Imprecisiones técnicas de la Operación Huracán

Autor: Paulo Colomés (pcolomes@nis.cl)

Agosto 2018

QUIEN HABLA

Nombre: Paulo Colomés
Profesión: Ingeniero Informático de la Universidad Católica de Temuco
Especialización: Redes de comunicaciones y seguridad TI
Experiencia: +15 años en el área técnica y docencia universitaria
Contacto: pcolomes@nis.cl

CONTENIDO DE LA PRESENTACIÓN

- Breve análisis técnico de la aplicación Antorcha
- Breve análisis técnico de la aplicación Tubicación
- ¿Es posible interceptar Whatsapp y otras aplicaciones de mensajería?
- Conclusiones

CONTEXTO GENERAL

La Unidad de Inteligencia Operativa Especial (U.I.O.E.) de Carabineros, con sede en Temuco aseguraba que, mediante algunas aplicaciones informáticas desarrolladas en esa unidad, era posible lograr la **intervención** de aplicaciones de mensajería instantánea (Whatsapp y Telegram) de terceras personas mediante algunas técnicas de infiltración, principalmente de teléfonos celulares para interceptar comunicaciones.

CONTEXTO GENERAL

La Unidad de Inteligencia Operativa Especial (U.I.O.E.) de Carabineros, con sede en Temuco aseguraba que, mediante algunas aplicaciones informáticas desarrolladas en esa unidad, era posible lograr la **intervención** de aplicaciones de mensajería instantánea (Whatsapp y Telegram) de terceras personas mediante algunas técnicas de infiltración, principalmente de teléfonos celulares para interceptar comunicaciones.

Whatsapp

Telegram

iPhone

Android

GMail

Facebook

Twitter

CONTEXTO GENERAL

La Unidad de Inteligencia Operativa Especial (U.I.O.E.) de Carabineros, con sede en Temuco aseguraba que, mediante algunas aplicaciones informáticas desarrolladas en esa unidad, era posible lograr la intervención de aplicaciones de mensajería instantánea (Whatsapp y Telegram) de terceras personas mediante algunas técnicas de infiltración, principalmente de teléfonos celulares.

Esta infiltración se habría logrado principalmente utilizando, de acuerdo a lo indicado por Carabineros, el denominado software ”**Antorcha**” creado por el Sr. Alex Smith Leay en su rol de asesor experto de la unidad en Temuco. No obstante, se ha determinado que tanto Antorcha como una segunda aplicación denominada “Tubicación” nunca habrían existido (Peritaje de la PDI, Mayo 2018)

CONTEXTO GENERAL

La Unidad de Inteligencia Operativa Especial (U.I.O.E.) de Carabineros, con sede en Temuco aseguraba que, mediante algunas aplicaciones informáticas desarrolladas en esa unidad, era posible lograr la intervención de aplicaciones de mensajería instantánea (Whatsapp y Telegram) de terceras personas mediante algunas técnicas de infiltración, principalmente de teléfonos celulares.

Esta infiltración se habría logrado principalmente utilizando, de acuerdo a lo indicado por Carabineros, el denominado software ”**Antorcha**” creado por el Sr. Alex Smith Leay en su rol de asesor experto de la unidad en Temuco. No obstante, se ha determinado que tanto Antorcha como una segunda aplicación denominada “Tubicación” nunca habrían existido (Peritaje de la PDI, Mayo 2018)

En esta sesión se analizarán algunos aspectos técnicos de esas aplicaciones con la finalidad de informar al respecto a la comisión investigadora de la Operación Huracán conformada por integrantes de la Cámara de Diputados de Chile y lograr esclarecer las dudas operativas de estas aplicaciones desde un punto de vista funcional y técnico.

LA APLICACIÓN ANTORCHA

Estos son algunas explicaciones extraídas de diferentes medios y emitidas por el propio Alex Smith que hacen referencia al funcionamiento de Antorcha:

LA APLICACIÓN ANTORCHA

Estos son algunas explicaciones extraídas de diferentes medios y emitidas por el propio Alex Smith que hacen referencia al funcionamiento de Antorcha:

- Antorcha consiste en la creación de un espejo del teléfono

LA APLICACIÓN ANTORCHA

Estos son algunas explicaciones extraídas de diferentes medios y emitidas por el propio Alex Smith que hacen referencia al funcionamiento de Antorcha:

- Antorcha consiste en la creación de un espejo del teléfono
- La aplicación se abría en el computador y debían ingresarse datos como correo electrónico, IMEI, Simcard

LA APLICACIÓN ANTORCHA

Estos son algunas explicaciones extraídas de diferentes medios y emitidas por el propio Alex Smith que hacen referencia al funcionamiento de Antorcha:

- Antorcha consiste en la creación de un espejo del teléfono
- La aplicación se abría en el computador y debían ingresarse datos como correo electrónico, IMEI, Simcard
- El servidor de la UIOE enviaba un correo electrónico al teléfono que se quería intervenir. El correo “contaminaba” el teléfono.

