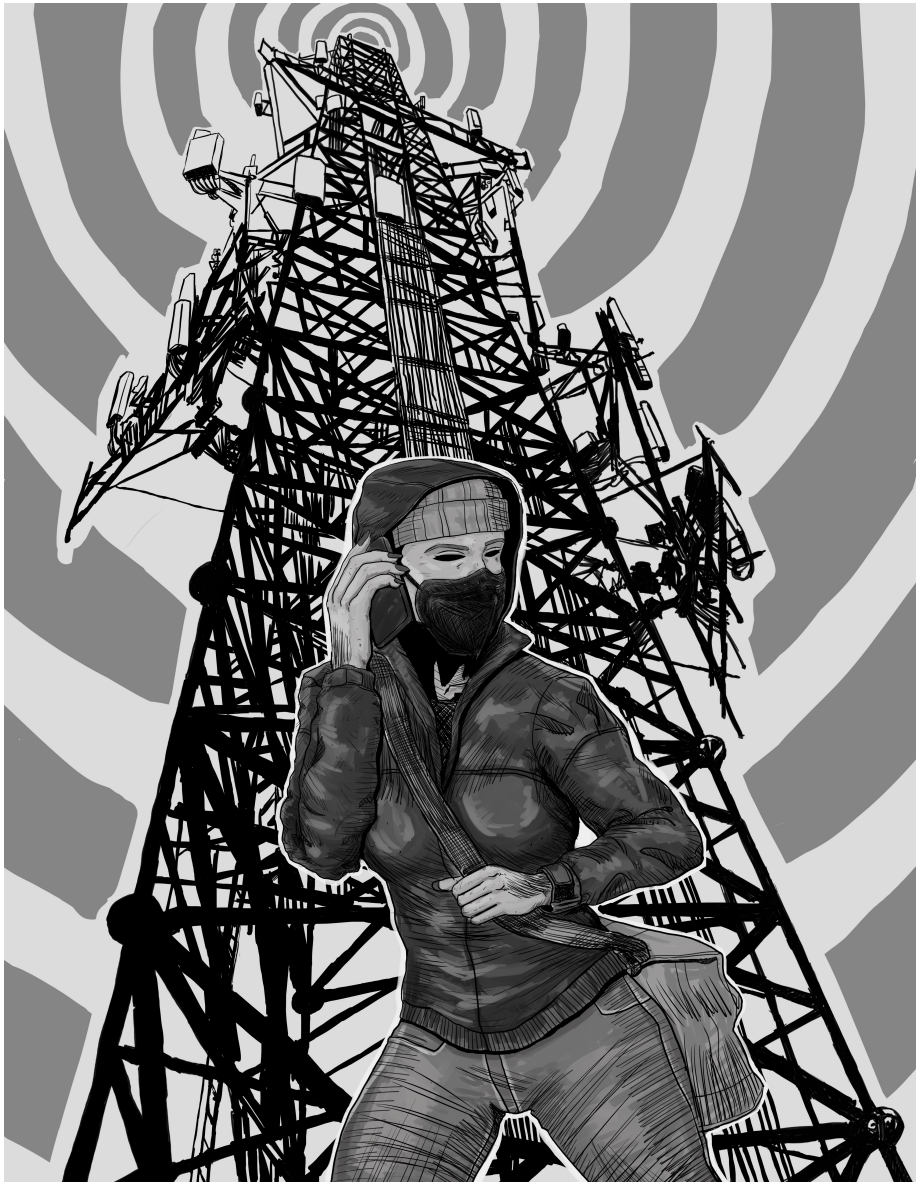
SEGURIDAD DEL TELÉFONO MÓVIL

PARA ACTIVISTAS Y ORGANIZADORES



HÅKAN GEIJER

Una de las herramientas más poderosas que tenemos a nuestra disposición son nuestros teléfonos inteligentes conectados a Internet. La comunicación instantánea, sumada al hecho de tener todo el conocimiento humano al alcance de la mano, aumenta de manera masiva nuestra capacidad de afectar al mundo que nos rodea. Sin embargo, esta conectividad se produce a costa de una mayor vigilancia por parte de los aparatos de seguridad del Estado y de los particulares. Las personas activas en movimientos de liberación son conscientes, en diferente medida, de esta vigilancia. Por esta razón, hemos desarrollado Prácticas de Seguridad Operacional (OpSec) y una cultura de seguridad interna para contrarrestar las interrupciones de nuestros esfuerzos organizativos.

Hay muchas leyendas urbanas en torno a los celulares. Por lo general, estos relatos se derivan de la falta de comprensión de la tecnología telefónica y de las capacidades que el Estado y los actores privados tienen a su disposición para vigilar a los individuos a través de sus celulares. El "modelado de amenazas" es el proceso de identificar las amenazas y construir contramedidas pragmáticas y específicas contra ellas. Sin embargo, sin modelos precisos de los adversarios, los modelos pueden conducir a contramedidas ineficaces. Las acciones basadas en información errónea pueden provocar arrestos fáciles o crear la impresión de un adversario omnividente, lo cual dificulta la acción. Este texto cubre la tecnología básica de los celulares y aborda las leyendas urbanas populares para que tú y tus compañeros puedan resistirse a la interrupción y organizarse de forma eficaz.

No existe la seguridad perfecta. No es una dualidad entre "seguridad" y "no seguridad," ni tampoco es un espectro entre "mejor seguridad" y "peor seguridad." La seguridad depende tanto de las medidas preventivas como de las circunstancias. Y, lo que puede ser útil para evitar que el Estado no te rastree tal vez no sea útil para prevenir que una pareja abusiva lea tus mensajes.

Esta guía te ayudará a comprender los riesgos a los que te enfrentas para que puedas tomar decisiones informadas. La cultura de seguridad no es una garantía, pero puede reducir los riesgos. Podría prevenir tu encarcelamiento, así como salvar tu vida, o la de los que te rodean.

Este texto fue escrito a comienzos de 2022 por anarquistas en Europa y Norteamérica y, por ello, será más relevante para aquellas personas que están cerca de nosotros tanto en el espacio como en el tiempo. Omitimos la mayoría de la información legal; solo porque tu adversario no tenga permitido hacer algo no significa que no lo vaya a hacer de todas formas. Por esta razón, abordamos las posibilidades. También reconocemos que no somos capaces de predecir el futuro. Vas a tener que usar la familiaridad de tu contexto personal y local para adaptar lo que escribimos a las amenazas específicas que enfrentas.

Tú y tu teléfono

Tu teléfono[1] no es sólo una pertenencia personal valiosa, sino que también constituye una extensión de ti mismo. Contiene tus memorias, tus conocimientos

[1] Para ahorrar espacio, usamos "teléfono" para referirnos a "teléfono móvil" o "teléfono celular."

o rastrearlo no significa que vayan a hacerlo para cogerte colándote a los parques después de la hora de cierre. Incluso en casos en los que el Estado quiere utilizar el máximo de espionaje puede que lo haga de forma inepta. Vuestro modelo de amenaza debería contar con una respuesta realista y esperable de vuestros adversarios dado su conocimiento de vuestras acciones.

Aprende acerca de cómo la policía, los fascistas y otros adversarios en tu área operan, e idea un modelo de amenaza para tí y tu grupo. Discútelo bien con tus compañeros. Comienza con pequeñas muestras de conocimiento de Seguridad Operativa y conviértelo en cultura de la seguridad. Adopta conocimiento y prácticas compartidas que lleven a una mayor seguridad contra las amenazas que podríais enfrentar. Dad pasos concretos, pero de forma pragmática. Empezad poco a poco con sólo unas cosas nuevas cada vez hasta que las normalicéis, y luego construid a partir de ahí. Un plan sólo es bueno si puedes llevarlo a cabo, e intentar hacer muchos cambios grandes apresuradamente tiende a sobrepasar y ser frustrante. La mayoría de los planes exitosos se aplican incrementalmente.

Cuidado con las leyendas urbanas. Los espacios activistas están plagados de ellas y la seguridad no es una excepción. Preguntad *Cómo?* Y *Por qué?* Cuando la gente diga cosas sobre seguridad o contramedidas. Basad vuestro modelo de amenaza y vuestro plan de seguridad en hechos verificables o, al menos, en conjeturas muy probables con pruebas que las apoyen.

Usad este conocimiento para protegeros mientras redibujáis el mundo.

Recomendaciones

El grupo de afinidad podría crear un subgrupo de miembros quienes estén de acuerdo en no llevar teléfonos a las acciones y continuar su trabajo. En paralelo, podrían trabajar con Felix para hacerle entender cómo y porqué llevar su teléfono crea riesgos innecesarios. Podrían debatir con el que sus acciones les causan incomodidad y que sus acciones no sólo le afectan a él. El grupo podría ser capaz de seguir siendo camaradas de Felix, pero podría verse obligado a excluirlo de acciones secretas si el rechaza dejar su teléfono en casa.

Notas Finales

La tecnología no es ni buena ni mala (al menos la mayoría). No es totalmente liberadora ni opresiva. Nueva tecnología crea nuevas oportunidades mientras cierra otras. Con los teléfonos sucede lo mismo. Tener acceso a comunicaciones instantáneas y un vasto conocimiento en nuestro bolsillo es un poder tremendo, pero viene con el coste de una vigilancia mayor.

Podrías pensar que el Estado no te está vigilando, pero si estásinvolucrado en movimientos sociales de liberación, aunque sea vagamente, seguramente lo hace. Protegerte a tí mismo puede proteger a tus amigos, familia o compañeros que están más metidos que tú en el movimiento. Podrías pensar que el Estado hackea tu teléfono para escuchar tu asamblea semanal de la cooperativa de vivienda, pero seguramente no lo hace. El máximo de seguridad todo el tiempo es insostenible y exigirlo es una mala idea.

