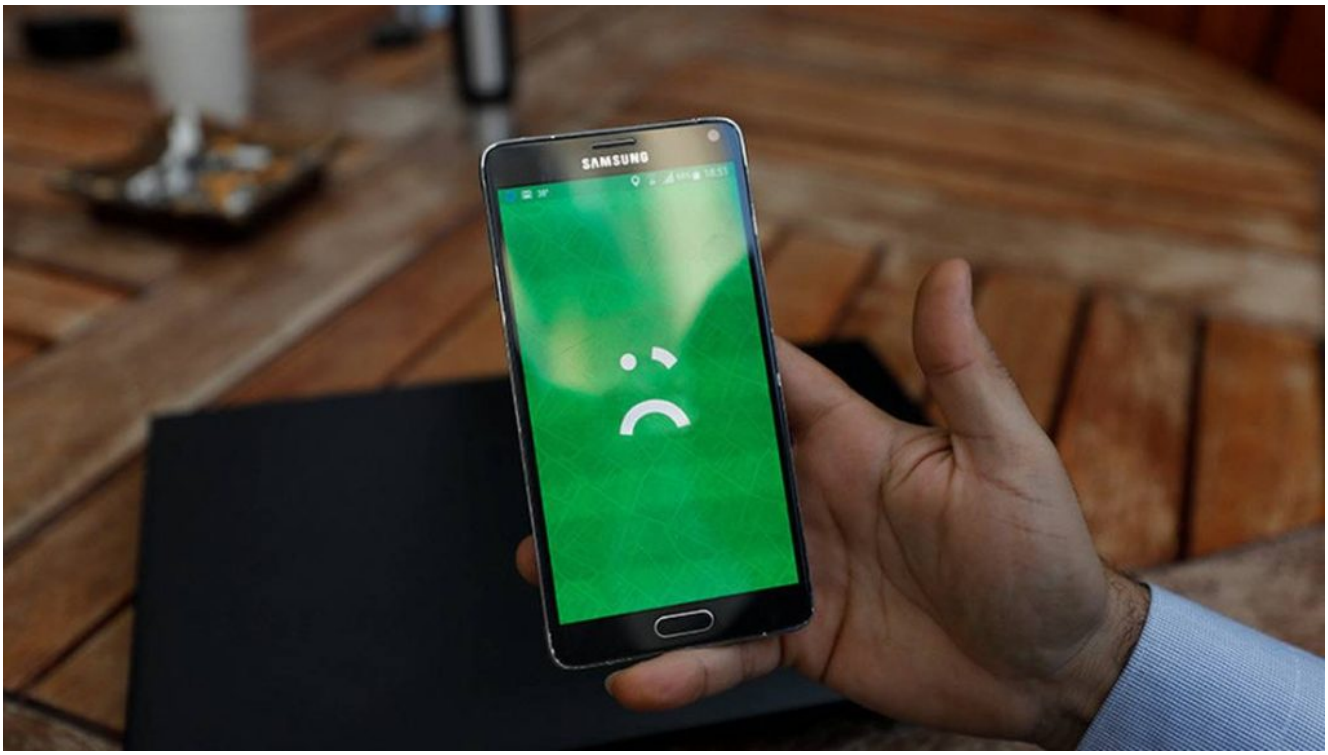
Peligro Play Store: reportan aplicaciones de seguridad que propagan virus bancarios

09/04/2022



Check Point Research, la división de Inteligencia de Amenazas del proveedor líder de soluciones de ciberseguridad a nivel mundial, descubrió seis aplicaciones antivirus en Play Store que propagan malware bancario, es decir, virus que roban información personal. Entérate cómo prevenirlos.

Según el estudio, el 62% de las víctimas están en Italia, el 36% en el Reino Unido y el 2% en otros países. Los ciberdelincuentes implementaron la función de geofencing, que ignora a los usuarios de smartphones en China, India, Rumanía, Rusia, Ucrania y Bielorrusia. Tras el descubrimiento, Google eliminó las aplicaciones.