LA APLICACIÓN ANTORCHA

Estos son algunas explicaciones extraídas de diferentes medios y emitidas por el propio Alex Smith que hacen referencia al funcionamiento de Antorcha:

- Antorcha consiste en la creación de un espejo del teléfono
- La aplicación se abría en el computador y debían ingresarse datos como correo electrónico, IMEI, Simcard
- El servidor de la UIOE enviaba un correo electrónico al teléfono que se quería intervenir. El correo "contaminaba" el teléfono.
- Bastaba que el correo llegue al teléfono para infectar el aparato. Los correos estaban diseñados para pasar la barrera de spam.

LA APLICACIÓN ANTORCHA

Estos son algunas explicaciones extraídas de diferentes medios y emitidas por el propio Alex Smith que hacen referencia al funcionamiento de Antorcha:

- Antorcha consiste en la creación de un espejo del teléfono
- La aplicación se abría en el computador y debían ingresarse datos como correo electrónico, IMEI, Simcard
- El servidor de la UIOE enviaba un correo electrónico al teléfono que se quería intervenir. El correo "contaminaba" el teléfono.
- Bastaba que el correo llegue al teléfono para infectar el aparato. Los correos estaban diseñados para pasar la barrera de spam.
- No era necesario que el usuario abriera el correo electrónico que se le había enviado. Solo bastaba con que ingresara a la bandeja y luego el usuario utilizara aplicaciones como Whatsapp y Telegram. Esa información se podía observar en otro aparato.

LA APLICACIÓN ANTORCHA

Algunos alcances adicionales respecto al funcionamiento de Antorcha:

- La UIOE compró múltiples dominios y hosting para sitios web (AIRS.CL y TUBICACION.CL, entre otros) la información contenida en ellos eran solo plantillas, pero nada funcional.
- En numerosas ocasiones Alex Smith cambió la versión sobre el funcionamiento de Antorcha.
- En numerosas ocasiones se intentó validar (incluso en TV) el funcionamiento de Antorcha sin resultados concretos.
- Nunca se ha explicado en lenguaje técnico cómo podría funcionar Antorcha realmente. Solo se han dado explicaciones sin sustento.
- Jamás se ha logrado explicar el detalle técnico profundo de **cómo** esta aplicación lograría infectar un teléfono (iPhone, Android) enviando solo un correo.
- No existe una explicación detallada del supuesto método utilizado para capturar estas conversaciones de mensajería que permita siquiera reproducirla en un ambiente de pruebas.
- Alex Smith nunca permitió que su aplicación fuera analizada por expertos en un entorno controlado.
- Alex Smith quiso viajar a EE.UU. para que el FBI analizara su aplicación, siendo que eso no es necesario.
- Los peritajes de la PDI ya establecieron la falsedad de esta aplicación.

