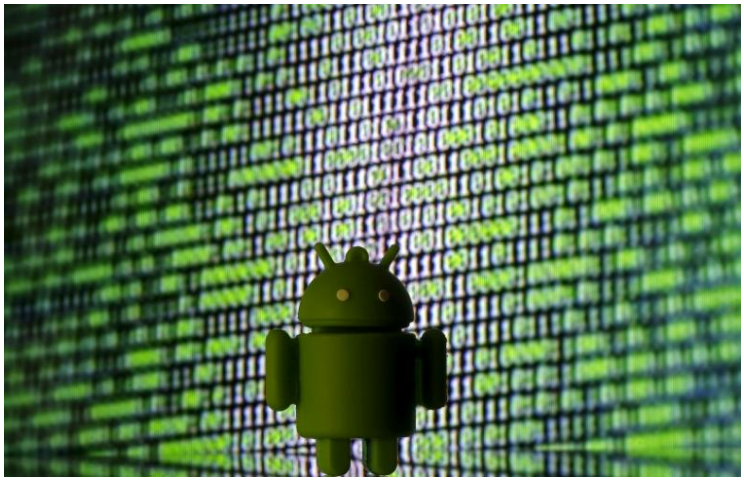
Android: un fallo permite capturas de pantalla remotas

El equipo de investigadores de **Check Point Software Technologies**, firma experta en ciberseguridad, ha informado sobre el descubrimiento de **un defecto de diseño en Android que permite a los ciberdelincuentes realizar capturas de pantalla o de audio de forma remota** sin el conocimiento de la víctima.



De acuerdo con un comunicado de prensa, el ataque se basa en el servicio MediaProjection de Android. Esta herramienta permite grabar sonido o hacer pantallazos con el permiso del usuario. El nuevo ataque usa una táctica de pantalla falsa para engañarle y que dé su consentimiento sin saberlo. A **finales de noviembre, Google sólo había corregido el problema en la versión 8.0 de Android (Oreo),** dejando vulnerables las versiones 5.0, 6.0 y 7.0, que representan aproximadamente el 77,5% de los dispositivos que utilizan este sistema operativo.

Como han explicado los expertos, "a diferencia de otras solicitudes de permiso en Android, como el acceso a contactos o ubicación**, el servicio MediaProjection no tiene una ventana de permiso dedicada para pedir el permiso**. En su lugar, cuando una aplicación intenta utilizarlo, aparece un mensaje diferente, llamada ventana emergente **SystemUI**".

Los investigadores de Check Point descubrieron que mediante una aplicación los ciberdelincuentes pueden detectar cuando está a punto de aparecer esta ventana, mostrar un mensaje falso superpuesto al de SystemUI, y persuadir al usuario para que conceda el consentimiento sin saberlo. Una vez que se ha engañado a la víctima, puede grabar la pantalla y el audio del dispositivo, convirtiéndolo en la herramienta de espionaje definitiva.

La segunda parte del ataque consiste en una táctica de superposición de pantalla, a menudo llamada "**clickjacking**", que es un método muy común utilizado por el **malware móvil,** especialmente el **malware bancario y el ransomware**. Si bien Google ha hecho un esfuerzo significativo para acabar con esta táctica, sigue siendo una manera exitosa de engañar a los usuarios y obtener sus credenciales.

Para protegerse tanto del ataque descubierto recientemente como del amplio panorama de malware móvil, los usuarios y las empresas deben utilizar medidas de seguridad avanzadas capaces de detectar y bloquear cualquier intento de mostrar una ventana falsa o llevar a cabo cualquier actividad maliciosa mediante el análisis dinámico y la determinación del contexto de la actividad.