Después de leer esto podrías tener la tentación de decir "pero me rastrearán de todos modos." La creencia de que cualquier nivel de seguridad contra las amenazas externas es imposible se llama *nihilismo de la seguridad*. La gente que se siente así a menudo toma dos caminos diferentes. Pueden creer que ninguna contramedida funciona, así que continúan actuando sin tomar ningún tipo de precaución, creando una profecía de autocumplimiento que concluye con su detención. O bien pueden creer en la supremacía del Estado y caer paralizados con la inacción. La represión no funciona únicamente mediante el palo que nos azota, sino también mediante el miedo a ese castigo y la consecuente inacción autoimpuesta.

Cualquier paso que des puede protegerte, y muchos son tan sencillos que podrías empezar a aplicarlos ahora mismo. Empezando por lo más fácil, puedes evitar el espionaje usando aplicaciones básicas encriptadas para enviar mensajes y dejando tu móvil en casa durante manifestaciones o acciones directas. Cada paso que des más allá de éstos requerirá que tus adversarios hagan más esfuerzos si quieren vigilar o interrumpir tus actividades. Tiempo y recursos son limitados, incluso para las grandes agencias de inteligencia. Los humanos cometemos errores y los ordenadores se rompen. Tus adversarios no son infalibles y puedes disminuir significativamente la cantidad de datos que pueden capturar y que tipo de pistas pueden atisbar a partir de ellos.

Además, el Estado no siempre usa el máximo teórico de métodos de vigilancia a su disposición. Sólo porque sea posible para el Estado hackear tu teléfono

y tus pensamientos privados y semiprivados. Te permite buscar información de manera rápida y compartirla con los demás.

Esta conectividad, junto con el acceso al conocimiento, nos hace más efectivos a la hora de perseguir nuestros objetivos. Los teléfonos se han convertido, hasta cierto punto, en una necesidad para funcionar en la sociedad moderna. Por ello, las personas casi siempre los llevamos encima. Además nos pasa que cuando salimos de casa sin él o se le agota la batería, casi todos nos sentimos desnudos e impotentes, como si nos faltara una parte de nosotros.

El compromiso de un teléfono por un adversario, ya sea por medio de confiscación o *malware*, puede ser desastroso. Todos tus mensajes, imágenes, correos electrónicos y apuntes pueden quedar a disposición de dicho adversario. Además, podrían acceder a todas las cuentas en tu teléfono. El *malware* o las aplicaciones de acecho podrían activar tu micrófono o el rastreo de tu ubicación en tiempo real.

Además de estos tipos de vigilancia activa, tu teléfono proporciona vigilancia pasiva a partes privilegiadas. Por ejemplo, la policía puede solicitar acceso en tiempo real o acceso masivo a los metadatos que están disponibles para tu operador o PSI.[2]

Ante estas posibilidades de vigilancia, los activistas sostienen, con toda razón, que "tu teléfono es un poli" y que "tu teléfono es un soplón." Entonces, ¿debemos seguir usando nuestros teléfonos por lo que nos proporcionan o debemos deshacernos de ellos por los riesgos que suponen? O quizás haya algún matiz acerca de cuándo y cómo podemos usar los teléfonos de modo que se nos permita conservar buena parte de los beneficios y eludir la mayoría de los detrimentos.

Tecnología telefónica

Para entender cómo los teléfonos pueden ser pinchados para la vigilancia, necesitamos tener una comprensión sólida de las diferentes tecnologías telefónicas. Necesitamos comprender el funcionamiento del *hardware*, el *firmware*, el sistema operativo, las redes móviles y, en cierta medida, la Internet en general. Esto te ayudará a construir un modelado de amenazas para que puedas tomar decisiones informadas, lo cual es preferible en lugar de memorizar pasos arbitrarios.

Redes celulares

Las redes celulares toman su nombre de las varias celdas superpuestas de cobertura proporcionadas por las torres transceptoras.[3]. La cobertura es más densa en zonas urbanas, por lo que un solo teléfono está en contacto con más torres. En zonas suburbanas y rurales, hay menos solapamiento de cobertura y, consecuentemente, un teléfono está en contacto con menos torres.

Los operadores de redes pueden usar información acerca de la propia señal para estimar la ubicación de los teléfonos. La ubicación imprecisa puede determinarse

[2]Proveedor de servicios de Internet

[3]No todos los emplazamientos celulares son torres, pero basta con usar el término común.

por el ángulo de llegada a la torre o por el conocimiento sobre desde qué sector[4] llegó la señal. Cuando se mide la distancia de un teléfono a varias torres, el proveedor de la red puede triangular la ubicación del teléfono con gran precisión.[5]. Las redes LTE pueden situar la posición de un teléfono con una precisión de unas decenas de metros, y las redes 5G son capaces de hacerlo con una precisión de cinco metros. Cuántas más torres haya, más fiable será la localización de un teléfono y, por lo tanto, la triangulación rural suele ser menos precisa que la urbana.

Cuando los teléfonos se conectan a una red celular, envían una identificación de dispositivo único (IMEI[6]) junto con su identificación de abonado (IMSI[7]). El IMSI suele almacenarse en una tarjeta SIM[8] o en una eSIM.[9] Esto significa que el intercambio de varias tarjetas SIM entre un dispositivo o el intercambio de una tarjeta SIM entre varios dispositivos puede crear un enlace duro entre esas identidades. No se requiere una SIM o una IMSI para hacer una llamada; estas sólo autentican el dispositivo ante el operador y determinan si el aparato está autorizado a hacer llamadas o a utilizar los datos móviles. Por ejemplo, en todas (o en casi todas) las regiones se puede llamar a los servicios de emergencia sin necesidad de una SIM. Retirar una tarjeta SIM del teléfono **no impide el rastreo.**

Tipos de teléfonos

La mayoría de la gente que dice "teléfono" quiere decir "teléfono inteligente", es decir, uno con un sistema operativo y aplicaciones que pueden ser instaladas por los usuarios. Un teléfono con funciones básicas es el tipo menos sofisticado de teléfono móvil, como los que se veían en los viejos tiempos y que sólo pueden hacer llamadas telefónicas y enviar mensajes SMS.

Los teléfonos *feature* son algo raros hoy en día. Están a medio camino entre los teléfonos inteligentes y los teléfonos sencillos. Pueden tener aplicaciones específicas del proveedor, tales como una *app* de correo electrónico o un navegador de Internet incorporado. Para distinguir los teléfonos *feature* y aquellos con funciones básicas de los teléfonos inteligentes, se usa el término "teléfono sencillo" para describir los dos primeros tipos.[10]

Teléfonos inteligentes

Los teléfonos inteligentes suelen tener un servicio de localización que permite a los teléfonos proporcionar datos de ubicación de gran precisión y en tiempo real a las aplicaciones, en particular a los mapas. El servicio de localización utiliza se-

[4] El área en forma de cono cubierta por una sola antena.

[5] Esto se llama "multilateración de enlace ascendente." En este caso, usamos "triangulación" para referirnos a "multilateración" porque vale la pena cambiar la terminología técnica por la comprensibilidad.

[6] Identidad Internacional de Equipo Móvil.

[7] Identidad de Suscriptor Móvil Internacional.

[8] Módulo de Identificación de Abonado.

[9] SIM integrada, un chip integrado directamente en el dispositivo.

[10] A veces, se usa el termino "teléfono tonto" para referirse o a todos los telefonos sencillos o solamente a los teléfonos basicos. En aras de la claridad, evitamos usar este término.

Análisis

No publicitar el evento es, obviamente, un paso correcto para evitar que la policía se entere. Pedir a la gente que sólo difundan la info a contactos de confianza mediante canales seguros también es una buena forma de reducir el riesgo, pero sólo es necesaria una persona que envíe una versión abreviada del mensaje con el lugar y la hora para que éste aviso se pierda. Incluso sabiendo esto, es un riesgo que el colectivo tiene que aceptar.

Recomendaciones

Hay poco que el colectivo pueda hacer para evitar que la gente llegue al evento con sus teléonos encendidos, así como poco pueden hacer para asegurarse que el mensaje permanece sólo en las partes seguras y de confianza de la web. Esto es un problema difícil en la cultura de la seguridad porque la falta de seguridad de una parte de los individuos puede comprometer al grupo por completo, especialmente cuando el beneficio individual de mantener el teléfono encendido es alto, mientras que el riesgo para el individuo es bajo. Los organizadores que han creado el evento y cedido el equipo son los que tienen más posibilidades de afrontar las consecuencias. Si la muchedumbre se disuelve durante una redada ellos se enfrentarán a las consecuencias con toda seguridad. Lo mejor que el colectivo puede hacer es intentar utilizar la vergüenza y la presión social antes y durante el evento para convencer a la gente de que sus acciones podrían arruinar la rave para todos.

Caso 9: Lidiando con un eslabón débil

Escenario

Un grupo de afinidad va a por los nazis que acosan a la gente de su comunidad. Tienen el acuerdo de no llevar teléfonos a sus acciones nocturnas. Felix, uno de sus miembros más activos, cree que esto es un comportamiento paranoico y rechaza dejar el suyo en casa.

Supuestos

El grupo ha asumido que el Estado quizá use los datos de localización de sus teléfonos para investigar sus actividades. También son conscientes de que el comportamiento de Felix, llevando su teléfono, les pone en peligro.

Contramedidas

Para evitar que Felix les ponga el peligro han parado sus actividades hasta que puedan llegar a un acuerdo con él.

Análisis

Las acciones de Felix ponen en riesgo al grupo y el grupo tiene razón cuando considera que no deberían dejarle participar en sus acciones. Si el grupo al completo interrumpe sus actividades el daño podría volver a su comunidad. Y los riesgos de ser arrestados por culpa de un teléfono podría ser muy bajo dependiendo de cómo la policía investigue estos asuntos en dicha región.

