Un troyano fue detectado en Play Store, que tiene como objetivo robar dinero de cuentas PayPal, aún teniendo la autenticación de dos factores.

ESET fue la compañía de seguridad cibernética que descubrió el troyano, y según la compañía, se encuentra oculto dentro de una aplicación que promete mejorar el rendimiento de la batería, dicha app es Optimization Battery.

Lukas Stefanko, analista de malware de ESET, informó que el malware tiene la base de un troyano bancario controlado de forma remota, que se ha mejorado y se combina con los servicios de accesibilidad de Android para la app oficial de PayPal.

Su funcionalidad se divide en dos partes principales, una es robar dinero de cuentas PayPal, requiriendo la activación de un servicio de accesibilidad malicioso. Esta característica es muy peligrosa, ya que le permite a una aplicación automatizar los toques de pantalla y las interacciones del sistema operativo.

El troyano presenta la solicitud como si formara parte del servicio de *«Habilitar estadísticas»* de Android. Si el usuario cuenta con la app oficial de PayPal en el dispositivo, el malware le solicita al usuario que lo inicie.

Después de esto, cuando el usuario abra la aplicación de PayPal e inicie sesión, el servicio de accesibilidad maliciosa interviene y realiza la transferencia a la dirección de PayPal del atacante, el usuario no pude hacer nada para detener la transferencia.

> *«Todo el proceso toma alrededor de 5 segundos, para un usuario desprevenido, no existe una forma viable de intervenir a tiempo»*, dice Stefanko.

La segunda función del troyano es la suplantación de identidad, denominada como phishing. El troyano se mantiene encubierto sobre aplicaciones específicas y legítimas descargando pantallas de superposición basadas en HTML para cinco apps, Google Play, WhatsApp, Skype, Viber y Gmail.

Aunque esta técnica ya es muy utilizada, es mejor que en otros malware porque para superar la pantalla de superposición es necesario rellenar el formulario falso, sin embargo, las entradas aleatorias e inválidas hacen que dichas pantallas desaparezcan.

Stefanko asegura que ESET notificó sobre este troyano a PayPal, pidiéndole además que bloquee la cuenta del autor del malware.

ESET recomienda lo siguiente para evitar que este tipo de malware infecte tu dispositivo:

1.- Utilizar aplicaciones de Play Store.
2.- Verificar el número de descargas, calificaciones de las apps y el contenido de las mismas antes de descargarlas.
3.- Revisar los permisos que se otorgan a las aplicaciones que se instalan.
4.- Mantener el dispositivo actualizado.

El especialista en seguridad asegura que para la tranquilidad de todos, la app no es propia de Play Store, sino de un tercero, lo que se traduce en menos usuarios afectados.

Si tuviste la mala suerte de instalar dicha app, debes revisar el resumen de transacciones de PayPal y abrir una controversia ante transacciones no autorizadas.