Google reveló que sus funciones de seguridad mejoradas y los procesos de revisión de aplicaciones lo ayudaron a bloquear la publicación de 1.43 millones de aplicaciones maliciosas en Play Store en 2022.

Además, la compañía dijo que prohibió 173,000 cuentas maliciosas y evitó más de 2 mil millones de dólares en transacciones fraudulentas y abusivas por medio de funciones para desarrolladores como API de compras anuladas, ID de cuenta ofuscada y API de integridad de juegos.

La adición de métodos de verificación de identidad como número de teléfono y dirección de correo electrónico para unirse a Google Play contribuyó a una reducción en las cuentas usadas para publicar aplicaciones que van en contra de sus políticas, dijo Google.

La compañía dijo también que *«evitó que alrededor de 500,000 aplicaciones enviadas accedieras innecesariamente a permisos confidenciales en los últimos 3 años».*

> *«En 2022, el programa de mejoras de seguridad de aplicaciones ayudó a los desarrolladores a corregir ~500,000 vulnerabilidades de seguridad que afectaban a ~300,000 aplicaciones con una base de instalación combinada de aproximadamente 250,000 millones de instalaciones»*, dijo.

En contraste, Google bloqueó la publicación de 1.2 millones de aplicaciones que violan las políticas y prohibió 190,000 cuentas maliciosas en 2021.

El desarrollo se produce semanas después de que Google promulgó una nueva política de eliminación de datos que requiere que los desarrolladores de aplicaciones ofrezcan una *«opción fácilmente detectable»* a los usuarios tanto dentro como fuera de una aplicación.

A pesar de estos esfuerzos de Google, los ciberdelincuentes siguen encontrando formas de eludir las protecciones de seguridad de la tienda de aplicaciones y publican aplicaciones maliciosas y de adware.

Por ejemplo, el equipo de investigación móvil de McAfee, descubrió 38 juegos disfrazados de Minecraft y que han sido instalados por no menos de 35 millones de usuarios en todo el mundo, principalmente ubicados en Estados Unidos, Canadá, Corea del Sur y Brasil.

Se ha descubierto que estas aplicaciones de juegos, si bien ofrecen la funcionalidad prometida, incorporan el malware HiddenAds para cargar anuncios sigilosamente en segundo plano para generar ingresos ilícitos para sus operadores.

Algunas de las aplicaciones más descargadas son:

- Caja de bloques Master Diamond (com.good.robo.game.builder.craft.block)
- Craft Sword Mini Fun (com.craft.world.fairy.fun.everyday.block)
- Caja de bloques Skyland Sword (com.skyland.pet.realm.block.rain.craft)
- Craft Monster Crazy Sword (com.skyland.fun.block.game.monster.craft)
- Bloque Pro Forrest Diamond (com.monster.craft.block.fun.robo.fairy)

> *«Uno de los contenidos más accesibles para los jóvenes que usan dispositivos móviles son los juegos. Los autores de malware también son conscientes de esto y tratan de ocultar sus características maliciosas dentro de los juegos»,* dijo McAfee.

Para complicar el problema, está el aumento del malware bancario de Android que los hackers pueden usar como arma para obtener acceso a los dispositivos de las víctimas y recopilar información personal.

Otra tendencia emergente es el uso de servicios vinculantes para troyanizar aplicaciones legítimas y ocultar una carga maliciosa de APK. Esta técnica ha sido adoptada por atacantes para distribuir una botnet de Android denominada DAAM, según Cyble.

El malware, una vez instalado, establece conexiones con un servidor remoto para realizar una amplia gama de acciones maliciosas, incluyendo la actuación como ransomware mediante el cifrado de archivos almacenados en los dispositivos mediante una contraseña

recuperada del servidor.

DAAM también abusa de los servicios de accesibilidad de Android para monitorear la actividad de los usuarios, lo que le permite registrar pulsaciones de teclas, grabar llamadas VoIP desde aplicaciones de mensajería instantánea, recopilar el historial del navegador, registros de llamadas, fotos, capturas de pantalla y mensajes SMS, ejecutar código arbitrario y abrir URL de phishing.

> *«Los autores de malware por lo general aprovechan aplicaciones genuinas para distribuir código malicioso y evitar sospechas»,* dijo la compañía de seguridad cibernética.

Los hallazgos también siguen un aviso de CloudSEK, que descubrió que varias aplicaciones populares de Android como Canva, LinkedIN, Strava, Telegram y WhatsApp no invalidan ni revalidan las cookies de sesión después de que los datos de la aplicación se transfieren de un dispositivo a otro.

Aunque este escenario de ataque requiere que un adversario tenga acceso físico al teléfono de un objetivo, podría permitir la apropiación de la cuenta y otorgar a un adversario acceso no autorizado a datos confidenciales.

Para mitigar dichas amenazas, se recomienda habilitar la autenticación de dos factores (2FA) para agregar una capa adicional de protección de la cuenta, examinar los permisos de las aplicaciones, proteger los dispositivos con una contraseña y evitar dejarlos desatendidos en lugares públicos.