Alertan sobre nuevo virus que circula en los dispositivos Android

Expertos en ciberseguridad emitieron una alerta sobre un nuevo y peligroso virus que ha logrado infiltrarse en dispositivos Android, poniendo en riesgo la privacidad y seguridad de los usuarios. Se trata del Virus Android Xamalicious, que ha logrado evadir los filtros de seguridad de la Google Play Store y se propaga a través de apps aparentemente inocentes.

El Xamalicious se ha distribuido camuflándose en aplicaciones que van desde salud y juegos hasta horóscopos y productividad. A pesar de que algunas de estas aplicaciones ya han sido eliminadas de la Google Play Store, el virus continúa representando una amenaza para aquellos que podrían haberlas descargado anteriormente.

Una vez instalado, el Xamalicious roba información sensible del dispositivo, incluyendo detalles del sistema operativo, ubicación, contactos y contraseñas. Además, tiene la capacidad de instalar de forma encubierta otra aplicación maliciosa denominada «Cash Magnet», diseñada para generar clics automáticos fraudulentos.

Además de la eliminación de las aplicaciones infectadas de la Google Play Store, se ha publicado una lista de 13 aplicaciones identificadas como portadoras del Xamalicious. Asimismo, se brindan consejos adicionales para protegerse de posibles ataques cibernéticos.

Las aplicaciones afectadas son: Step Keeper: Easy Pedometer. Track Your Sleep, Essential Horoscope for Android, 3D Skin Editor for PE Minecraft, Logo Maker Pro, Auto Click Repeater, Count Easy Calorie Calculator, Sound Volume Extender, LetterLink, Numerology: Personal Horoscope & Number Predictions, Sound Volume Booster, Astrological Navigator: Daily Horoscope & Tarot, y Universal Calculator.

Consejos de protección contra Xamalicious

El Xamalicious representa una amenaza seria, porque ha logrado eludir las medidas de seguridad de la Google Play Store. Los usuarios deben mantenerse vigilantes al descargar aplicaciones y limitarse a fuentes confiables para reducir el riesgo de infección.

Para protegerse contra el Xamalicious y otros riesgos similares, se recomienda seguir algunas prácticas de seguridad. Primordialmente se recomienda descargar aplicaciones únicamente de tiendas oficiales, como la Google Play Store.

Es importante evitar el sideloading, es decir, la instalación de aplicaciones desde sitios web no oficiales. Además, se recomienda instalar y mantener actualizado un antivirus en todos los dispositivos Android. En caso de que se sospeche que un dispositivo ha sido infectado por el Xamalicious, se deben tomar medidas inmediatas para minimizar el riesgo:

Cambiar todas las contraseñas desde otro dispositivo seguro.

Monitorear detenidamente cuentas y transacciones financieras.

Considerar la utilización de servicios de protección de identidad.

Contactar al banco y a las compañías de tarjetas de crédito para informar sobre la situación.

Alertar a todos los contactos sobre la posible infección.

Restaurar el dispositivo a la configuración de fábrica.

Con información de El Tiempo