Stealth Phones

El significado de seguridad.

"¿Qué teléfono móvil puedo utilizar para protegerme de diversos ataques?" Para responder a esta pregunta, es esencial saber de quién hay que protegerse. ¿Busca protección frente a miradas indiscretas, por ejemplo, de un socio comercial, piratas informáticos o instituciones profesionales como empresas de espionaje, compañías sin escrúpulos o gobiernos abusivos? Evaluar la respuesta y analizar los distintos "teléfonos móviles seguros" lleva mucho tiempo y debe ser realizado por expertos con experiencia.

Los vendedores y desarrolladores de "teléfonos móviles seguros" se aprovechan de la falta de comprensión de este complejo asunto por parte del usuario final sugiriendo seguridad sin mencionar a qué se aplica su protección. **Los usuarios finales corren el riesgo de utilizar un "teléfono móvil seguro" que no cumple en absoluto los requisitos necesarios.**

La vigilancia de las telecomunicaciones se está convirtiendo en un problema cada vez mayor.

"¿Cuál es la intención detrás de la interceptación de las telecomunicaciones individuales?" Las escuchas telefónicas y la vigilancia de los ciudadanos es un asunto extremadamente grave. La posibilidad de invadir la intimidad es un poder enorme que puede utilizarse para vigilar, abochornar, controlar, avergonzar o incluso arruinar a una persona. El derecho a la intimidad nos protege de la persecución por nuestras creencias, nuestra religión o nuestro estilo de vida. Como la tecnología de interceptación es tan crucial, ha estado sujeta a controles legales y cuidadosamente elaborados casi desde su invención. No hacer caso de estos controles y realizar escuchas telefónicas sin orden judicial es un delito penal en todos los países, castigado con importantes penas de prisión. Pero todo esto se ignora y la interceptación de ciudadanos sin orden judicial se ha convertido en algo cotidiano incluso en los países democráticos. En la actualidad ya no es posible distinguir entre vigilancia legal e ilegal, pues cada vez son más las entidades privadas que tienen acceso a sistemas de vigilancia y escuchas telefónicas, y basta un momento de corrupción para utilizar la información obtenida en beneficio propio. Se está invadiendo nuestra intimidad sin que nos demos cuenta.

> Un "teléfono móvil seguro" debe proteger al usuario en cualquier circunstancia, tratar todas las amenazas por igual y no distinguir entre vigilancia legal e ilegal de las telecomunicaciones.

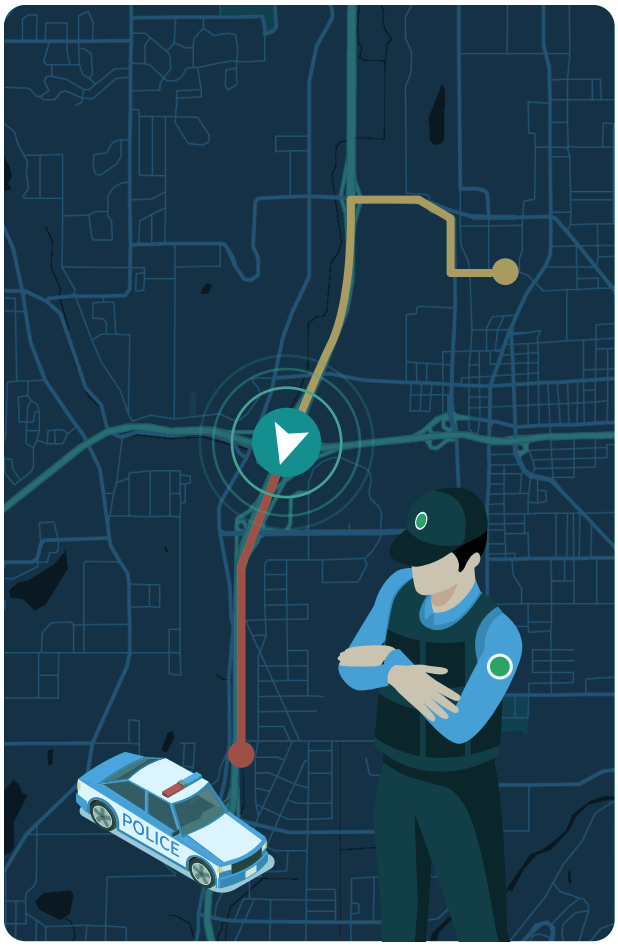
"Diferencia de tecnología" No hay diferencia tecnológica entre la interceptación legal y la ilegal. La interceptación legal debe ser autorizada por un funcionario para que los resultados sean admisibles ante un tribunal. Las medidas ilegales utilizan las mismas tecnologías de vigilancia e interceptación, pero sin autorización ni control de una autoridad superior, ya que los resultados no se recogen para su uso oficial ante los tribunales. **Los resultados obtenidos ilegalmente sirven de base para autorizar la vigilancia legal, cuyos resultados recién obtenidos son válidos ante los tribunales.**