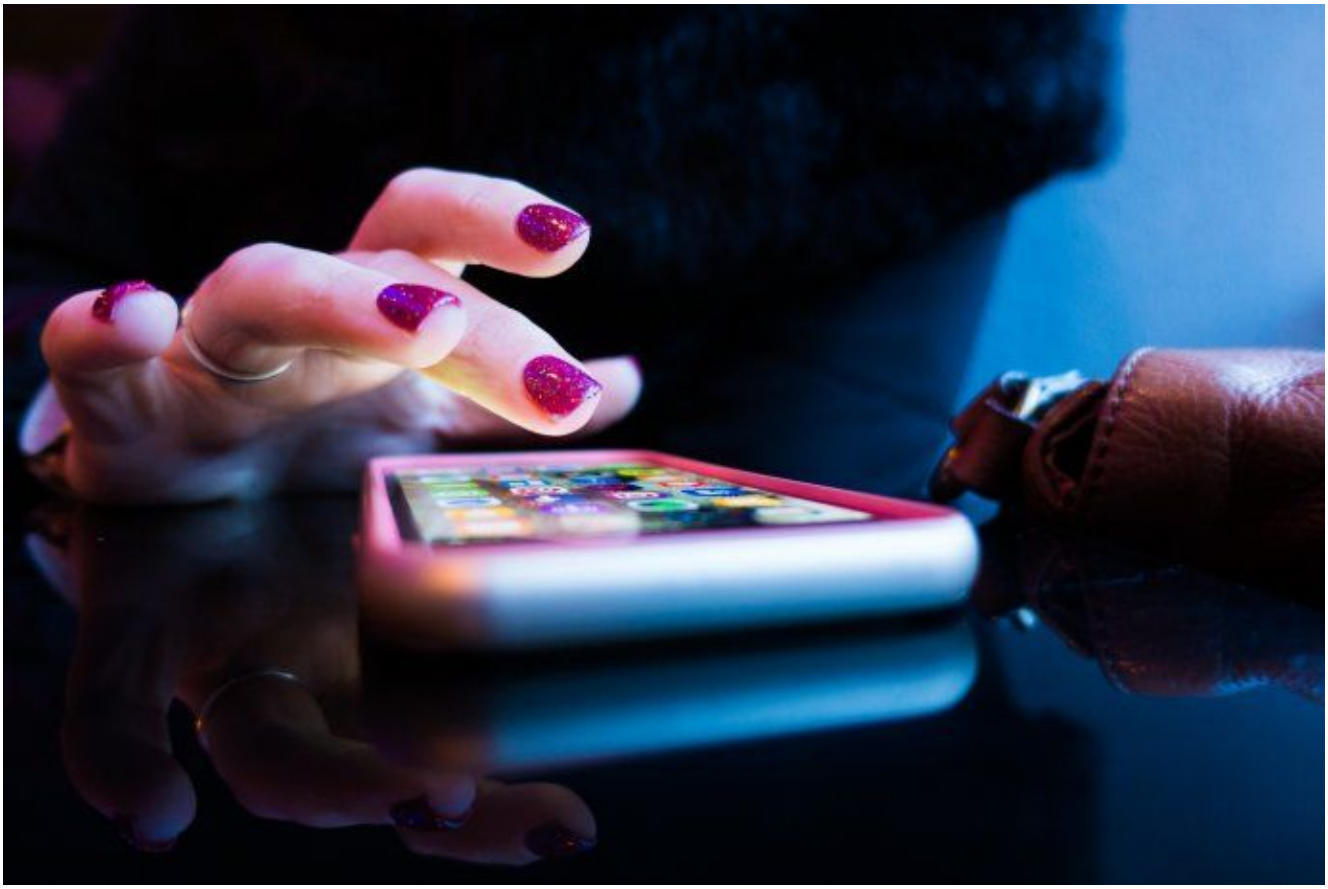
Los investigadores recogieron datos estadísticos durante una semana. A lo largo del tiempo, contaron **más de 1.000 IPs de víctimas**, en su mayoría de Reino Unido e Italia. A su par,

aumenta aproximadamente en **100 nuevas personas afectadas cada día**. Según las estadísticas de Google Play, **hay 11.000 descargas de las seis aplicaciones maliciosas detectadas**.

Cómo funciona el ataque a los smartphones Android

«**Sharkbot**» es el tipo de ataque utilizado que **roba credenciales e información bancaria de los usuarios de Android**. Se trata de un malware que **atrae a sus víctimas** para que introduzcan sus credenciales en ventanas que imitan los formularios de inserción de credenciales.

Entonces, cuando el usuario ingresa sus datos, **la información comprometida se envía a un servidor malicioso**. Asimismo, los investigadores descubrieron que los autores implementaron una función de **geofencing** que hace que no se ejecute el malware si los usuarios de smartphones están en **China, India, Rumanía, Rusia, Ucrania o Bielorrusia**.



Metodología del ataque

- Incluir al usuario para que conceda **permisos de servicio de accesibilidad a la aplicación**.
- Tras ello, el malware obtiene el **control de gran parte del dispositivo** de la víctima.
- Los ciberdelincuentes también pueden enviar **notificaciones push con enlaces maliciosos**.

Pixabay

Cuáles son las aplicaciones de seguridad que propagan virus bancarios

Cuatro de las solicitudes procedían de tres cuentas de desarrolladores: **Zbynek Adamcik, Adelmio Pagnotto y Bingo Like Inc**. Check Point Research detectó que dos de ellas estaban activas desde **2021**. Mientras que algunas de las aplicaciones vinculadas a las mismas **se eliminaron de Google Play, pero siguen existiendo en mercados no oficiales**. Aquello podría significar que el ciberdelincuente que está detrás intenta **pasar desapercibido** mientras sigue participando en actividades maliciosas.

Consejos de seguridad para los usuarios de Android

- Instalar aplicaciones sólo de **proveedores de confianza y verificados**.
- Al ver una aplicación de un editor nuevo, busca **análogos** de uno de confianza.
- **Informa a Google de cualquier aplicación aparentemente sospechosa que se encuentre.**

Fuente: Ámbito