4.7. Espionaje

Los móviles y nuestra intimidad

A medida que los teléfonos móviles continúan estando estrechamente integrados en nuestra vida personal y laboral. Registran nuestra actividad telefónica, ubicación, etc. Tener acceso a esta información es posible teniendo acceso al dispositivo móvil.

Por este motivo, algunas empresas están creando aplicaciones sofisticadas que pueden ejecutarse en los dispositivos de las víctimas sin que ellas sepan de la presencia de la amenaza o de la intención de los actores.

Esto se puede ver en la diversidad de amenazas que tienen como objetivo los dispositivos móviles:

Las que tienen una motivación financiera, como el adware, los troyanos bancarios y el fraude por SMS

Las que buscan información personal,propiedad intelectual o información corporativa.

¿Qué es el spyware?

Se trata de una aplicación maliciosa diseñada para recopilar y recuperar información de un dispositivo infectado sin el conocimiento de la víctima.

Entre la información que pueden extraer se encuentran:

- Mensajes SMS de la víctima
- Detalles de contacto, o grabar sus llamadas
- Registros de llamadas

Activar de forma remota el micrófono y la cámara de un dispositivo para capturar de forma subrepticia audio, video, y contenido de la imagen.

¿Qué es Pegasus?

Pegasus es un spyware que se creó para espiar sistemas operativos (iOS y Android). Pegasus es el principal software espía del grupo NSO.

¿Cómo se descubrió la existencia de Pegasus?

Pegasus fue descubierto en agosto de 2016. Un activista recibió un mensaje sobre la revelación de secretos a través de un enlace en su teléfono. Ante la sospecha, envió el link recibido al citizen lab de la universidad de Toronto, que lo investigó.

El Citizen lab es un laboratorio de investigación multidisciplinario ubicado en la Universidad de Toronto. Se centra en la investigación centrado en el estudio de las amenazas digitales para la sociedad civil y el compromiso político de alto nivel.

¿Quién es NSO?

Se trata de una empresa de ciberseguridad con sede en Israel fundada en 2010. Esta empresa desarrolla y vende software de vigilancia de teléfonos móviles a gobiernos de todo el mundo.

NSO afirma que proporciona el spyware a las agencias autorizadas de los gobiernos de manera legal para combatir el terrorismo y el crimen, pero varias veces se ha descubierto que su spyware se ha utilizado para espiar a activistas humanos, periodistas, etc.

El nombre NSO viene de sus creadores:

- N-Niv Carmi.
- S-Shalev Hulio
- O-Omri Lavie

Funcionamiento de un ataque

El funcionamiento es el de un virus del tipo troyano. Al tener acceso al dispositivo, se conecta remotamente para descargar otros programas, instalarlos, y transmitir información a través de internet sin que el usuario se de cuenta.

En los ataques de un clic, el ataque comienza cuando el atacante envía un URL del sitio web (a través de SMS, correo electrónico, redes sociales o cualquier otro mensaje) a un objetivo identificado.

El usuario solo tiene que hacer clic en el enlace. Entonces, el software ejecuta silenciosamente una serie de exploits contra el dispositivo de la víctima para poder instalar los paquetes de software de espionaje.

El software de espionaje contiene códigos maliciosos, procesos y aplicaciones que se utilizan para espiar, recopilar datos e informar de lo que hace el usuario en el dispositivo.

Fases del ataque

En la primera fase se incluye la parte de la URL que apunta a un archivo HTML. Este archivo explota una vulnerabilidad en webkit.

En una segunda fase se descarga más código en un paquete ofuscado y encriptado. Este contiene el código necesario para explotar el kernel y un loader que descarga y desencripta un paquete para la fase 3.

En esta fase se descarga el software de espionaje, daemons y otros procesos que se usan cuando el dispositivo ha sido jailbreakeado. Se instalan para ello unos hooks en las apps que se quieren espiar.

También comprueba si el dispositivo ha sido jailbreakeado previamente y cancela el acceso.

En esta fase se despliegan una serie de tarballs, cada uno con una finalidad concreta.

Ataques sin interacción del usuario

Las versiones más nuevas han desarrollado capacidades como ataques de clic cero (zero-click).

Estos ataques no requieren ninguna interacción por parte del propietario del teléfono para tener éxito. Explotan las vulnerabilidades de "día cero" en el sistema operativo, que aún no han sido identificadas.

En 2019 Whatsapp reveló que Pegasus había explotado una vulnerabilidad relacionada con hacer una llamada perdida en whatsapp, por ejemplo.

Hacia 2020, Pegasus cambió hacia exploits sin clic y ataques basados en la red. Estos métodos permitieron a los clientes entrar en los teléfonos de destino sin requerir la interacción del usuario y sin dejar rastros

detectables.

En 2022, a partir de una investigación se hace público que varios teléfonos de políticos en España se habrían visto comprometidos por el uso de este software.