"La identidad del objetivo coincide con la identidad del teléfono móvil" Cualquier teléfono móvil es en realidad un dispositivo de rastreo que puede utilizarse para hacer llamadas, enviar mensajes y utilizar Internet. Un teléfono móvil se identifica ante la red con dos números de serie de 15 dígitos, mediante los cuales un teléfono móvil puede identificarse de forma inequívoca en todo el mundo.

El IMEI
Número único de registro del teléfono.

El IMSI
Número único de registro de la SIM.

En cuanto se enciende el teléfono, **se conecta automáticamente a la torre celular con la señal más fuerte**, ¡incluso sin tarjeta SIM insertada! Independientemente de la marca, el sistema operativo, el precio o la tecnología de red (2G, 3G, 4G o 5G). Este proceso se repite periódicamente. Así se evita que un teléfono móvil se desconecte accidentalmente de la red. Sin embargo, esta función básica de establecer una conexión también sirve para otro propósito: la localización de un teléfono objetivo. El establecimiento de una conexión puede ser objeto de abuso por parte de entidades privadas y estatales para determinar la ubicación del usuario del teléfono en un momento dado. Los operadores de telefonía móvil almacenan cada conexión en función de la identidad del teléfono móvil y la identidad de la torre de telefonía móvil. Retrospectivamente, estos conjuntos de datos pueden ser solicitados por las autoridades o descargados directamente de la torre de telefonía móvil, como ocurre en Estados Unidos (el llamado procedimiento de volcado de la torre). Como este proceso se repite con regularidad, la ubicación de las torres de telefonía móvil puede utilizarse para crear un perfil casi completo de los movimientos de un usuario.



Retrospectivamente, sólo se registran los detalles de la conexión, como fecha, hora, duración, dirección, números de teléfono, IMEI e IMSI y ubicaciones de todos los teléfonos móviles implicados. No es posible analizar el contenido de las llamadas de voz, los SMS y los datos a posteriori sin una orden judicial previa. El contenido de la comunicación se evalúa en tiempo real o, si hay una orden de interceptación activa, se analizará durante el proceso de seguimiento (de 1 día a 6 meses). Esto puede hacerse a nivel directo de la red básica móvil explotando las vulnerabilidades SS7 conocidas, o con la ayuda de sistemas móviles de vigilancia e interceptación diseñados explícitamente para la interceptación de telecomunicaciones.

> Un "teléfono seguro" tiene que poder cambiar su identidad modificando su IMEI e IMSI, y debe tener funciones para detectar intentos de interceptación. Confiar únicamente en el cifrado de un teléfono no es garantía de seguridad frente a métodos de interceptación profesionales.