LA APLICACIÓN ANTORCHA

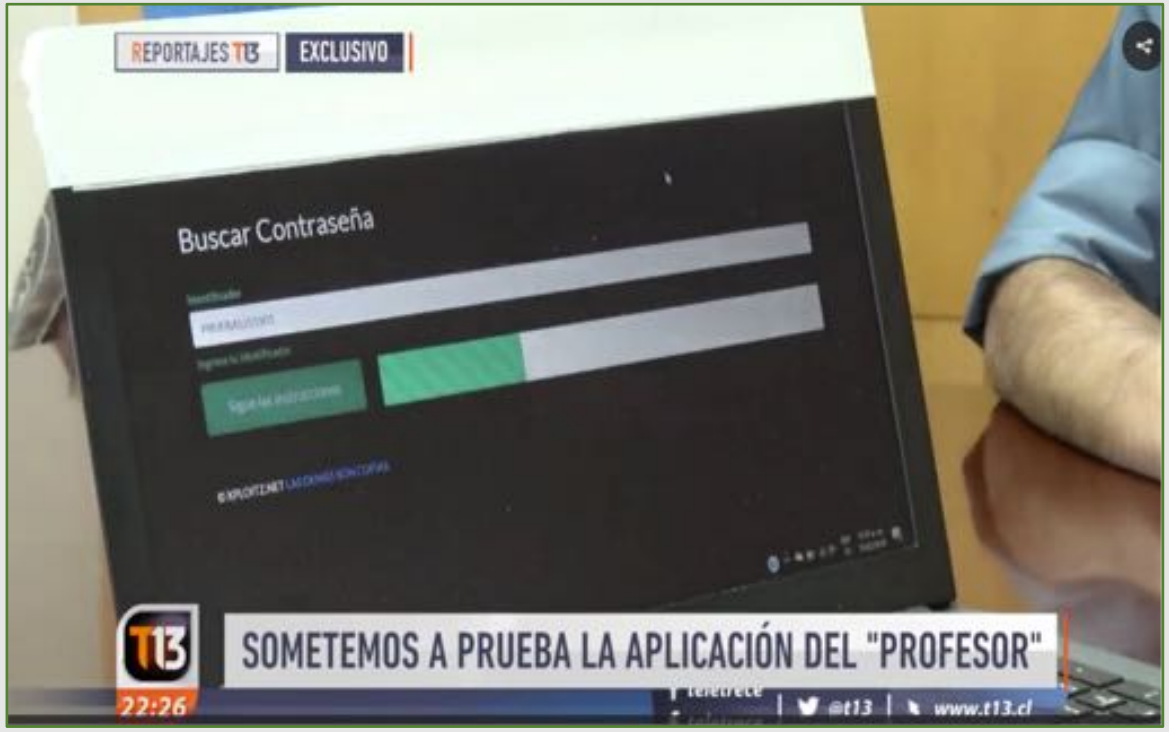
El show de TV

El día 11 de Febrero de 2018 se presentó por Canal 13 (*) un reportaje donde se muestra a Alex Smith realizando una demostración de la supuesta efectividad de Antorcha. Gran parte de la población se convenció de que esta aplicación era real y funcionaba. Sin embargo, al analizar detenidamente esta emisión es posible determinar que eso jamás ocurrió.

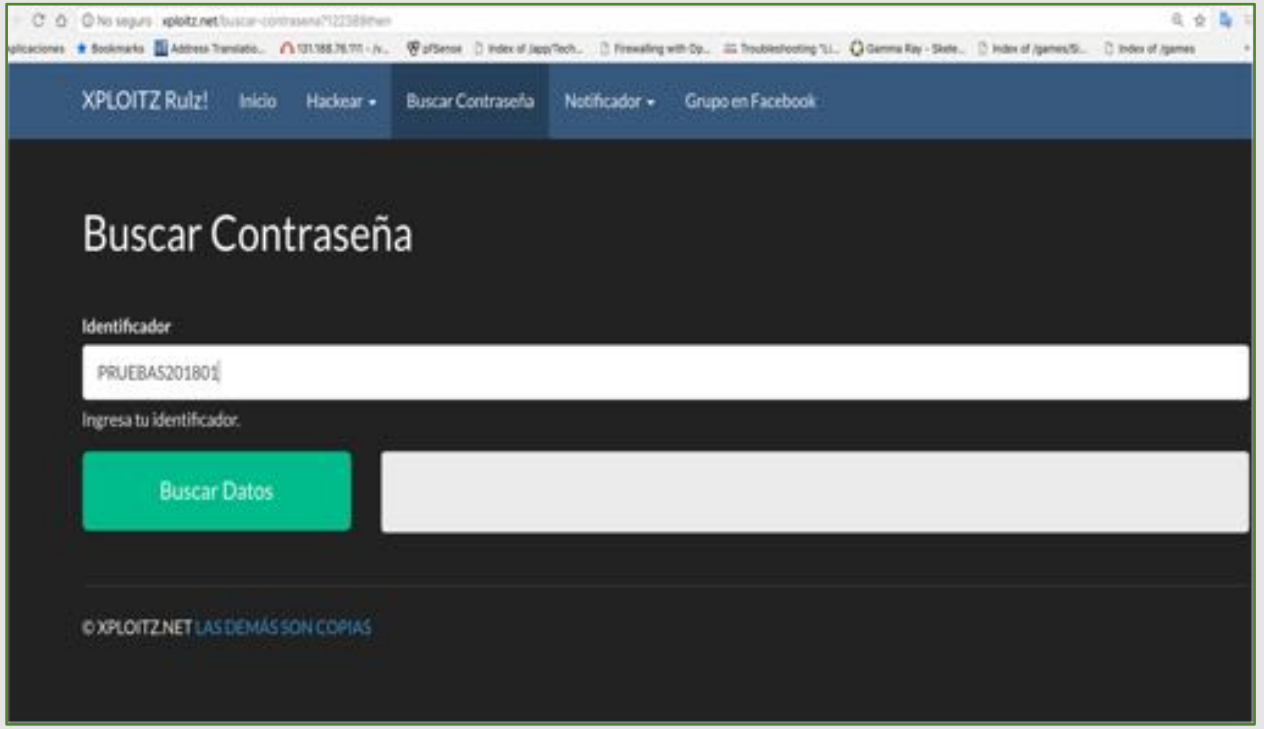
(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV



