Los perpetradores de amenazas están empleando una táctica conocida como *«versioning»* para eludir los mecanismos de detección de malware de Google Play Store y focalizarse en los usuarios de Android.

*«Las campañas que emplean versioning suelen apuntar a las credenciales, datos y recursos financieros de los usuarios»*, expresó el Equipo de Acción de Ciberseguridad de Google (GCAT) en su Informe de Horizontes de Amenazas de agosto de 2023, compartido con The Hacker News.

Aunque el versioning no es una novedad, su astucia y difícil detección son notables. En este método, un desarrollador lanza una versión inicial de una aplicación en la Play Store que supera las verificaciones previas a su publicación de Google, pero posteriormente se actualiza con un componente de malware.

Esta modificación se logra al enviar una actualización desde un servidor controlado por el atacante para insertar código malicioso en el dispositivo del usuario mediante una técnica denominada *«dynamic code loading»* (DCL), transformando efectivamente la aplicación en una puerta trasera.

En mayo pasado, ESET descubrió una aplicación de grabación de pantalla llamada *«iRecorder – Screen Recorder»* que se mantuvo inofensiva durante casi un año después de su primera subida a la Play Store, antes de introducir sigilosamente cambios maliciosos para espiar a sus usuarios.

Otro ejemplo de malware que utiliza el método DCL es SharkBot, que ha aparecido repetidamente en la Play Store disfrazado de aplicaciones de seguridad y utilidades.

SharkBot es un troyano financiero que ejecuta transferencias de dinero no autorizadas desde dispositivos comprometidos mediante el protocolo Automated Transfer Service (ATS).

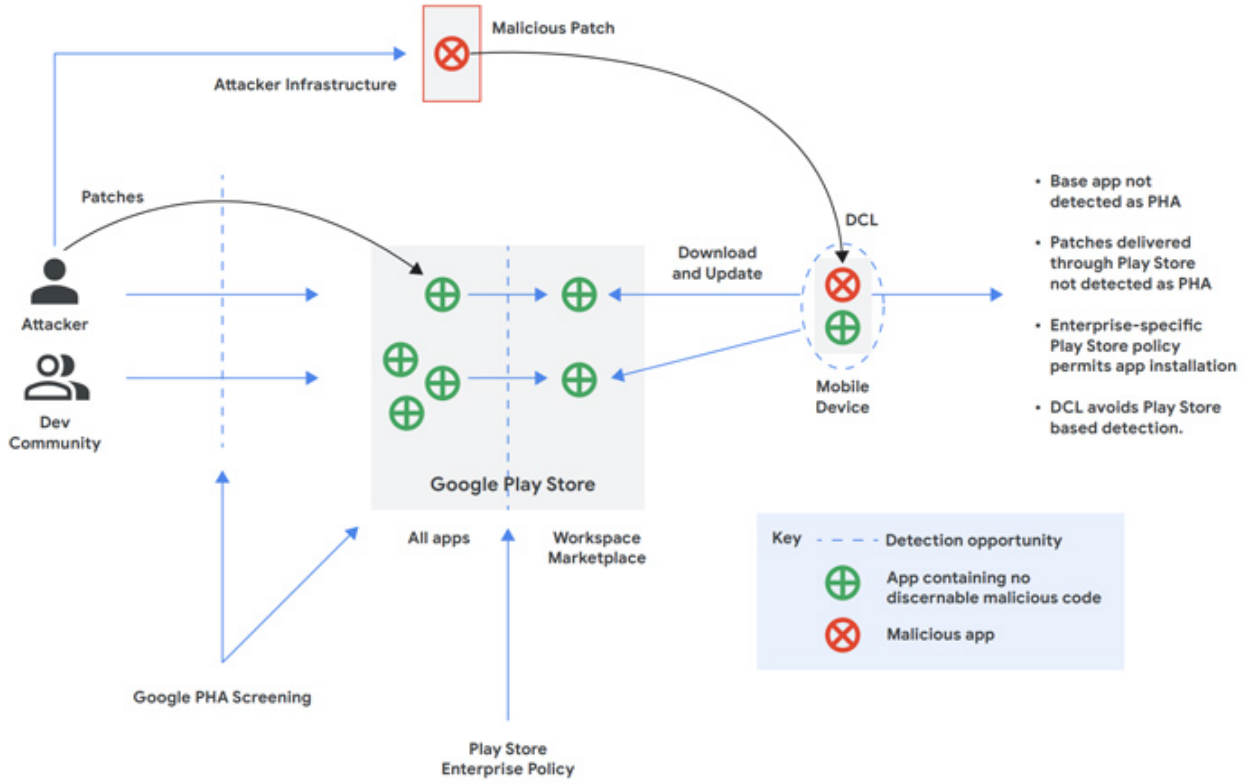


**Fig 1. DCL circumvention of Play Store based security controls to patch malicious behaviors into already-installed applications.**

Las aplicaciones instaladoras que aparecen en la tienda vienen con funcionalidades limitadas que, una vez instaladas por las víctimas, descargan una versión completa del malware con el objetivo de pasar desapercibidas.

> *«En un entorno empresarial, el versioning demuestra la necesidad de principios de defensa en profundidad, incluyendo, entre otros, la limitación de fuentes de instalación de aplicaciones a fuentes confiables como Google Play o la administración de dispositivos corporativos a través de una plataforma de gestión de dispositivos móviles (MDM)»*, afirmó la compañía.

Estos hallazgos surgieron cuando ThreatFabric reveló que los distribuidores de malware han estado aprovechando una vulnerabilidad en Android para disfrazar aplicaciones maliciosas como benignas al *«corromper componentes de una app»* de manera que la aplicación en su conjunto sigue siendo válida, según informó KrebsOnSecurity.

> *«Los actores pueden tener varias aplicaciones publicadas en la tienda al mismo tiempo bajo diferentes cuentas de desarrollador; sin embargo, solo una de ellas es maliciosa, mientras que la otra actúa como respaldo para ser utilizada después de una eliminación»*, mencionó la empresa de ciberseguridad holandesa en junio.

> *«Esta táctica ayuda a los actores a mantener campañas prolongadas, minimizando el tiempo necesario para publicar otro instalador y continuar con la distribución».*

Para reducir los posibles riesgos, se recomienda que los usuarios de Android descarguen aplicaciones solo desde fuentes confiables y que activen Google Play Protect para recibir notificaciones cuando se detecte una aplicación potencialmente dañina (PHA) en el dispositivo.