Los celulares que sólo se basan en la encriptación no tienen protección contra la interceptación de llamadas/SMS, la monitorización y el rastreo de localización realizados por hackers que utilizan equipos de laboratorio como una femtocelda modificada, dispositivos SDR, simuladores de sitios, dispositivos de prueba de redes y dispositivos tipo USRP. Un hacker inexperto sólo puede husmear la interfaz aérea, recopilando en el aire algunos datos como IMEI, IMSI, números de teléfono, ubicación relativa y, a veces, contenido de texto SMS, pero no puede interceptar una llamada telefónica. Los hackers expertos con el hardware adecuado pueden hacer lo mismo que las fuerzas de seguridad: interceptar llamadas telefónicas, SMS, tráfico de datos (incluidas credenciales de cuentas, contenido de chat, contenido de mensajería, etc.) y seguimiento de la ubicación con una precisión de hasta +/-3 metros.

Un Criptófono no es tan seguro como usted piensa. Un operador de telefonía móvil o la institución que opera un interceptor GSM puede averiguar información importante como: Contactos, ubicaciones exactas y comportamiento de comunicación sobre el usuario. La información enumerada puede (y será) utilizada para averiguar en última instancia sus secretos, que luego se utilizarán como pruebas contra usted ante un tribunal.

Detección de escuchas como Ventaja de seguridad

A menudo equiparamos la seguridad móvil con la seguridad física. Una empresa contrata a un guardia de seguridad y lo coloca en la puerta de entrada de su edificio. El vigilante de seguridad permanece en su puesto. Controla los documentos de identidad y garantiza la seguridad en la entrada. Como está en la puerta principal, no puede vigilar todas las zonas de la empresa. Si alguien salta la valla y entra, no puede ver que existe un riesgo para la seguridad.

Lo mismo ocurre con el uso de una solución de cifrado (software o hardware): Nunca sabrás cuándo te están pinchando el móvil. **Por tanto, nunca sabrás cuándo estás realmente en peligro.** Además, cualquiera (incluso un niño o un ciudadano medio) en posesión de un inhibidor sencillo y barato puede inutilizar a distancia cualquier teléfono móvil seguro interfiriendo el canal de bajada o, como hacen las fuerzas de seguridad, interfiriendo sólo el canal de datos. Esto obliga al usuario del teléfono a utilizar su teléfono seguro como un teléfono móvil normal, haciendo y recibiendo llamadas normales y enviando y recibiendo mensajes de texto normales, que pueden ser fácilmente interceptados en estas circunstancias.

> Un "teléfono móvil seguro" tiene que detectar los intentos de interceptación de llamadas/SMS y alertar al usuario en tiempo real. Sólo recibiendo una alerta en tiempo real es posible que el usuario garantice la seguridad de su vida y adapte su comportamiento a las nuevas amenazas.

Stealth Phones para la seguridad móvil, no hay sustituto. El resto del mercado sigue el camino del cifrado de texto y voz, que sólo da al usuario una falsa sensación de seguridad. Los XCell Stealth Phones van directamente al corazón del problema explotando las mismas vulnerabilidades de la red responsables de la identificación del usuario, la localización y la interceptación de voz y datos.

"Detección de escuchas telefónicas" Los Stealth Phones son capaces de detectar todo tipo de escuchas telefónicas de llamadas, SMS y datos y avisar al usuario en tiempo real:

- ✓ IMSI Catcher.
- ✓ Interceptores GSM activos.
- ✓ Interceptores GSM semiactivos.
- ✓ Interceptores GSM pasivos.
- ✓ SS7 (con la ayuda del operador de red, también llamada interceptación legal).