ANTORCHA



SITIO REAL: XPLOITZ.NET

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

Esto es XPLOITZ.NET. Un sitio que tiene diseños predefinidos de sitios populares (Facebook, Gmail, etc.) que sirven para ser enviados a usuarios que eventualmente ingresarán sus credenciales y ejecutar ataques de "phishing". Lo que hace Alex Smith es usar esta página Web para enviarle un simple phishing al periodista para ingresar a su correo Gmail. (solo funciona si el correo usa una página Web para ingresar)

El periodista escribe un mensaje en Whatsapp a una colega

Periodista: - "Hola Magaly.. ¿Podrías describir tu vestimenta?"
Colega:- "Polera gris, pantalón jeans. Cinturón café.
Periodista: - "El nombre de pila del camarógrafo que está contigo"
Colega: - "Guillermo"

El resultado fue que en el transcurso de la entrevista jamás se obtuvo esta conversación.

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

En la misma instancia, esa misma noche, Alex Smith indica que “le hackearon” su sistema. Una explicación conveniente.

Al día siguiente se realizaron nuevas pruebas pero nunca apareción la conversación anterior. Solo se menciona que se se obtuvieron las **fotografías** enviadas por Whatsapp en el celular del periodista.

EXPLICACIÓN: El sistema operativo Android tiene la opción de realizar un respaldo diario de todos los chats y fotos de Whatsapp y almacenarlos automáticamente en la nube de Google (Google Drive). Esta nube puede ser accedida desde la cuenta GMAIL del usuario. Basta tener el usuario y contraseña de GMAIL para poder acceder a esa información.

IMPORTANTE: Las fotos de Whatsapp se guardan **SIN CIFRAR** en la nube. Las conversaciones (chats), en cambio, requieren de un avanzado sistema criptográfico para ser accedidas y NO pueden ser vistas solamente desde el respaldo GMAIL. Una demostración: https://www.youtube.com/watch?v=yrd-H9LWj94&t=14 (Duración: 35 minutos)

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

Conclusión del funcionamiento de la aplicación Antorcha en el reportaje de C13:

- Jamás se obtuvo la conversación inicial

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

Conclusión del funcionamiento de la aplicación Antorcha en el reportaje de C13:

- Jamás se obtuvo la conversación inicial
- Se explicó que existía un “virus” “incubando” en el sistema operativo pero nunca se dio detalles técnicos de ello.

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

Conclusión del funcionamiento de la aplicación Antorcha en el reportaje de C13:

- Jamás se obtuvo la conversación inicial
- Se explicó que existía un “virus” “incubando” en el sistema operativo pero nunca se dio detalles técnicos de ello.
- Se utilizaron explicaciones superficiales para describir el no-funcionamiento (hackeos inexistentes y antivirus)

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

Conclusión del funcionamiento de la aplicación Antorcha en el reportaje de C13:

- Jamás se obtuvo la conversación inicial
- Se explicó que existía un “virus” “incubando” en el sistema operativo pero nunca se dio detalles técnicos de ello.
- Se utilizaron explicaciones superficiales para describir el no-funcionamiento (hackeos inexistentes y antivirus)
- Nunca se mostró como realizar este procedimiento en un teléfono iPhone (solo en un Android)

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

Conclusión del funcionamiento de la aplicación Antorcha en el reportaje de C13:

- Jamás se obtuvo la conversación inicial
- Se explicó que existía un “virus” “incubando” en el sistema operativo pero nunca se dio detalles técnicos de ello.
- Se utilizaron explicaciones superficiales para describir el no-funcionamiento (hackeos inexistentes y antivirus)
- Nunca se mostró como realizar este procedimiento en un teléfono iPhone (solo en un Android)
- Nunca se mostró como realizar este procedimiento en la aplicación Telegram

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

Conclusión del funcionamiento de la aplicación Antorcha en el reportaje de C13:

- Jamás se obtuvo la conversación inicial
- Se explicó que existía un “virus” “incubando” en el sistema operativo pero nunca se dio detalles técnicos de ello.
- Se utilizaron explicaciones superficiales para describir el no-funcionamiento (hackeos inexistentes y antivirus)
- Nunca se mostró como realizar este procedimiento en un teléfono iPhone (solo en un Android)
- Nunca se mostró como realizar este procedimiento en la aplicación Telegram
- La segunda vez que se realizó la prueba se encontraba la ex-abogada de Alex Smith (Marisa Navarrete) pero no hubo en ningún caso un experto técnico que pueda validar la efectividad de los procedimientos.