Los ecoactivistas de todo el mundo, incluyendo aquellos de las llamadas *democracias* occidentales, son un objetivo específico de vigilancia, incluso cuando no se involucran en acción directa. Autoalojar el email quizá disminuya el riesgo de vigilancia corporativa, pero siempre hay algún resquicio por donde se pueden filtrar datos. La policía podría ahorrarse tratar con el grupo de técnicos que gestionan el correo (y que quizá avisarían a los activistas incluso en el caso de tener una orden de registro) yendo directamente a por la empresa que aloja el servidor. Además, los técnicos quizá no tengan la competencia técnica de las grandes compañías de email para proteger el servidor o descubrir si ha sido hackeado por trolls o el Estado.

Recomendaciones

Si el espacio en el teléfono es un problema, los activistas deberían hacer una backup de sus fotos y vídeos para luego borrarlos y hacer espacio. Esto es generalmente una buena práctica para ayudar a conservar los datos si el móvil se daña o pierde.

Lo ideal sería que el colectivo pasase a usar una aplicación de chat encriptada, pero si continúan usando el email debería ser sólo para los detalles más básicos como las horas y lugares de sus actividades. Planes, debates internos y otras discusiones importantes deberían permanecer fuera del email ya que esta información puede dar al Estado grandes pistas sobre la situación del colectivo que pueden usarse en su contra.

Caso 8: Raves Underground

Escenario

Un colectivo planea raves al aire libre durante la pandemia del coronavirus. Piden que la gente lleve máscaras y creen que con esto bastará para contener el virus. La policía tiene restricciones para las reuniones de gente (excepto para ir a trabajar o a cualquier otra cosa que mantenga la máquina del capital engrasada).

Supuestos

El estado ha hecho esfuerzos para disolver reuniones masivas (únicamente las de clase baja y marginal, por supuesto), pero no van a andar buscando pruebas o pistas de este tipo de reuniones. Tienen la capacidad de reunir datos de localización de los teléfonos en tiempo real que podrían usar para detectar varios cientos de personas en una localización remota. La Policía tiene informantes que escuchan cosas como ésta, y otra gente simplemente disfruta jodiendo a otros si oyen algo que no les gusta.

Contramedidas

La rave no se ha publicado en las redes sociales y se solicita información antes de enviar los datos del evento a alguien mediante canales seguros. En la info se pide a la gente que pongan sus teléfonos en modo avión cuando se acerquen a la localización.

ñales recibidas de los satélites GPS[11] o GLONASS[12] para triangular la ubicación del dispositivo. La mayoría de los teléfonos inteligentes utilizan A-GPS.[13] A-GPS combina las señales de las torres, las señales de wifi e incluso los datos intercambiados a través de la Internet para calcular de manera rápida y precisa la posición del dispositivo.

Los teléfonos inteligentes contienen frecuentemente una brújula, un acelerómetro, un giroscopio y un barómetro. Incluso sin GPS o multilateración, las mediciones de esos sensores pueden combinarse para obtener una ubicación actual aproximada desde una ubicación anteriormente conocida.

Esto significa que pese a que las señales GPS son recibidas por el dispositivo de manera pasiva, el uso de los servicios de ubicación puede dar a conocer la posición del teléfono. Esto también evidencia que desactivar las funciones de localización tal vez no sea suficiente para evitar que un *malware* o una aplicación no deseada encuentre la ubicación de tu teléfono de manera aproximada.

Teléfonos sencillos

Muchos activistas creen que usar teléfonos sencillos en lugar de teléfonos inteligentes es "más seguro." Dado que un teléfono sin GPS ni servicios de localización todavía puede ser geolocalizado, los móviles sencillos no ofrecen una protección significativa contra el rastreo de ubicación. Los teléfonos *feature* típicamente carecen de las aplicaciones de chat de voz o texto, y, por definición, los teléfonos con funciones básicas no tienen esas capacidades. Esto significa que sólo se dispone de SMS y llamadas telefónicas sin cifrar, y estas son susceptibles a ser interceptadas de más maneras que si hubiera un modelo cliente-servidor o un cifrado de extremo a extremo. Los teléfonos con funciones básicas, los que parecen menos avanzados tecnológicamente, solo pueden tener capacidades 2G. Esto significa que las llamadas y los textos SMS pueden ser interceptados fácilmente usando productos no profesionales por un valor de 25 euros. Y, además, muchos de estos dispositivos podrían tener capacidades ocultas de Internet que envían datos telemétricos de vuelta a los fabricantes sin el conocimiento del usuario.

En resumen, **los teléfonos sencillos no son más seguros** que los teléfonos inteligentes contra la mayoría de las amenazas enfrentadas por los activistas.

Malware

El *malware* es un *software* malicioso. Es un programa que hace cosas que no quieres que haga mientras que, al mismo tiempo, intenta ocultar sus actividades. El *malware* creado por el Estado tiene el objetivo de vigilar y extenderse a otros teléfonos o incluso a dispositivos electrónicos como los *routers* de wifi.

Viejas recomendaciones sobre seguridad decían que el *malware* se instalaba al visitar páginas sospechosas o abrir adjuntos en correos electrónicos de remitentes desconocidos y, aunque esto sigue siendo verdad, la superficie de ataque es mucho

[11] Sistema de Posicionamiento Global.
[12] Sistema Global de Navegación por Satélite.
[13] GPS asistido.

más grande. La mayoría de las aplicaciones (por no decir todas) esperan a que lleguen las notificaciones de los servicios de Google Play y luego hacen peticiones a los servidores de la *app*. Algunos de los *malwares* son de clic cero, o sea, no requieren la interacción del usuario. Por ejemplo, el *spyware* Pegasus de NSO Group utilizó un virus de clic cero para atacar a activistas, periodistas y políticos. El *malware* puede instalarse en tu teléfono aunque solo uses aplicaciones de confianza y solo aceptes a sabiendas mensajes de contactos conocidos.

Algunos casos de *malware* solo permanecen en la memoria de tu teléfono mientras están encendidos y son incapaces de persistir entre reinicios. Debido a esto, algunos tipos de *malware* piratean las rutinas de apagado de tu teléfono y realizan un falso apagado. Aun así, reiniciar tu teléfono podría potencialmente eliminar un *malware*. Dicho esto, si crees que tu dispositivo ha sido infectado, tendrás que encontrar un especialista de *malware* que te pueda ayudar a determinarlo. También es posible que vayas a necesitar un nuevo teléfono. El *malware* es menos común de lo que se cree, pero no dejes que su rareza te haga ignorar las señales de advertencia. El *malware* creado por el Estado no se detecta tan fácilmente como el *malware* de bajo esfuerzo, por lo que los métodos comunes pueden no ser aplicables.

Lamentablemente, la detección no es algo que puedas hacer por tu cuenta.

Sistemas operativos

Una de las preguntas más comunes que se hacen los activistas con respecto a los teléfonos inteligentes es la siguiente: "¿Qué es más seguro, iOS o Android?" Como con todas las otras preguntas de seguridad, la respuesta es "depende."

Los sistemas operativos de los teléfonos inteligentes son de dos tipos: iOS para dispositivos Apple, y Android para todo lo demás. iOS es propietario y tiene un "código fuente privado." Android es un sistema operativo base que tiene un código fuente público que los fabricantes pueden modificar para sus dispositivos. Los sistemas operativos Android de los fabricantes suelen tener un código fuente privado. Además, hay muchas versiones completas de Android mantenidas por la comunidad de código abierto, sobre todo LineageOS[14]. GrapheneOS y CalyxOS son sistemas operativos Android de código abierto que se centran en la privacidad y la seguridad.

Cuando un teléfono está encendido, el *hardware* empieza a cargar el sistema operativo a través de un proceso en el que cada paso verifica la integridad del *software* necesario para el siguiente paso. Este proceso se llama "arranque seguro." Para instalar un sistema operativo personalizado, el arranque seguro debe ser desactivado. De no ser así, el *hardware* se negaría a cargar el sistema operativo personalizado. La razón de esto radica en que el *hardware* no está firmado criptográficamente por una llave confidencial incluida por el fabricante. Esto permite la posibilidad de que se instale un sistema operativo malicioso que pueda leer los datos a través de *malware*, en lugar de un verdadero sistema operativo . Sin embargo, esto no significa que los sistemas operativos integrados (los sistemas operativos precargados en

[14] LineageOS es el sucesor popular del descontinuado CyanogenMod.

su móvil. A partir de aquí la policía podría aprender de sus redes sociales o las actividades de sus amigos más externos. Esto puede ponerles en peligro más que a ella misma.

Recomendaciones

Incluso si Isa no se anticipa a su detención, debería andar con más cuidado con su teléfono. Podría quedar con sus amigos en localizaciones fijas algún tiempo antes de la mani para poder evitar traer sus teléfonos o, si realmente quieren tener información en tiempo real, solo una persona del grupo debería llevar un teléfono. Ser cuidadosa con su teléfono puede proteger a su círculo más externo de amigos radicales que quizá están involucrados en medios de resistencia militante al fascismo.

En cualquier caso, las probabilidades de que ocurran cualquiera de estas cosas es baja y el beneficio esperado de llevar un teléfono es alto. Eso hace que en este caso esté "bien" que Isa lleve su teléfono… hasta que, de repente, no lo esté.

Caso 7: Comunicaciones y planes generales

Escenario

Un colectivo organiza protestas legales y reparte folletos promoviendo alternativas verdes y ecológicas al status quo, como hacerse vegano, inversión en infraestructura ciclista, disminución de la dependencia del automóvil… Utilizan una lista de mail alojada en un servidor proporcionado por un grupo de activistas tecnológicos local.

