Troyano «Necro» infecta a 11 millones de usuarios de apps

Un nuevo informe de Kaspersky, compañía dedicada a la seguridad informática, revela que el troyano denominado ‘Necro’ ha infectado al menos 11 millones de dispositivos Android a través de aplicaciones en Google Play y versiones modificadas de apps populares.

De acuerdo a los investigadores de Kaspersky, dos aplicaciones en Google Play, Wuta Camera y Max Browser, se encontraban entre las afectadas, acumulando más de 10 millones y 1 millón de descargas respectivamente. Solo una de estas ha sido eliminada de la tienda.

Wuta Camera ha sido descargada más de 10 millones de veces en Google Play Store, según su página oficial. Esta aplicación, fue obligada por Google a eliminar el código malicioso en una actualización, por lo que aún se encuentra disponible para su descarga.

Por otro lado está Max Browser, un navegador que se promocionaba como centrado en la privacidad y que superó el millón de descargas, fue señalada por contener el troyano ‘Necro’. Frente a esto, Google decidió retirarla completamente de la tienda de aplicaciones.

Las alertas continúan

Sin embargo, a pesar de que las acciones que se tomó frente a estas apps, la amenaza persiste en sitios web que ofrecen versiones modificadas o ‘APKs’ de aplicaciones populares como Spotify, WhatsApp y Minecraft.

Estos mods a menudo atraen a los usuarios con la promesa de funciones premium gratuitas, pero esconden el malware ‘Necro’. Como usuarios hay que tener en cuenta que una vez instalado, Necro puede:

Mostrar anuncios intrusivos en ventanas WebView invisibles.
Descargar y ejecutar archivos maliciosos.
Suscribir a los usuarios a servicios de pago sin su conocimiento.
Redirigir el tráfico de Internet a través de dispositivos infectados, usándolos como servidores proxy.
Sin embargo, hay formas de evitar caer en este tipo de troyanos,

por lo que para protegerse contra esta amenaza, se recomienda:

Descargar aplicaciones únicamente de fuentes oficiales como Google Play Store.
Ser cauteloso con las ofertas que parecen demasiado buenas para ser verdad, especialmente las que prometen funciones premium gratuitas.
Mantener el dispositivo actualizado con los últimos parches de seguridad.
Utilizar un software de seguridad confiable para detectar y eliminar amenazas como Necro.

Es importante destacar que incluso Google Play Store no es completamente inmune a este tipo de malware, por lo que es fundamental ser precavido al descargar cualquier aplicación, incluso si proviene de una fuente aparentemente confiable.

Con información de RPP