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN ANTORCHA

El show de TV

Conclusión del funcionamiento de la aplicación Antorcha en el reportaje de C13:

- Jamás se obtuvo la conversación inicial
- Se explicó que existía un “virus” “incubando” en el sistema operativo pero nunca se dio detalles técnicos de ello.
- Se utilizaron explicaciones superficiales para describir el no-funcionamiento (hackeos inexistentes y antivirus)
- Nunca se mostró como realizar este procedimiento en un teléfono iPhone (solo en un Android)
- Nunca se mostró como realizar este procedimiento en la aplicación Telegram
- La segunda vez que se realizó la prueba se encontraba la ex-abogada de Alex Smith (Marisa Navarrete) pero no hubo en ningún caso un experto técnico que pueda validar la efectividad de los procedimientos.

En definitiva: La aplicación Antorcha es un fraude. No existe.

(*) http://www.t13.cl/videos/nacional/video-operacion-huracan-creador-antorcha-explica-como-funciona (minuto 6 en adelante)

LA APLICACIÓN TUBICACIÓN

La otra aplicación utilizada por Carabineros ha sido denominada “**tubicación**” y consistiría en georreferenciar teléfonos celulares a partir de la señal WiFi emitida por los routers inalámbricos.

LA APLICACIÓN TUBICACIÓN

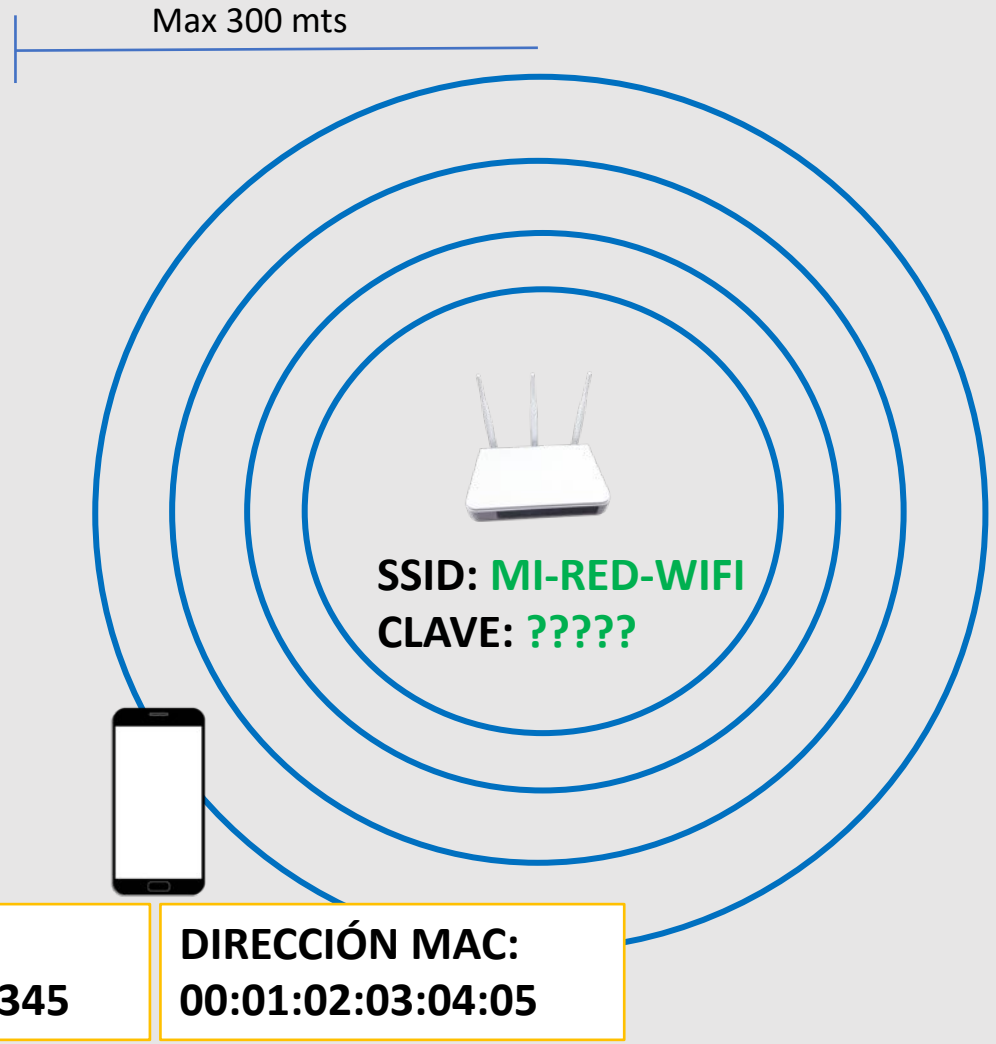
La otra aplicación utilizada por Carabineros ha sido denominada "**tubicación**" y consistiría en georreferenciar teléfonos celulares a partir de la señal WiFi emitida por los routers inalámbricos.