Supuestos

El colectivo asume que la policía está interesada en los activistas en general, pero que el colectivo en sí mismo no está siendo amenazado específicamente. Saben que los *trolls* locales gustan de acosar a los "comunistas hipis." También que hay otras organizaciones verdes militantes más en su misma región, y que los miembros de su colectivo quizá estén en todo tipo de otros grupos.

Contramedidas

El colectivo quiere evitar el acoso, así que mantienen su lista de correo privada y por invitación. Quieren evitar ser rastreados por las grandes compañías de email, por lo que alojan su propio servicio de email.

Análisis

Las listas de email son bastante populares porque todo el mundo tiene acceso al email, mientras que hay muchas aplicaciones de chat diferentes y no todo el mundo usa las mismas, por lo que los colectivos tienden a continuar usando listas de correo. Frecuentemente la gente dice no tener suficiente espacio en sus teléfonos para más aplicaciones. Algunos miembros de colectivos tienen pocas habilidades técnicas y no quieren aprender a usar otras aplicaciones, por lo que, a veces, el email es inevitable.

interesante está ocurriendo. Esto podría suponer un incentivo para aumentar la vigilancia, como por ejemplo poniendo micros en la zona (si se reúnen siempre en el mismo lugar) o enviar a un secreta con un micrófono a seguirles en los bares o restaurantes donde se reúnen. Es más, si un miembro del grupo cae pero no dice nada durante el interrogatorio, la policía podría mirar en su teléfono si existen pistas sospechosas. La policía podría reunir la información preguntándose: En el momento en que se apagó el teléfono, qué otros teléfonos se apagaron cerca de él? Y qué estaban haciendo los teléfonos de otros sospechosos en ese momento? Esto podría revelar el resto de los miembros del grupo de afinidad o proporcionar pruebas que apoyen que los miembros del grupo de afinidad eran cómplices. Es posible que la policía no piense en estas preguntas o no formen parte de sus operaciones habituales, pero es mejor no dejar ningún rastro.

Recomendaciones

Ya que se están anticipando a la vigilancia y métodos para investigar sus actividades, deberían dejar todos sus aparatos en casa y elegir localizaciones al azar para sus reuniones que sean o bien muy ruidosas, o bien muy aisladas.

Caso 6: Teléfonos en acciones masivas

Escenario

Isa es una activista que principalmente acude a grandes manifestaciones y, aunque ella misma no es muy radical, tiene algunos amigos que sí lo son y generalmente se entera de las cosas que hacen. Los fascistas han planeado una marcha y Isa, junto con algunos amigos, van a ir a unirse a las masas que esperan bloquear la ruta planeada. Para contactar con sus amigos y tener información al minuto sobre el bloqueo o cambio de rutas Isa va a llevar su teléfono habitual (el único que tiene).

Supuestos

Isa no está preocupada por si le arrestan porque en acciones similares en el pasado, con una gran cantidad de gente que no aparenta ser el clásico antifa bloqueando las calles, la policía sólo les aparta a la vez que reconduce la marcha fascista. Ella no piensa en que si es arrestada mirarán en su móvil, ya sea de forma legal o ilegal. Tampoco está concienciada sobre los datos de localización de su móvil.

Contramedidas

Isa no ha tomado contramedidas contra la recolección de datos de localización de su teléfono o la confiscación de éste.

Análisis

En acciones masivas la policía puede utilizar rastreadores IMSI para ver quién ha asistido a las protestas y construir perfiles. Estos datos de localización podrían usarse para perseguir a gente por disturbios incluso si los cargos no suponen penas de prisión.

Si detienen a Isa, lo cual podría ocurrir si el bloqueo no es muy grande o es una de las personas con la mala suerte de ser pilladas en las calles, podrían registrar

tu dispositivo por defecto) sean más o menos seguros que aquellos personalizados. Evidencia que hay un perfil de riesgo diferente al desactivar el arranque seguro y usar un sistema operativo personalizado.

Cuando se desarrolla un *malware*, este debe dirigirse a una sola aplicación o sistema operativo. El desarrollo del *malware* cuesta tiempo y dinero, y, una vez que se implementa, puede ser detectado y volverse incapaz de infectar nuevos dispositivos a causa de actualizaciones de la aplicación o del sistema operativo.[15] Por esta razón, resulta más económico codificar *malware* que pueda atacar a muchos usuarios. iOS cuenta con un número limitado de versiones para un número limitado de dispositivos, mientras que el ecosistema

Android es mucho más diverso. Esto significa que crear *malware* dirigido a los usuarios de Android es menos económico y más difícil para los adversarios.

Nuestras recomendaciones son las siguientes:

- Para la mayoría de los individuos que tratan de evitar la vigilancia masiva y los *hackers* de bajo esfuerzo, iOS o Android estándares son suficientes puesto que son más fáciles de usar.
- Para las personas significamente involucradas en movimientos sociales o personas que esperan ser apuntadas, recomendamos para su organización y trabajo político que usen GrapheneOS sin servicios de Google Play, que usen F-Droid como único repositorio de aplicaciones y que instalen solo el número mínimo de aplicaciones necesarias para las comunicaciones.
- Para las personas que han atraído o esperan atraer la atención de las agencias de inteligencia, se deben evitar los teléfonos para todo lo relacionado con el activismo.

Cifrado de dispositivos

iOS y Android ofrecen la posibilidad de cifrar tus datos personales. Esto recibe diferentes nombres, tales como Protección de Datos y Cifrado de Dispositivos. Generalmente, los teléfonos **no tienen activado** el cifrado de dispositivos por defecto. Esta función **debe ser activada** por el usuario, ya sea al configurar el teléfono o, luego, a través de los ajustes. Asimismo, la protección contra repetidos intentos de inicio de sesión debe ser activada.

La implementación de cifrado de dispositivos suele utilizar un módulo de seguridad de *hardware* (HSM) o un co-procesador de seguridad,[16] o sea, *chips* especiales en el teléfono que se encargan del cifrado, el descifrado y las claves criptográficas utilizadas para estas operaciones. Estos *chips* son importantes porque protegen las

[15] Además, el *malware* tiene la interesante propiedad de que, cuando se utiliza, puede ser capturado y clonado para que otro puedan reutilizarlo. Sería como si existiera la posibilidad de que los misiles pudieran ser copiados y recreados de manera instantánea e infinita cada vez que un misil cayera en territorio enemigo; y también como si ese tipo concreto de misil tuviera muchas más probabilidades de ser interceptado en el futuro. Los ejércitos dudarían en disparar tantos misiles y tendrían que ser mucho más estratégicos en sus objetivos.

[16] En los dispositivos de Apple, este chip se llama Enclave Seguro.

claves de la manipulación o del acceso no autorizado. También pueden impedir que tus adversarios accedan tus datos, pero no es una garantía. La herramienta GrayKey, entre otras, puede aprovecharse de los *bugs* en los HSM y, en algunos casos, puede *hackear* la contraseña de desbloqueo y descifrar los datos. Aunque los HSM pueden estar seguros ahora, puede que se descubran nuevos *bugs* el mes que viene y las autoridades también pueden desarrollar nuevas técnicas para recuperar datos dentro de 5 o 10 años.

El cifrado de dispositivo es bueno para prevenir que tus datos sean accesados si un ladrón roba tu teléfono o si un policía te lo quita durante una detención. No es probable que resista los esfuerzos concertados para acceder a tus datos por parte de agencias de inteligencia estatales como el MI5 o el FBI.

Un ejemplo destacado es cuando el FBI descifró la contraseña del teléfono del tirador masivo alrededor de un año después del tiroteo de San Bernardo en 2015. Unos cinco años después, se reveló que el acceso a los datos fue realizado a través de una serie de vulnerabilidades contra el *software* en el HSM.

El uso del cifrado de dispositivo puede proteger contra la captura de datos, pero **la única forma de garantizar que los datos no caigan en manos de las autoridades es asegurando que esos datos nunca hayan existido**.

VPNs

Una red privada virtual (VPN), en el uso más común del término, se refiere a una aplicación que enruta el tráfico de Internet de un dispositivo a un servicio cuyo propósito es ocultar el tráfico *web* y la dirección IP de los observadores de la red o de los servidores a los que se está conectando. Cuando se usan, las VPNs protegen tu tráfico de ser controlado a través de redes wifi públicas y, al mismo tiempo, esconden tu dirección IP de los servidores a los que se ha conectado.

Las aplicaciones VPN pueden causar distracciones durante una investigación o dificultar la vigilancia pasiva, pero también uno puede olvidarse de permitirlas o puede haber un escape de tráfico. El tráfico hacia y desde tu proveedor de VPN puede ser obtenido por las agencias de inteligencia estatales que son capaces de ver todo el tráfico de Internet. Y, además, tu servicio de VPN puede ser legalmente obligado a recopilar registros y entregarlos a las autoridades. Las VPNs son baratas y pueden mejorar la seguridad en algunos aspectos, pero no se debe confiar en ellas para proporcionar anonimato contra el Estado.

IMSI catchers

Un IMSI *catcher*[17] es un dispositivo que se disfraza como una torre celular legítima, lo que obliga a los teléfonos a conectarse a él, permitiendo así la escucha telefónica o el envío de mensajes o llamadas telefónicas. A veces, esta "suplantación" se puede detectar, pero no se debe confiar por completo en la detección. En algunas regiones, los IMSI *catchers* pueden ser usados sin orden judicial, especialmente durante las manifestaciones. Funcionan en parte al degradar los protocolos

[17]También conocido como Stingrays después de una marca popular de ellos.

Análisis

La localización de Ruben es prácticamente igual de rastreable usando un smartphone que usando un teléfono básico. Sus comunicaciones son más inseguras porque no tiene la posibilidad de enviar o recibir mensajes de "emergencia" con sus compañeros usando su teléfono básico y, si lo hace, serán interceptados y almacenados por el Estado. Sus contramedidas contra el espionaje han creado una barrera entre el y su grupo, además de no proporcionarle una mayor seguridad ante las amenazas que enfrenta.

