuración de seguridad restringida. BugDrop se hace pasar por una aplicación de lector de códigos QR y sus autores la están probando para implementar cargas útiles maliciosas a través de un proceso de instalación basado en sesiones.

> *«Lo que probablemente sucede es que los actores están usando un malware ya creado, capaz de instalar nuevos APK en un dispositivo infectado, para probar un método de instalación basado en sesiones, que luego se incorporaría en un cuentagotas más elaborado y refinado»,* dijeron los investigadores.

Los cambios, si se hicieran realidad, podrían convertir a los troyanos bancarios en una forma más peligrosa capaz de eludir las defensas de seguridad incluso antes de que estén en su lugar.

> *«Con la finalización y resolución de todos los problemas actualmente presentes en BugDrop, los delincuentes tendrán otra arma eficaz en la guerra contra los equipos de seguridad y las instituciones bancarias, derrotando las soluciones que Google está adoptando actualmente, que claramente no son suficientes para disuadir a los delincuentes»,* dijo la compañía.

Se recomienda a los usuarios que eviten ser víctimas del malware oculto en las tiendas de aplicaciones oficiales y solo descarguen aplicaciones de desarrolladores y editores conocidos, analicen las reseñas de las aplicaciones y verifiquen sus políticas de privacidad.