Esta aplicación se habría utilizado para identificar a los supuestos responsables en el atentado ocurrido a la empresa Sotraser en agosto de 2017 donde se destruyeron 29 camiones en San José de la Mariquina, Región de Los Ríos. (Operación Huracán II)

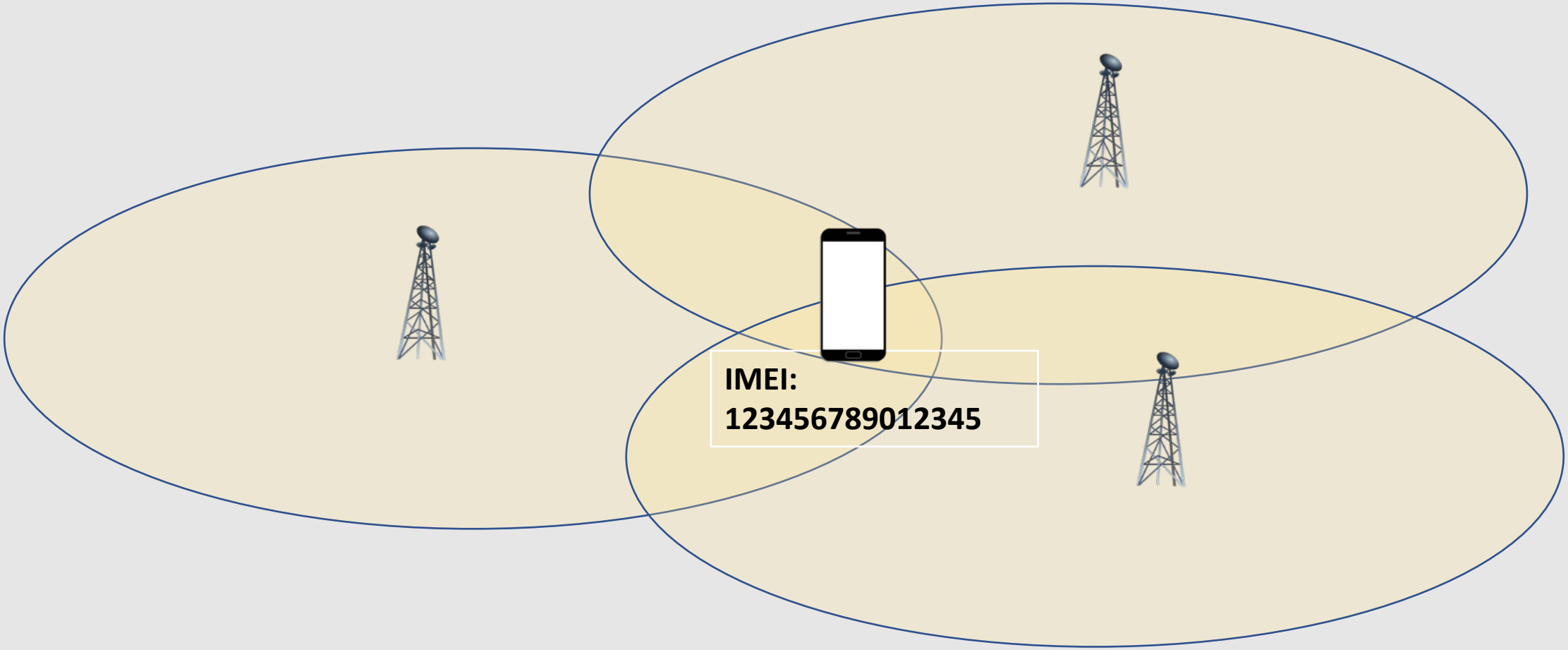
LA APLICACIÓN TUBICACIÓN ES UN FRAUDE

NO es posible determinar el número de teléfono ni la ubicación fisica de un dispositivo móvil con el solo hecho de acercarse a una red WiFi.

Para conocer el número de teléfono se debe extraer información de la red 3G/4G lo cual no es compatible con WiFi.