Recomendaciones

Ruben debería usar su propio smartphone para comunicarse en general. Si hay veces en las que necesita esconder su ubicación o sus conversaciones debería dejar el móvil en casa.

Caso 5: Planear sin móviles

Escenario

Los miembros de un grupo de afinidad han estado involucrados en movimientos de liberación durante el tiempo suficiente para ser conocidos por el Estado. Actualmente están planeando Algo Grande. Se han prohibido hablar sobre el tema cerca de aparatos electrónicos y únicamente lo hacen en persona.

Supuestos

Dan por supuesto que el Estado hará lo que sea necesario para prevenir su acción e incluso más para investigarla si llega a ocurrir. Dan por hecho que es posible que sus aparatos electrónicos hayan sido comprometidos por malware del Estado. También dan por hecho que, incluso en ausencia de pruebas, estarán en la lista de principales sospechosos de la acción, por lo que su seguridad operacional necesita ser afinada.

Contramedidas

Debido a la posibilidad de malware, están tratando sus aparatos como menos que fiables. Por la posibilidad de ser el blanco de una investigación no discuten sobre la acción en sus hogares, vehículos o centros sociales conocidos u otros espacios ligados a movimientos de liberación. Para ayudar a reducir los metadatos que les vinculan entre ellos apagan sus teléfonos antes de llegar a los lugares de reunión y los vuelven a encender cuando se han ido.

Análisis

El grupo está en lo cierto cuando supone que podrían estar siendo vigilados y también al tratar sus teléfonos como a chivatos. Apagar los teléfonos disminuye la posibilidad de que un malware use su micrófono para espiarles y crea cierta confusión sobre sus localizaciones durante las reuniones. Pero esta ausencia de información podría resultar anormal en comparación con su uso habitual del móvil y todos sus móviles desapareciendo prácticamente al mismo tiempo cerca de una ubicación podría ser una pista para el Estado de que durante esos periodos algo

El grupo ha pasado por alto las implicaciones de seguridad de usar un teléfono simple para comunicarse con el equipo de negociaciones. La policía podría desplegar un receptor IMSI para poder leer los SMS que se intercambian entre el equipo de okupación y el de negociación. Esto podría dar ventaja a la policía en las negociaciones o la oportunidad de aprovecharse de las divisiones dentro del grupo para forzar un desalojo más fácilmente.

En cualquier caso, si la policía quiere invertir este nivel de esfuerzo en rastrear los individuos basándose en los teléfonos presentes en la okupación es que probablemente hay motivos para pensar que la okupación en sí misma no será viable por la fuerte presión de la "ley y el orden".

Recomendaciones

Las razones de que el equipo de okupación quisiera llevar un teléfono simple al interior del edificio eran legítimas, pero deberían haber usado un teléfono para manis con una cuenta de un sólo uso que creasen en una app de chat encriptado. Esta cuenta debería comunicarse únicamente con una cuenta anónima perteneciente a los equipos del exterior para prevenir filtrar las redes sociales del grupo si el teléfono es confiscado o el desarrollador de la app está guardando datos de esas cuentas que después puede ser requerida por un juzgado.

Caso 4: Teléfono simple + Signal de Escritorio

Escenario

Ruben es un activista involucrado en un grupo que cree que está bajo vigilancia activa debido a su carácter antigubernamental. Para minimizar el rastreo de las agencias de inteligencia y policía local utiliza un teléfono básico con una SIM cuando está por ahí. Algunos debates con su grupo son más delicados y necesitan una app de mensajería encriptada, para lo cual han elegido Signal. Signal requiere de un registro con un número de teléfono y sólo generará las claves de encriptación iniciales a través de la aplicación de Android o iOS. Para hacer que la aplicación de escritorio de Signal funcione en su portátil, Ruben ha usado la SIM de su teléfono básico en el smartphone de un amigo para poner en marcha la app de Signal y poder vincularla con su aplicación de escritorio. Después ha cerrado la sesión de su cuenta en el teléfono de su amigo.

Supuestos

La decisión de no llevar un smartphone se basa en la creencia de que los smartphones son más fácilmente rastreables que los teléfonos básicos. Ruben también supone que Signal es más seguro que las llamadas de teléfono o SMSs, así que usa signal para algunas de sus comunicaciones.

Contramedidas

La decisión de Ruben de usar un teléfono básico tiene la intención de minimizar el rastreo de la localización de un smartphone. Su decisión de usar Signal desktop pretende prevenir la interceptación de sus mensages sensibles con sus compañeros.

de seguridad a unos sin cifrado o con cifrado débil. Aunque los teléfonos inteligentes prefieren protocolos que ofrecen más protección contra la interceptación y la suplantación, los IMSI *catchers* todavía pueden degradar los teléfonos a protocolos inseguros. Con respecto a esto, las llamadas telefónicas y los mensajes SMS enviados y recibidos por los teléfonos inteligentes no son lo suficientemente resistentes contra la interceptación.

Bolsas de Faraday

Los teléfonos envían y reciben información mediante la radiación electromagnética. Esta radiación puede ser bloqueada por materiales especiales. Las leyendas urbanas y algunas evidencias dicen que las señales se pueden bloquear metiendo un teléfono en una o varias bolsas forradas de aluminio. Sin embargo, al igual que muchas otras contramedidas, no se debe depender de esto. Se puede confiar en las bolsas de Faraday para bloquear las señales telefónicas. Si necesitas transportar los teléfonos y asegurar que las señales no se filtren, apagarlos tal vez no sea suficiente. A pocos teléfonos inteligentes se les puede quitar la batería, y algo en tu bolsa rozando tu teléfono puede presionar el botón de encendido. El malware puede piratear las rutinas de apagado y prevenir que el teléfono se apague al intenta apagarlo. Colocar un teléfono apagado en una bolsa de Faraday puede reducir considerablemente las probabilidades de que se determine tu ubicación.

Elementos básicos de seguridad

Hay algunas prácticas telefónicas que son recomendables para la mayoría de los activistas. Algunas de ellas son las siguientes:

Actualizaciones

No cabe duda de que lo mejor que puedes hacer para evitar ser hackeado por las autoridades o por un hacker cualquiera es actualizar rápidamente el sistema operativo y las apps de tu teléfono. Puede ser molesto tener que actualizarlo todo el tiempo, pero las actualizaciones contienen parches de seguridad para las vulnerabilidades críticas. Y, además, esto puede evitar que se vacíen tus cuentas bancarias, de pago, y de transferencia.

Gestores de contraseñas

La segunda práctica de seguridad más útil es usar un gestor de contraseñas para todas tus cuentas, incluidas las usadas en tu teléfono. Hay versiones de pago que permiten la sincronización automática de las contraseñas de diferentes dispositivos y de los inicios de sesión automáticos a sitios web. Sin embargo, estas requieren un cierto nivel de confianza en la corporación que vende el producto. Existen alternativas gratuitas como KeePassX, pero no tienen la maniobrabilidad de los productos de pago. Al usar un gestor de contraseñas, todas tus cuentas deben tener contraseñas seguras, únicas, y aleatorias. Estas suelen ser generadas automáticamente por el gestor. La contraseña maestra para desbloquear el gestor debe ser una frase larga y aleatoria.

Los humanos son notoriamente malos en generar la aleatoriedad necesaria para las contraseñas. Usar la primera línea de tu poema preferido o alterar los caracteres de antifascismo a `an7if4sc1sm0!` puede ser fácilmente descifrado por los computadores. Diceware es un método para generar contraseñas tirando los dados y usarlos para seleccionar palabras de una lista predefinida. Cinco palabras es lo mínimo, seis es mejor, pero cualquier número más de ocho es excesivo. Hacer esto proporciona una aleatoriedad indescifrable que no se puede crear por cuenta propia, y, por otra parte, esta aleatoriedad es fácil de recordar. La EFF proporciona una lista de palabras fácil de usar en inglés. La lista de palabras en español disponible del sitio web de A. G. Reinhold tiene algunas palabras difíciles de recordar, pero aún así puede ser más fácil de usar para los hispanohablantes que la lista de la EFF. Una frase de ejemplo de la lista de EFF es `MutableCalmBlubberFitJustify` (por favor **no uses esta**, crea la tuya propia).

Cuadro 1: Muestra de Diceware del EFF

Números	**EFF**	**Original**
24311	drowsily	baste
24312	drudge	basto
24313	drum	q92
24314	dry	basura
24315	dubbed	bata
24316	dubiously	q91
24321	duchess	batel
24322	duckbill	bateo

Bloquear tu teléfono

Dependiendo de tu modelo de amenazas, tal vez te convenga hacer que sea difícil (o casi imposible) desbloquear tu teléfono. Esto tiene una importancia especial porque el método de desbloqueo es también el método de descifrado, por lo que un método de desbloqueo seguro ayuda a proteger contra el acceso no deseado a tus datos si se confisca tu teléfono. Generalmente, debes preferir las contraseñas por encima de los códigos PIN o los patrones, porque el primero es más difícil de descifrar por las máquinas. Probablemente deberías desactivar la función de desbloqueo facial, y quizás debas desactivar el desbloqueo de huella dactilar. En algunas regiones existen protecciones legales para las contraseñas pero no para las huellas u otros biométricos.

Algunos teléfonos ofrecen la capacidad de eliminar todos los datos si se han realizado demasiados intentos de inicio de sesión fallidos. Debes activar esto (y luego mantener tu teléfono alejado de los niños curiosos y las mascotas).

