Microdesafío Clase 15 - Grupo 5

https://thehackernews.com/2020/03/android-apps-ad-fraud.html

Tipo de amenaza

Adware.
Simula clicks de los usuarios sobre los anuncios.

Cómo comienza y se propaga

Se clonan apps y se ponen como disponibles para descargar en Google Play sin ser detectadas. Luego, una vez que un usuario la descarga, el malware Tekya registra un recibidor (un componente de Android que se invoca cuando se realiza cierta acción). Cuando ese recibidor detecta ciertos eventos, carga una librería ("libtekya.so") que incluye una subfuncion ("sub_AB2C,") que crea “touch-events”, imitando clicks a través de la API MotionEvent.
Así es como incrustan malware en aplicaciones y servicios online para generar clicks fraudulentos para recibir pagos de sistemas de publicidad.

Cuántas amenazas hay aplicadas

Adware.
Troyano.