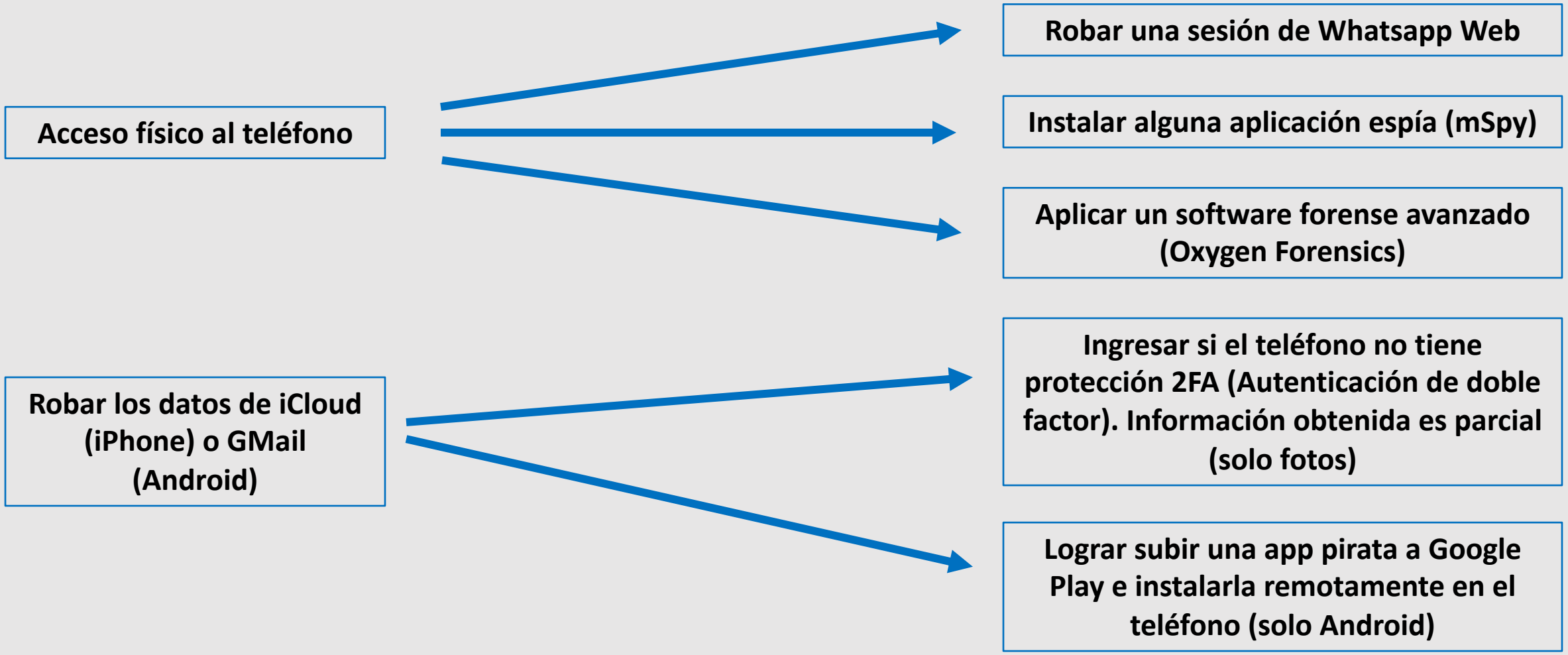
¿Cómo SI se pueden georreferenciar celulares?