Debes desactivar las notificaciones de la pantalla de desbloqueo, o al menos desactivarlas desde las apps que contienen información delicada. También debes desactivar el acceso a las apps desde la pantalla de desbloqueo.

construir hábitos que nos permitan resistir a esa represión nuestra sugerencia es más moderada. Practicas de alta seguridad comenzando desde ya. Intentar organizar eventos sin móviles. Cuando vas a hacer senderismo o quedas con alguien, incluso cuando vas a un pub, intenta convencer a todo el mundo de que dejen sus teléfonos en casa. Acostúmbrate a su ausencia. Siente la libertada de saber que no estás filtrando datos de localización al Estado y que nadie puede oir tus conversaciones excepto aquellos presentes.

Caso 3: Okupación y teléfonos simples

Escenario

Un grupo de activistas quieren okupar un edificio vacío con el objetivo de llamar la atención sobre las especulación inmobiliaria y, si la okupación tiene éxito, convertirlo en hogares gratis para personas locales que han sido deshauciados recientemente. Un equipo estará en el edificio realizando la okupación, mientras que otros estarán sobre el terreno negociando con el Estado y escribiendo en las redes sociales.

Supuestos

El equipo de okupación cree que la policía podría averiguar sus identidades viendo qué teléfonos se están comunicando desde el interior del edificio, e incluso si no fuesen arrestados o perseguidos por esta acción, ese conocimiento podría ser usado contra ellos en el futuro.

Contramedidas

Para reducir la probabilidad de que se descubran sus identidades aunque no sean detenidos durante la acción, el equipo de okupación ha escogido no llevar sus teléfonos personales. Únicamente llevarán un teléfono "quemable" para comunicarse con el equipo de negociación y poder participar de las decisiones, enviar posts al equipo de redes sociales y tener sensación de seguridad en lugar de permanecer aislados hasta el final de la acción. Usarán un teléfono con una SIM que no está registrada a nombre de ninguno de ellos para así permanecer anónimos.

Análisis

El grupo está acertado no llevando sus teléfonos personales al edificio que están okupando ya que podría ser usado para identificarles. La policía podría hacerlo mirando qué teléfonos están en el edificio y a nombre de quién están registrados o dónde tienden a pasar más tiempo (Por ejemplo, cuando el usuario está en casa durmiendo). El grupo se equivoca en llamar al teléfono "quemable" ya que su uso continuado puede ser utilizado para vincularlo con el grupo y sus integrantes. Este teléfono puede ser descrito más precisamente como un teléfono para manis. Ya que hay miembros del grupo que permanecen fuera del edificio, sin enmascarar, la identidad del grupo se conoce incluso si no todas las identidades de la okupación son conocidas. Si el teléfono es un "quemable" personal de uno de los activistas y éste se ha encendido en su casa, ésto puede ser usado para probar que el activista estaba dentro del edificio o estaba involucrado.

Contramedidas

El grupo no ha tomado ninguna contramedida contra la vigilancia de sus conversaciones.

Análisis

Si el grupo no discute planes o acciones deliberadamente, entonces ningún micrófono podrá registrar lo que se planea. En cualquier caso, las acciones planeadas y llevadas a cabo no es lo único en lo que el Estado está interesado. Los chismorreos, dramas, intereses amorosos, lazos sociales e incluso las medidas que las personas y organizaciones de un gueto político toman contra otro son información valosa. Esto podría permitir al Estado crear mapas sociales más precisos. Si el Estado sospecha que un individuo estuvo involucrado en algo que están investigando, y saben que éste tiene cómplices, el uso de mapas sociales construidos a partir de pequeños pedazos de conversaciones casuales pueden ayudarles a reducir su lista de sospechosos o revelar los miembros de un grupo de afinidad. Dichas charlas descubiertas pueden dar al Estado pistas acerca de quién se siente desplazado y resentido para que puedan intentar convertirlo en un informante. Los pequeños conflictos pueden ser explotados y los ánimos caldeados pueden ser convertidos en feroces disputas.

Recomendaciones

Hay una brecha generacional entre los activistas que se organizaban antes de la generalización de los teléfonos móviles y aquellos que empezaron a organizarse después de que éstos fueran ubicuos. Hay, también, una brecha más entre quienes se organizaban usando teléfonos simples antes de que los smartphones fuesen populares y aquellos que se han organizado siempre en un mundo donde casi todos sus contactos tienen smartphones. Esta brecha puede percibirse por la habilidad de hacer planes asumiendo que los demás no tendrán teléfonos, por ejemplo fijando lugares y horarios sin hacer cambios de última hora.

Como se ha mencionado anteriormente en este fanzine, los smartphones nos permiten comunicarnos instantáneamente y tener información ilimitada en mano en cualquier momento. Esto tiene el coste de nuevas vías de vigilancia. Los activistas deberían estar al tanto de que los teléfonos presentes en hogares, coches y ambientes sociales podrían estar reuniendo información de grupos sociales. Si hiciésemos la recomendación de que los teléfonos deberían estar apagados más frecuentemente se reirían en nuestra cara por paranoicos o por la imposibilidad de seguir la recomendación. La llamada democracia liberal proporciona la ilusión de que no vivimos bajo un estado policial represivo, pero aun así hay muchos casos de circulos sociales inofensivos y grupos activistas hackeados y espiados, por no mencionar los grupos más involucrados y radicales.

Nuestra sugerencia no es que nunca deberíamos llevar móviles encima, sino que queremos sugerir que todo el mundo tenga más conciencia del esfuerzo que invierte el Estado en espiar y de la utilidad de la información sacada de conversaciones casuales. Podría llegar el día en que la represión se recrudezca y comencemos a sentir su presencia de manera más aguda. Para prepararnos para ese tiempo y

Si tienes el cifrado de dispositivo activado en tu teléfono, tus datos son más protegidos cuando el teléfono está apagado (o se ha encendido pero aun no se ha introducido la contraseña de desbloqueo). Después de desbloquear tu teléfono una vez, la protección de tus datos es menos fuerte.

Muchos activistas dejan activado el desbloqueo de huella dactilar porque es muy conveniente si se compara con escribir una contraseña 100 veces al día. El hecho de que la conveniencia tiende a primar sobre la necesidad de mayor seguridad es otra razón para no mantener información delicada en tu teléfono. Si tienes activado el desbloqueo de huella dactilar, puedes desactivarlo temporalmente manteniendo pulsado el botón de encendido. Esto se puede hacer antes de interactuar con la policía, ir a la cama, o dejar tu teléfono sin vigilancia.

Funciones inalámbricas

Es recomendable que desactives el wifi y el bluetooth cuando no se están usando. Ambos pueden ser puntos de acceso vulnerables para el robo de datos o de identidad. Y, además, aumentan la superficie de ataque disponible para los hackers que intentan entrar en tu teléfono. Aunque los riesgos de dejarlos continuamente activados son mínimos, estas prácticas pueden añadir algunas pequeñas mejoras a la seguridad, y si no necesitas wifi o bluetooth, ¿por qué no hacerlo?

Copias de seguridad

Los teléfonos inteligentes a menudo vienen con una función para hacer copias de seguridad en una cuenta de *Cloud* vinculada al teléfono (en Apple para iOS y en Google para Android). Apple ha interrumpido anteriormente sus planes para cifrar las copias de seguridad en su iCloud tras presión del FBI, por lo que sus copias de seguridad no están cifradas. Sin embargo, Google ofrece copias de seguridad cifradas de extremo a extremo que, tras revisiones externas, ofrecen sólidas garantías de privacidad por parte de las autoridades o del propio Google. Además, algunas apps pueden tener sus propios servicios de copias de seguridad. Por ejemplo, WhatsApp puede hacer copias de seguridad de tus conversaciones en sus servidores.

No recomendamos hacer una copia de seguridad en Apple, pero las copias de seguridad de Google son lo suficientemente seguras porque tu teléfono no debe contener evidencias incriminatorias de todos modos. Dado que los datos enviados a terceros pueden perderse o destruirse incluso si no pueden ser recuperados por la policía, deberías considerar hacer una copia de seguridad de tus datos en un disco duro cifrado que tengas en casa o en algún lugar seguro.

Apps de mensajería

Las apps de mensajería son alternativas más seguras a las llamadas telefónicas y los mensajes SMS.

Cifrado

Las apps de chat de texto y voz ofrecen uno de dos tipos de cifrado.

El cifrado cliente-servidor es un tipo de cifrado en el que el canal entre un cliente (por ejemplo, tu teléfono) y el servidor es cifrado y protegido contra

la interceptación, la manipulación, y la falsificación. El mensaje se descifra y se almacena en el servidor. Cuando el mensaje es solicitado por otro cliente (por ejemplo, el teléfono de tu amigo), se vuelve a cifrar para el tránsito y se envía.

El cifrado de extremo a extremo es un tipo de cifrado en el que los clientes generan claves criptográficas e intercambian sus partes públicas entre sí. Los mensajes se cifran usando la clave pública del otro cliente y se envían a través del servidor. El servidor trabaja como transmisor ciego porque los mensajes solo pueden ser descifrados por el otro cliente.

El cifrado de extremo a extremo solo significa que un servidor o alguien entre tu teléfono y el de tu compañero no puede leer o manipular un mensaje. Un adversario todavía puede inferir información usando los metadatos sobre el tamaño del mensaje, la hora de envío, el remitente y el destinatario.

Algunas apps de mensajería ofrecen un cifrado de extremo a extremo de *opt-in*, como Telegram con sus chats secretos. Sin embargo, esta función no está disponible para los grupos. Otras apps tales como Signal o Wire cuentan con un cifrado de extremo a extremo obligatorio, al igual que iMessage y WhatsApp.[18]. Algunas apps como Element tienen activado por defecto el cifrado de extremo a extremo, pero puede desactivarse para la compatibilidad con clientes más antiguos.

