Sophos descubre *malware* espía en aplicaciones apócrifas de Android

- ***El caso más relevante se presentó en la aplicación del Gobierno de Pakistán y un sitio apócrifo del mismo.***
- ***El 82.89% de los smartphones en México utilizan dicho sistema operativo.***

CIUDAD DE MÉXICO. 26 de enero de 2021.- Una investigación de SophosLabs reveló la existencia de un pequeño grupo de **versiones troyanizadas de aplicaciones de Android** que fueron modificadas y a las que se les agregaron funciones maliciosas enfocadas a la vigilancia y el espionaje.

Sophos indica que se trata de versiones idénticas a aplicaciones legítimas descargables en Google Play Store. Estas *apps*, incluso, **pueden hacer las mismas funciones que realizan sus contrapartes originales**, pero están diseñadas para descargar dentro del teléfono una carga útil de *malware*, en forma de un archivo ejecutable de Android Davis (DEX).

Este archivo contiene las funciones maliciosas de filtrar de forma encubierta datos del usuario como su lista de contactos, historial de mensajes, entre otros. Según la investigación de Sophos, las aplicaciones envían posteriormente la información robada a un sitio web de comando de control alojado en servidores de Europa del Este, sin que el usuario se dé cuenta.

Uno de los casos más relevantes se encontró en Pakistán, donde fue hallada **una imitación de la app gubernamental Pakistan Citizen Portal.** Esta app, según el sitio Virustotal, no está disponible en Google Play Store, sino en un sitio web idéntico al del gobierno pakistaní, bajo el dominio pmdu.info.

Sophos encontró que, al descargar la app, se le solicita al usuario que ingrese datos sensibles como su número de identificación, detalles de su pasaporte, usuario y contraseña de Facebook, además de accesos invasivos a la privacidad, como la capacidad de leer mensajes SMS y listas de contactos. Una vez entregados dichos datos, los usuarios encuentran una plataforma **casi idéntica a la original**, que aparentemente **cumple con las mismas funciones**, lo que hace que la víctima nunca note que su dispositivo está siendo infiltrado.

¿Cómo protegerse?

En el ecosistema actual de Android, las aplicaciones deben contar con una firma criptográfica como forma de certificar que el código se origina en una fuente legítima, vinculando la aplicación a su desarrollador. Sin embargo, Android no les indica a los usuarios qué apps cuentan con dicha firma de manera válida y cuáles no, lo que implica un riesgo para el

consumidor final. Es decir, **los usuarios no tienen una forma de saber si una aplicación fue publicada por su desarrollador genuino** o si se trata de una copia.

Para evitar ser presa de estas apps maliciosas, los usuarios solo deben instalar aquellas provenientes de fuentes confiables como Google Play Store. Cabe destacar que los desarrolladores de aplicaciones populares a menudo tienen un sitio web que dirige a los usuarios a la app original. Otra recomendación para el usuario es instalar un antivirus en su dispositivo móvil, como Sophos Intercept X for Mobile, que puede detectar este tipo de amenazas

La existencia de casos como los anteriores implica un riesgo importante para la población si consideramos que, de acuerdo con datos de Statcounter, Android cuenta con el 72.48% de los usuarios de telefonía móvil en el mundo, por encima de iOS (26.91%). En México, la relevancia del caso no es menor, ya que el 82.89% de los usuarios cuentan con un *smartphone* que utiliza dicho sistema operativo, mientras que apenas el 16.71% tiene un dispositivo de Apple.

"Contar con soluciones antivirus en el dispositivo móvil, hoy en día, es una necesidad para todos los usuarios ante el creciente riesgo de ser víctimas de amenazas como el spyware, considerando el gran número de usuarios que existen del sistema operativo Android y las vulnerabilidades detectadas en el mismo. Este tipo de aplicaciones maliciosas tienen el peligro de parecer inofensivas y funcionar como apps legítimas, una forma sigilosa de los ciberdelincuentes de infiltrarse en los dispositivos de la gente sin que lo noten", concluyó Leonardo Granda, Gerente de Ingeniería de Ventas en Sophos para Latinoamérica.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de

cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com.

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/