Se han encontrado hasta 30 aplicaciones maliciosas de Android con descargas acumuladas de casi 10 millones en Google Play Store que distribuyen adware.

> *«Todos ellos se integraron en varios programas, incluido el software de edición de imágenes, teclados virtuales, herramientas y utilidades del sistema, aplicaciones de llamadas, aplicaciones de colección de fondos de pantalla y otros»,* dijo Dr. Web el martes.

Mientras se hacen pasar por aplicaciones inocuas, su objetivo principal es solicitar permisos para mostrar ventanas sobre otras aplicaciones y ejecutarlas en segundo plano para publicar anuncios intrusivos.

Para dificultar que las víctimas detecten y desinstalen las aplicaciones, los troyanos de adware ocultan sus iconos de la lista de aplicaciones instaladas en la pantalla de inicio o reemplazan los iconos con otros que probablemente se notarán menos (por ejemplo, SIM Toolkit).

Algunas de estas aplicaciones también ofrecen las características anunciadas, como se observa en el caso de dos aplicaciones: *«Water Reminder- Tracker & Reminder»* y *«Yoga- For Beginner to Advanced»*. Sin embargo, también cargan de forma encubierta varios sitios web en WebView y simulan las acciones del usuario para hacer clic en banners y anuncios.

También se descubrió otro conjunto de aplicaciones que distribuyen el malware Joker en forma de aplicaciones de inicio, cámara y pegatinas emoji que, cuando se instalan, suscriben a los usuarios a servicios móviles pagos sin su conocimiento y consentimiento.

La tercera categoría de aplicaciones maliciosas se relaciona con aquellas que se hacen pasar por software de edición de imágenes pero, realmente, están diseñadas para entrar en las cuentas de Facebook.

> *«Después del lanzamiento, pidieron a las posibles víctimas que iniciaran sesión en sus cuentas y luego cargaron una página de autorización genuina de Facebook. Luego, secuestraron los datos de autenticación y los enviaron a actores maliciosos»*, dijeron los investigadores de Dr. Web.

- Editor de fotos: Filtro de belleza (gb.artfilter.tenvarnist)
- Editor de fotos: Retoque y recorte (de.nineergysh.quickarttwo)
- Editor de fotos: Filtros artísticos (gb.painnt.moonlightingnine)
- Editor de fotos – Creador de diseños (gb.twentynine.redaktoridea)
- Editor de fotos y borrador de fondo (de.photoground.twentysixshot)
- Photo & Exif Editor (de.xnano.photoexifeditornine)
- Editor de fotos – Efectos de filtros (de.hitopgop.sixtyeightgx)
- Filtros y efectos de fotos (de.sixtyonecollice.cameraroll)
- Editor de fotos: Imagen borrosa (de.instgang.fiftyggfife)
- Photo Editor : Cut, Paste (de.fiftyninecamera.rollredactor)
- Teclado emoji: pegatinas y GIF (gb.crazykey.sevenboard)
- Teclado de tema de neón (com.neonthemekeyboard.app)
- Tema de neón – Teclado de Android (com.androidneonkeyboard.app)
- Cashe Cleaner (com.cachecleanereasytool.app)
- Carga elegante (com.fancyanimatedbattery.app)
- FastCleaner: Cashe Cleaner (com.fastcleanercashecleaner.app)
- Máscaras de llamadas – Temas de llamadas (com.rockskinthemes.app)
- Persona que llama divertida (com.funnycallercustomtheme.app)
- Temas de CallMe Phone (com.callercallwallpaper.app)
- Llamada entrante: Fondo de contacto (com.mycallcustomcallscrean.app)
- MyCall – Personalización de llamadas (com.mycallcallpersonalization.app)
- Tema de llamada (com.caller.theme.slow)
- Tema de la persona que llama (com.callertheme.firstref)
- Fondos de pantalla divertidos – Pantalla en vivo (com.funnywallpapaerslive.app)
- 4K Wallpapers Auto Changer (de.andromo.ssfiftylivesixcc)
- NewScrean: fondos de pantalla 4D (com.newscrean4dwallpapers.app)

- Fondos de pantalla y fondos de archivo (de.stockeighty.onewallpapers)
- Notas: recordatorios y listas (com.notesreminderslists.app)

Finalmente, también se vio en la tienda de aplicaciones una app de comunicaciones no autorizada conocida como *«Chat Online»,* que engaña a los usuarios para que proporcionen sus números de teléfono móvil con el pretexto de suscribirse a servicios de citas en línea.

En una versión distinta del mismo malware, se inicia una conversación aparentemente real, solo para que la aplicación solicite a los usuarios que paguen por el acceso premium para seguir con el chat, lo que genera cargos fraudulentos.

Aunque estas aplicaciones fueron eliminadas, es seguro que el malware haya demostrado ser resistente, ya que los atacantes constantemente encuentran nuevas formas de eludir las protecciones implementadas por Google.

Se recomienda a los usuarios que tengan cuidado extremo al descargar aplicaciones incluso de Google Play u otras tiendas, además de abstenerse de otorgar permisos extensos a las aplicaciones.