2B **C6** DE **D5** 12
CF **B0** 69 **10** 56
8C **FB** 1D **8F** 60
B5 **03** 1D **60** B5

Figura 1: Código QR y Huella Dactilar

La seguridad del cifrado de extremo a extremo depende de la verificación de las claves intercambiadas, la cual se realiza a menudo por escanear códigos QR que contienen una huella dactilar que es estadísticamente única para la clave generada. Algunas apps requieren que verifiques solo una sola huella dactilar para todos los dispositivos, pero otras requieren que verifiques una huella dactilar para cada dispositivo. Algunas apps te envían una notificación en la conversación para informarte cuando la huella dactilar de tu contacto se cambia, lo que podría significar algo nefasto. Desafortunadamente, otras apps no lo hacen. **Debes verificar** todas las huellas dactilares para todos los dispositivos, y si una huella dactilar se cambia, **debes volver a verificarla**. Si no, toda tu seguridad podría ser anulada. Además,

[18] Existen apps de chat más interesantes tales como Briar y Cwtch que protegen contra la fuga de los metadatos y poseen otras propiedades de seguridad interesantes, pero no se usan ampliamente. Además, no están disponibles para iOS, lo cual impide a la mayoría de los grupos usarlas para la comunicación segura.

en la habitación contigua.

Análisis

Es cierto que los teléfonos podrían haber sido infectados con un malware y también podría ser cierto que mover los teléfonos a otra habitación impide que sus micrófonos graben la conversación. En cualquier caso, estamos suponiendo la efectividad de mover los teléfonos a la habitación contigua, algo que podría ser fácilmente comprobado si comenzamos a grabar con un teléfono dentro de una caja y después tenemos una conversación en voz alta en la habitación de al lado para verificar si se entiende lo que se ha grabado. Si las voces son mínimamente reconocibles podrían recuperarse pedazos de conversación con software de edición de audio.

Si el centro social no se registra en busca de micrófonos regularmente las conversaciones pueden ser grabadas de todos modos. Si el grupo u otros grupos que frecuentan el local están fuertemente vigilados las conversaciones pueden ser grabadas mediante micrófonos láser instalados en los edificios cercanos.

Si los individuos están bajo vigilancia pasiva, la existencia de una asamblea y sus asistentes podría ser revelada por la presencia recurrente del mismo grupo de teléfonos en la misma localización a la misma hora.

Recomendaciones

Si los teléfonos se recolectan para prevenir la vigilancia, también deberían apagarse. Debería haber un sonido ambiente ruidoso donde se coloquen los teléfonos para minimizar las probabilidades de que capturen audio de las conversaciones.

Si el grupo cree que pueden ser buscados por conspirar para cometer un crimen quizá quieran dejar sus teléfonos en casa o apagarlos antes de trasladarse a la asamblea. Estas medidas pueden mejorarse incluso si no se llevan los mismos teléfonos a la acción en sí.

Si se desea una alta seguridad se puede reducir la probabilidad de vigilancia reuniéndose en localizaciones que no estén relacionadas con movimientos de liberación. Si el grupo quiere reunirse en una localización central y conocida por conveniencia, se debería establecer al inicio de la reunión que sólo se discutirá de la acción actual (y nada más ilegal que eso).

Caso 2: Cháchara Descubierta

Escenario

Algunos miembros de un grupo de afinidad han quedado en un parque para socializar, no para planear una acción. Sus teléfonos están presentes y encendidos, pero su cultura de la seguridad incluye no discutir acciones pasadas o intercambiar batallitas ya que éstas pueden contener información que los incrimine.

Supuestos

El grupo ha asumido que la policía sólo quiere escuchar sus conversaciones si éstas van sobre actividades ilegales pasadas o futuras. Han asumido que sus conversaciones diarias no son interesantes ni informativas.

el orden del día de tu asamblea accesible de forma analógica. También te permite tomar nota de nuevos contactos y, si eres avispado, puedes llevar a mano una copia de tu clave pública criptográfica para establecer un canal seguro de comunicación incluso sin llevar el móvil encima. Un calendario de papel te permitirá agendar eventos. Imprimir mapas del área de una acción hará que puedas orientarte durante la misma. Si creas copias de papel de cualquier información, asegúrate de que te deshaces de ellas de manera adecuada para evitar dejar, literalmente, un rastro de papel de tus actividades.

Imprevistos sin teléfono

Aunque tu plan puede que funcione hoy, hay que seguir pensando. Puede que confíes mucho en tu teléfono para organizarte mientras aceptes los riesgos de seguridad, pero quizá llegue un momento en el que la represión o una catástrofe desactive vuestros teléfonos o el internet. Es frecuente, en momentos represivos álgidos, que el Estado corte el servicio de telefonía móvil o internet de regiones enteras. Si vuestra capacidad de organizarte y tu seguridad se basa en que casi todos tengáis teléfonos e internet funcional os estáis preparando para ciertos tipos de fracaso. El boca a boca y el llamado sneakernet[22] son planes B y vuestro plan necesita incorporar la posibilidad de que esta sea la única manera de mover información.

Casos de estudio

Para concretar acerca de las discusiones anteriores, proporcionamos una serie de casos de estudio sacados de nuestras experiencias. Algunos de ellos muestran individuos que ya tienen un modelo de amenaza más concreto y otros no. Algunos están basados en leyendas urbanas y otros más en hechos verificables o conjeturas muy probables. Donde hay errores, éstos se discuten.

Caso 1: Planear asambleas para una acción semi-pública

Escenario

Un colectivo planea una okupación que se mantendrá en secreto hasta que empiece, después de lo cual se hará pública en las redes sociales. La planificación se lleva a cabo principalmente en reuniones presenciales en el centro social local.

Supuestos

El colectivo supone que la policía está interesada en prevenir okupaciones y los activistas podrían estar bajo vigilancia. Esta vigilancia incluye, pero no se limita a, malware usado por el estado que podría estar infectando los teléfonos de los participantes en la acción.

Contramedidas

Para prevenir que el estado pueda grabar la asamblea usando los micrófonos de los teléfonos, los teléfonos se recolectan y se ponen en una bolsa de plástico sellada

[22] *N. del T.*: Se denomina así a las formas de mover información físicamente mediante soportes de memoria como USBs, discos, etc. en lugar de a través de internet.

algunas apps de chat no comparten los dispositivos que has verificado con tus otros dispositivos, y este mal diseño requiere que verifiques cada uno de los dispositivos de tus contactos desde cada uno de tus propios dispositivos.

Uso

El mantra "solo usa Signal" se repite a menudo por los activistas, pero se basa en la falsa suposición de que todo el mundo tiene modelos de amenazas idénticos. En algunas regiones, el uso de Signal es bloqueado por los *firewalls* nacionales, o su uso es tan infrecuente que usarlo puede marcar a un usuario como sospechoso. En Norteamérica y Europa, estas desventajas por lo general no existen. Sin embargo, hay muchas quejas contra Signal tal que requiere un número de teléfono para registrarse, y esa lista de contactos es compartida con el servidor de manera semi-segura para permitir el descubrimiento de contactos y el intercambio de claves inicial.

Para la mayoría de las apps, al recibir un mensaje, es descifrado y almacenado en un texto plano en el dispositivo. Algunas apps como Signal te permiten establecer una contraseña para evitar el acceso al mensaje mientras otra persona está usando tu teléfono, pero esta función no vuelve a cifrarlas de ninguna forma. Si el cifrado de dispositivo es activado en tu dispositivo, se recupera parte de tu privacidad sobre estos mensajes, como se explicó anteriormente en la sección de "cifrado de dispositivo."

Como los mensajes son almacenados en texto plano, y dado que podrían ser recuperados incluso con el cifrado de dispositivo, probablemente querrás activar los mensajes que desaparecen. En algunas apps, una de las partes puede activar los mensajes que desaparecen para todos los miembros del chat. En otras apps, cada una de las partes deben activar los mensajes que desaparecen para asegurar que todos los mensajes desaparezcan eventualmente. Puede ser inconveniente tener activado los mensajes que desaparecen puesto que la búsqueda de una imagen, un archivo, o alguna decisión solo es posible hasta cierto punto, como dentro de una semana o un mes. Sin embargo, esto es preferible a tener un registro de varios años de todo lo dicho y pensado y, en particular, todos los lugares que has estado.

Esto significa que debes preferir firmemente las apps de chat de texto y voz que tienen el cifrado de extremo a extremo obligatorio, a menos que haya una razón de seguridad convincente para no hacerlo. Por último, debes verificar las claves antes de enviar mensajes, y probablemente deberías activar los mensajes que desaparecen.

No "solo uses Signal"

Varias organizaciones de privacidad además de activistas preocupados hicieron un excelente trabajo de promover la adopción de Signal entre los activistas y también el público en general. Posiblemente hicieron un trabajo *demasiado* bueno, considerando que muchas personas lo malinterpretaron como "si usan Signal, están totalmente seguros." Esto ha llevado a que algunas personas hablen de cosas de las que absolutamente no deben hablar a través de medios electrónicos y luego suponen que está bien porque usaron Signal. Todas las contramedidas de seguridad vienen con una serie de supuestos y entendimientos, y con eso, puede haber un riesgo acep-

tado o cosas que están fuera de nuestro alcance. Signal es muy bueno en prevenir el uso por parte del estado de la vigilancia masiva para leer los mensajes. Incluso oculta algunos pero no todos los metadatos. Otras apps de chat tienen un modelo de amenazas más o menos similar. Sin embargo, si tu teléfono se ve comprometido por el malware porque llamaste la atención o tuviste mala suerte, Signal no evitará que se lean tus comunicaciones.[19]

Figura 2: Editor de Métodos de Entrada y Candidatos de Pinyin

Para algunos idiomas, en particular los basados en los caracteres más que en las letras, se utiliza un Editor de Métodos de Entrada (IME) para convertir secuencias de letras latinas en los caracteres del idioma de destino. Suelen ser aplicaciones de terceros. Signal falla en advertir adecuadamente a los usuarios que usan IMEs sobre la posibilidad de que sus chats puedan ser leídos por el *software* y reportados al Estado antes de que los mensajes sean cifrados.

