SOBRE ESCUCHAS TELEFÓNICAS

colectivo disonancia

SOBRE CÓDIGOS DE VERIFICACIÓN

Las escuchas telefónicas son un procedimiento habitual de vigilancia por parte de empresas y policías. Ante este hecho, suelen compartirse en redes códigos que, supuestamente, permitirían verificar si estamos siendo objeto de alguna escucha.

Esos códigos, de tipo "*#62#" o similares son utilizados para verificar el "desvío de llamadas" que es una función habitual en los teléfonos móviles y que permite la existencia de buzones de voz y los avisos de "fuera de cobertura" o de "dispositivo apagado". La presencia de desvío de llamadas NO corrobora, en ningún sentido, la existencia de escuchas telefónicas.

SOBRE CÓDIGOS DE VERIFICACIÓN

Lo que se puede hacer, luego de ver cuál es el número de desvío de llamada de nuestro dispositivo, es consultar con la compañía si ese número es el que corresponde a este tipo servicio.

Incluso, dependiendo de las funciones que permita la compañía telefónica —y los costos asociados—, podemos configurar nuestros desvíos de llamadas para que se dirijan a personas cercanas en caso de que no podamos contestar o nos encontremos sin señal.

EL PROBLEMA DE FONDO

Las llamadas telefónicas y los SMS no tienen ningún tipo de seguridad porque su protocolo de comunicación no posee cifrado.

Por este motivo, en Chile, ya sea por solicitud a las compañías telefónicas (obligadas a almacenar información de conexión y colaborar por el art. 222 del código procesal penal) o por interceptación directa de la señal telefónica (GPRS y extensiones), permitida por las amplias facultades de la Ley de Inteligencia (19974); este tipo de comunicación es insegura y sencilla de vigilar para policías y empresas, vigilancia que NO necesariamente dejará rastro en el dispositivo.

INFECCIONES A DISPOSITIVOS

Las intervenciones más agresivas a los dispositivos se hacen por medio de programas maliciosos, o malware, que infectan el sistema operativo del teléfono.

El malware Pegasus, de NSO Group, es el más documentado y el 2021 Amnistía Internacional realizó una investigación exhaustiva sobre cómo funciona este programa y publicó una herramienta que ayuda a su detección (cuya guía tradujimos al español).

https://colectivodisonancia.net/pegasus

EL PROBLEMA CON LOS TELÉFONOS MÓVILES

La raíz del problema se encuentra en que los teléfonos móviles son dispositivos inseguros por diseño, primero porque sus sistemas operativos tienen, parcial o completamente, código privativo que es difícil de auditar, volviéndolos un objetivo fácil de atacar. Y segundo porque las redes de telefonía no cuentan con ningún tipo de cifrado por lo que son sencillas de vigilar.

La Electronic Frontier Foundation realizó una lista con los problemas de seguridad propios de los dispositivos móviles a tener en cuenta:

https://ssd.eff.org/es/module/el-problema-con-los-teléfonos-móviles

CONSIDERACIONES BÁSICAS

Una organización que maneja información sensible no debe centrar su estrategia de comunicación en el uso de teléfonos móviles, razón por la cual se deben tener estas consideraciones:

- Usar un teléfono móvil nos mantiene geolocalizados permanentemente por el solo uso de la señal telefónica. La única forma confiable de garantizar no ser localizado es no llevar teléfono o utilizar un bolso de Faraday (este método puede levantar alertas en caso de seguimiento previo).

- No usar llamadas ni SMS como medio de comunicación.

CONSIDERACIONES BÁSICAS

- Si nos comunicamos por chat usando teléfonos, debe ser por medio de aplicaciones confiables y cifradas como Signal o sistemas descentralizados como Matrix (app Element) o XMPP (app Conversations).

Signal

Element

Conversations

CONSIDERACIONES BÁSICAS

- La información que una organización considere como sensible debiese ser tratada en primer lugar de manera presencial; mientras menos intermediarios tecnológicos existan, menos registros.

Si no es posible, se deben usar computadores con Sistemas Operativos (SO) confiables. Un buen tratamiento de la información sensible, si no se quiere migrar todo el SO del computador, es aprender a usar TAILS, un sistema operativo que se instala en una memoria USB, permite navegación anónima y no deja registro en el dispositivo en que se utilizó.

https://tails.boum.org/

AUTONOMÍA TECNOLÓGICA

Mientras exista capitalismo y dependencia tecnológica, la vigilancia permanecerá; y cualquier técnica de autodefensa digital será siempre provisoria y falible. Solo la construcción de autonomía tecnológica permitirá recuperar su sentido emancipador para una sociedad libre y comunitaria.

colectivodisonancia.net/redes-baja-tecnologia

colectivo disonancia