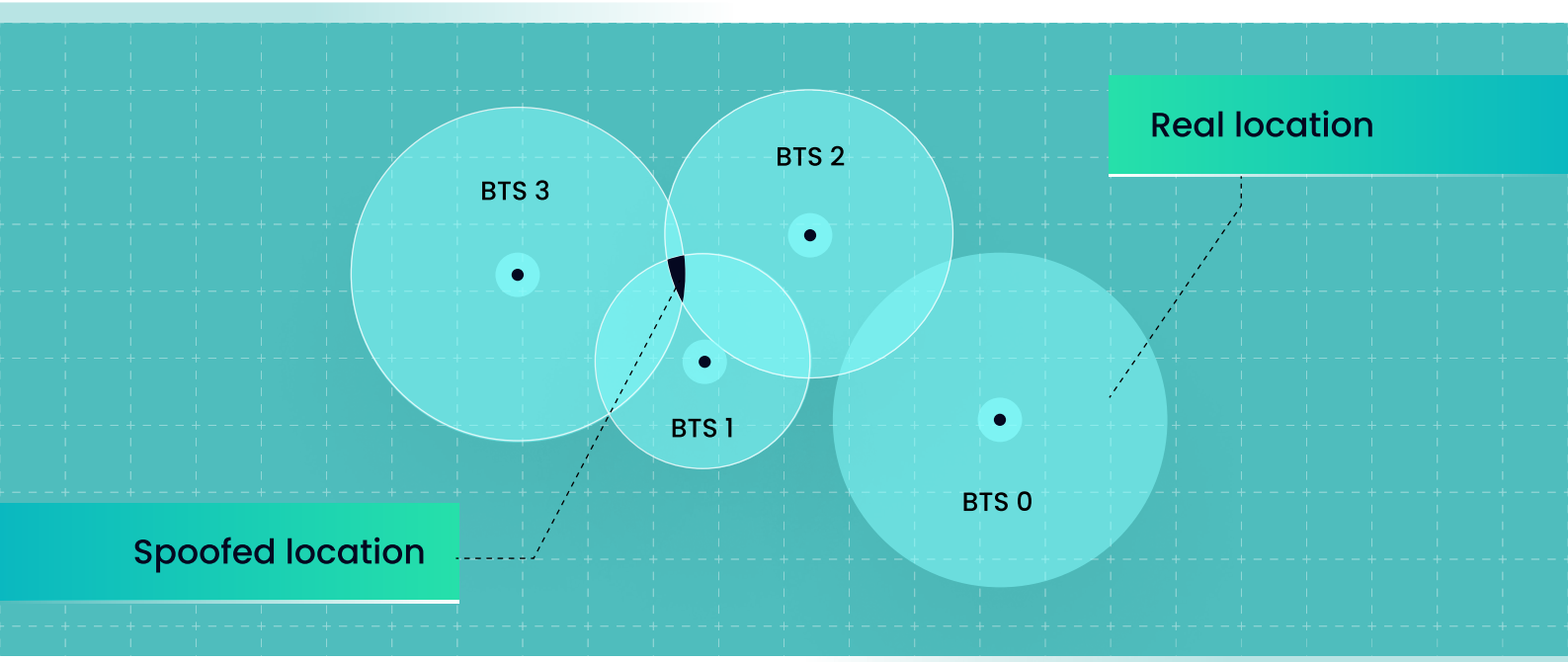
Stealth Phones también detecta cuando el otro teléfono móvil implicado en la llamada está siendo intervenido.

"Identificación del usuario" Algunos Stealth Phones están equipados con una función de cambio automático de IMEI e IMSI que convierte su teléfono móvil en un arma inteligente de contrainteligencia. Cambiar el IMEI y el IMSI al mismo tiempo impide controlar la ubicación, las llamadas, los SMS y los datos. El hecho de que se hayan cambiado todos sus identificadores telefónicos (previamente registrados en la lista de selección de objetivos de un interceptor GSM o de un operador de telefonía móvil) significa que el operador ya no sabe quién debe ser vigilado. El organismo de control debe hacer esfuerzos adicionales para obtener y registrar sus nuevos identificadores telefónicos.