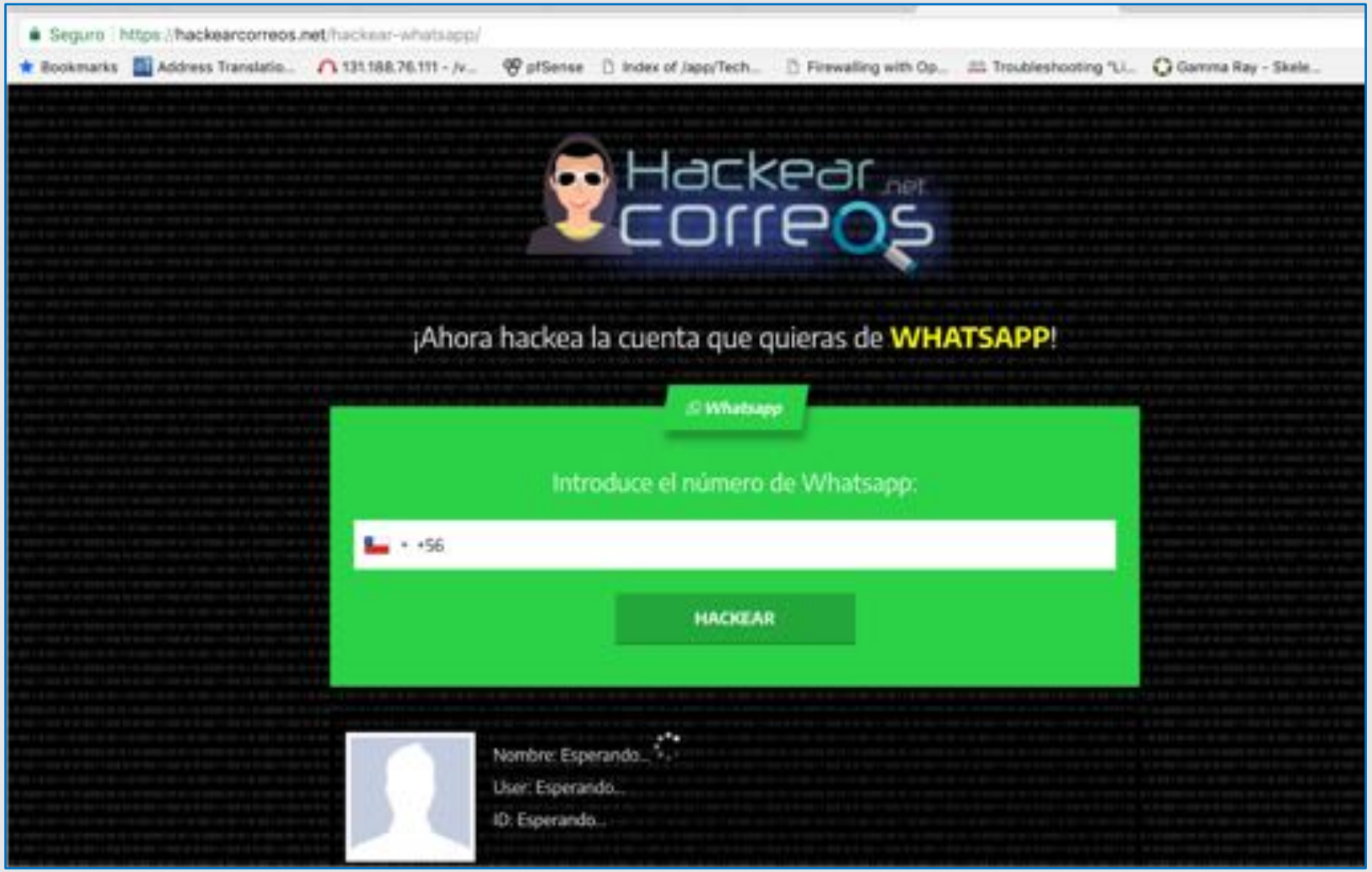
Ubicación aproximada: radio de 500 mts a 4 – 5kms

¿ES POSIBLE ”HACKEAR” WHATSAPP?

Claro que sí. Pero bajo ciertas condiciones:



MI PROPIO ANTORCHA 2.0



https://hackearcorreos.net/hackear-whatsapp/

CONCLUSIONES DEL CASO

- **La aplicación Antorcha no existe. En el mejor de los casos podría tratarse de un simple procedimiento que cualquier persona podría realizar. No garantiza efectividad.**

- **La aplicación Tubicación no solo no existe sino que su supuesto funcionamiento es un fraude.**

- **Queda ampliamente demostrado y documentado que las aplicaciones informáticas que dieron sustento a la Operación Huracán carecen de los mínimos requerimientos técnicos para ser consideradas incluso como "posiblemente factible".**

- **Es posible (no concluyente) que toda la información divulgada por Alex Smith en relación a los resultados de esas aplicaciones haya provenido de otra fuentes (escuchas telefónicas, intervenciones de correos electrónicos, etc)**

CONCLUSIONES DEL CASO

- **Los países industrializados invierten una buena parte de sus recursos en formar verdaderos ejércitos de hackers para defender la soberanía o proteger/atacar objetivos de interés nacional (internos, externos)**

- **Las policías de esos países cuentan con grupos de especialistas en seguridad quienes pueden obtener información legítima (no falsa) de sistemas existentes utilizando sus conocimientos y esas evidencias resisten cualquier peritaje forense.**

- **Si Carabineros hubiese recurrido a constuir un grupo de élite (en Chile hay personas capaces) que esté detrás de la inteligencia informática, los resultados de la Operación Huracán probablemente hubiesen sido muy diferentes y los verdaderos responsables ya estarían procesados por la justicia.**

MUCHAS GRACIAS POR SU ATENCIÓN