Más de 300,000 usuarios en 71 países fueron víctimas de una nueva campaña de amenazas para Android llamada Schoolyard Bully Trojan.

Diseñado especialmente para robar las credenciales de Facebook, el malware se camufla como aplicaciones legítimas con temas educativos para atraer a los usuarios desprevenidos para que las descarguen.

Las aplicaciones, que estaban disponibles para descargar desde la tienda oficial de Google Play, ahora se han eliminado. Sin embargo, siguen disponibles en tiendas de aplicaciones de terceros.

> *«Este troyano usa la inyección de JavaScript para robar las credenciales de Facebook»,* dijeron los investigadores de Zimperium, Nipun Gupta y Aazim Bill SE Yaswant.

Esto se logra al iniciar la página de inicio de sesión de Facebook en un WebView, que también incorpora código JavaScript malicioso para filtrar el número de teléfono, la dirección de correo electrónico y la contraseña del usuario a un servidor de comando y control (C2) configurado.

El troyano Schoolyard Bully utiliza además bibliotecas nativas como *«libabc.so»* para evitar la detección por parte de las soluciones antivirus.

Aunque el malware identifica aplicaciones en idioma vietnamita, también se ha descubierto en varias otras aplicaciones disponibles en más de 70 países, lo que subraya la escala de los ataques.

Los hallazgos se producen más de un año después de que Zimperium descubriera una

actividad similar destinada a comprometer las cuentas de Facebook a través de aplicaciones de Android no autorizadas como parte de una campaña cuyo nombre en código es FlyTap.

> *«Los atacantes pueden causar muchos estragos al robar contraseñas de Facebook. Si pueden hacerse pasar por alguien desde su cuenta legítima de Facebook, se vuelve extremadamente fácil engañar a amigos y otros contactos para que envíen dinero o información confidencial»,* dijo Richard Melick, director de inteligencia de amenazas móviles de Zimperium.

> *«También es muy preocupante cuántas personas reutilizan las mismas contraseñas. Si un atacante roba la contraseña de Facebook de alguien, existe una alta probabilidad de que el mismo correo electrónico y contraseña funcionen con aplicaciones bancarias o financieras, cuentas corporativas y mucho más».*