Si la IMSI no se cambia localmente en el teléfono (como ocurre sólo con los XCell Stealth Phones), sin utilizar una conexión a Internet y sin el apoyo de servidores que el usuario no puede comprobar y en los que no puede confiar, sino a través de una conexión a Internet a través del fabricante de la SIM, como hacen algunas empresas rusas y polacas, esto no resuelve el problema, ya que un IMSI catcher o un interceptor GSM con capacidad de interferencia puede simplemente desactivar esas tarjetas SIM que cambian la IMSI. Hoy en día, esta es una práctica común entre los operadores de interceptores GSM.

Nota: Si solo ha cambiado el IMSI (tarjeta SIM) o solo el IMEI, no obtendrá ningún valor añadido y sus llamadas seguirán siendo interceptadas como si no hubiera cambiado nada, ya que se puede detectar una correlación entre el valor del IMEI y del IMSI sin cambios y con cambios.

"Localización" Algunos Stealth Phones están equipados con una función de "suplantación de ubicación real". Se trata de una auténtica manipulación de emplazamientos GSM basada en la manipulación de torres de telefonía móvil y proporciona un resultado de triangulación falso. Todos los sistemas de posicionamiento utilizan la triangulación GSM. El seguimiento por GPS no se ve afectado por esto. Esto se debe a que todos los teléfonos móviles deben ser rastreados, incluso los que no tienen función GPS, los llamados teléfonos tontos. Algunos "teléfonos móviles seguros" sólo ofrecen una solución para la localización GPS a través de una conexión de datos, que no es más que una falsificación del GPS a través de una aplicación instalada en el teléfono (VPN) que crea una localización GPS falsa visible para el usuario del teléfono y otras aplicaciones instaladas, utilizada principalmente con fines de broma y entretenimiento. La falsificación de GPS no es adecuada para el seguimiento profesional de ubicaciones. Una vez determinada la ubicación GSM, el sistema de seguimiento puede calcular fácilmente una posición GPS. Un sistema de rastreo nunca puede leer directamente los datos GPS del teléfono móvil. Esto sólo puede hacerse con la ayuda del llamado software espía, que debe instalarse en el teléfono objetivo. El usuario de un Stealth Phones puede elegir a qué torro de telefonía móvil se conecta el teléfonoDe este modo, cualquier técnica de triangulación utilizada para determinar la ubicación dará resultados incorrectos y, por tanto, una ubicación incorrecta. Dado que un teléfono envía el ID de la célula a la que está conectado, los datos de conexión manipulados también son almacenados por el operador de telefonía móvil. La distancia entre la ubicación real del usuario y la ubicación de la torre móvil conectada oscila entre 1 y 10 km. Si estos conjuntos de datos son solicitados posteriormente por las autoridades, todos los datos de localización conducirán a resultados falsos y, por tanto, a un perfil de movimiento inútil. Lo mismo ocurre si el seguimiento de la ubicación se realiza en tiempo real mediante un interceptor GSM.



Los XCell Stealth Phones incorporan tecnologías patentadas y un nivel de seguridad que actualmente no tiene parangón en ningún otro teléfono móvil.

Para garantizar la seguridad de sus comunicaciones, XCell Stealth Phones le ofrece la mayor protección posible contra los riesgos de las escuchas y el rastreo de teléfonos móviles. Los Stealth Phones protegen las conversaciones de la vigilancia de operadores móviles, empresas de espionaje, hackers expertos y gobiernos abusivos, y garantizan que sus llamadas, SMS y datos sigan siendo 100% confidenciales y no puedan ser interceptados por terceros o IMSI catchers.

Los Stealth Phones son la elección perfecta para cualquiera que reconozca la necesidad de una comunicación completamente segura.

Contacto

Si está interesado en nuestras soluciones y demostraciones, no dude en concertar una cita con nosotros. Estaremos encantados de conocer mejor sus próximos retos y de presentarle nuestras soluciones en detalle, en la situación actual también en una sesión en línea.

+41 76 452 99 93

info@anti-interception.com

www.anti-interception.com

ECN GmbH
Ettenhauserstrasse 50
8620 Wetzikon ZH, Suiza