Signal no es una garantía de la seguridad. No lo trates como si la fuera. Lo mismo aplica para cualquier app de chat cifrada de extremo a extremo.

Aunque tenemos fuertes críticas para Signal, esta crítica es motivada por la popularidad de Signal y las ideas erróneas al respecto; pero en el momento de escribir este texto, sigue siendo una de las pocas apps de chat cifradas que se puede confiar para obtener una seguridad sólida.

Correo electrónico

Hay formas de hacer que la comunicación por correo electrónico sea más segura, pero el correo electrónico como protocolo y medio de comunicación no suele ser seguro para las comunicaciones privadas. Los proveedores de correo electrónico que son amigables para los activistas (es decir, no Gmail/no Microsoft, etc.) no ofrecen ventajas de seguridad significativas contra la interceptación por parte de las autoridades o los hackers. Al enviar un correo electrónico, algunas personas usan PGP o S/MIME, pero estas son difíciles de usar y en general tienen una pobre experiencia de usuario. Dos personas que usan estos métodos de cifrado pueden tener una protección bastante buena contra la lectura de sus correos electrónicos, pero un clic por error puede enviar la historia entera de la conversación en texto plano, haciéndola así visible a las autoridades. ProtonMail ha hecho audaces afirmaciones acerca del cifrado de sus correos y clientes, y muchos activistas han interpretado

[19] Además, algunas personas tienen prácticas de seguridad terribles, como unirse a muchos grandes grupos de chat de Signal y hablar de sus acciones sin investigar quién más está en el grupo. No importa lo bueno que sea el cifrado si uno de los miembros del grupo es un infiltrado o un soplón.

- Usa preferentemente aplicaciones de mensajería con cifrado de extremo a extremo para comunicarte, activa la desaparición de mensajes y evita el email sin cifrar.
- Usa una contraseña para desbloquear tu teléfono y activa la encriptación del dispositivo.
- Desactiva el desbloqueo por huella dactilar de tu teléfono antes de ir a dormir o dejarlo por ahí.
- Haz una copia de seguridad de las fotos y otros datos sensibles de tu teléfono a un dispositivo encriptado y elimínalos del teléfono.
- Elimina los datos antiguos: Mensajes directos, grupos de chat, emails, eventos en calendarios, etc.
- Sal de los grupos de chat que ya no necesites y elimina a los miembros de grupos que no sean necesarios.
- Habitúate a dejar el teléfono en casa o apagarlo cuando vas a hacer pequeños recados o acciones para acostumbrarte a su ausencia.
- Empieza todas las reuniones estableciendo si los aparatos electrónicos están o no permitidos. Si no, apágalos, recoléctalos y ponlos fuera del alcance de vuestra conversación.

Y más importante:

> **No envíes mensajes o hagas llamadas de voz donde hables de temas sensibles. No fotografíes o filmes cosas incriminatorias. No crees pruebas que puedan ser usadas contra ti o contra otros.**

Sujeto a revisión

Lo que se escribe aquí, así como en el resto del fanzine, son recomendaciones. Puede que no se apliquen a tu caso. La seguridad digital, en concreto, puede dejar rastros especialmente llamativos. Si Signal es muy poco común en tu región, su uso puede convertirte en un objetivo. Las VPNs pueden ser criminalizadas. El uso de Tor puede acarrearte una visita de la policía. La presencia de aplicaciones de comunicación segura en tu teléfono puede convertir tu arresto en una desaparición. Antes de descargar cualquier cosa investiga acerca de la represión en tu región para determinar si las recomendaciones que te proporcionamos te harán estar más seguro o si te pondrán más en riesgo.

Alternativas

Es siempre más fácil decir “haz esto en vez de lo otro” en lugar de decir “no hagas eso” y, cuando estás intentando cambiar comportamientos o prácticas, proporcionar alternativas incrementa las posibilidades de que alguien deje aquel viejo e inseguro hábito. Hay razones legítimas para tener teléfonos, y las alternativas pueden aliviar la carga de tener que dejar de usarlos o cambiar nuestros hábitos.

Las barreras a la hora de librarnos de los teléfonos son que la gente quiere tener, intercambiar y reunir información. Un lápiz y un bloc de notas te permiten tener

la acción sin usar teléfonos en absoluto. Para dejar claro a otra gente que los teléfonos quemables deben tener estas propiedades, evita usar el término "teléfono quemable" y utiliza teléfono para manis o teléfono desechable en su lugar cuando sea adecuado.

Degradación elegante

Este zine se centra principalmente en debatir las características ideales del uso de teléfonos seguro, pero a menudo estas ideas no se pueden seguir. Un ejemplo es cuando os organizáis con gente que no se puede permitir un smartphone. Conseguir teléfonos simples y baratos para organizar una acción, o incluso para coordinar reuniones regulares, puede ser mas fácil y económicamente gestionable que hacer lo mismo con smartphones. Por desgracia, la falta de aplicaciones encriptadas tanto para voz como para chat significa un incremento de la vigilancia para vuestras comunicaciones.

Para prevenir que el Estado pueda adquirir demasiada información sobre vuestras acciones tendréis que confiar en soluciones humanas antes que en soluciones técnicas. Un acuerdo acerca de discutir la hora y el lugar de las reuniones siempre con la mínima cantidad de detalles e información puede reducir la información reunida por el Estado al mínimo. Un libro de códigos para reemplazar frases frecuentes usadas al organizarse por códigos aleatorios e inocuos puede crear confusión si alguien intenta investigar. Además, el uso de códigos puede evitar que los sistemas automáticos alerten a las autoridades.

El uso de patrones como estos os permite degradar vuestra seguridad de forma elegante de alta seguridad a baja seguridad sin exponeros completamente a la vigilancia y la represión del Estado. Estos métodos requieren gran cuidado, pero son factibles.

Haciendo un plan

No podemos saber a qué tipo de amenaza te enfrentas, ni tampoco detenernos en cada pequeño matiz de cada región y situación. Lo que sí podemos hacer es una lista de recomendaciones que son generalmente aplicables. Cuando las leas tienes que considerar qué es más práctico para tí. Qué puedes hacer realmente? Y qué hará la gente de tu círculo? Tu nuevo plan no tiene que ser perfecto, solo tiene que ser mejor que lo que sea que haces ahora. Si esto significa comprometerse en temas de seguridad para poder seguir organizándote, quizá tengas que hacerlo. Pero al mismo tiempo no dejes que la poca seguridad de otras personas te ponga en peligro. Encuentra un equilibrio.

Esto no es para nada una lista exhaustiva, pero son formas de desarrollar Seguridad Operacional personal y cultura de la seguridad grupal:

- Usa un smartphone ya que son más seguros que los móviles simples contra la mayoría de las amenazas a las que se enfrentan los activistas.
- No lleves tu móvil a actividades que puedan interesar a la policía, especialmente a protestas que puedan acabar en alborotos.

estas verdades a medias como que el uso de ProtonMail significa que todos sus correos son cifrados, pero este no es el caso. Por lo general, debe evitarse el correo electrónico para la planificación y, sobre todo, para la comunicación segura.

Dicho esto, el correo electrónico mantiene su popularidad porque cada dispositivo puede enviar y recibir un correo electrónico, y algunas personas no usan los apps de chat. Para organizar un sindicato de inquilinos o establecer turnos para un Infoshop, el correo electrónico probablemente está bien. Si optas por usar email, debes asumir que la policía está leyendo todos los mensajes y reducir las conversaciones al mínimo. No hables de la actividad ilegal. No hables del drama de la escena que puede ser aprovechado por el Estado.

Por último, hay casos de uso legítimos en los que el correo electrónico y PGP se utilizan como último recurso para establecer un segundo canal más seguro para alguien en la clandestinidad. En casos como este, los teléfonos todavía deben ser evitados, dado su rastreabilidad.

Alias múltiples, teléfonos múltiples

Dependiendo de tu modelo de amenaza, puedes elegir mantener varios teléfonos vinculados a a tus varios alias. Por ejemplo, podrías tener un teléfono vinculado a tu vida pública en el status quo con las cuentas de redes sociales que usas para conectar con tu familia y un segundo teléfono con una SIM separada y cuentas vinculadas a tu vida activista. Esta separación de cuentas es parte de un proceso llamado compartimentación.

El principal beneficio es que el uso de diferentes dispositivos para cada uno de tus alias previene que errores del usuario o de programación expongan tu información privada. Las aplicaciones de tu teléfono pueden tener comportamientos inesperados como enviar una invitación para conectar a todos tus contactos cuando descargas una nueva app de mensajería. Puede que respondas por error a un post en redes sociales desde la cuenta equivocada. Al hacer click en una dirección de email con la intención de usar uno de tus alias, el sistema operativo de tu teléfono quizá te lleve a escribir un email en el cliente de email por defecto con un alias diferente.

El segundo beneficio es que el dispositivo que uses para activismo puede ser mínimo y solo usarlo para comunicaciones seguras. Cada aplicación que instalas es una posible ruta de entrada para malware, por lo que si tu teléfono apenas tiene un sistema operativo y dos aplicaciones de chat es más difícil de comprometer.

Usar diferentes teléfonos por sí mismo no evita que las fuerzas de la ley sean capaces de vincular tus diferentes alias. Si llevas los teléfonos al mismo tiempo o bien los usas en los mismos lugares podrían ser vinculados.

Como alternativa a utilizar múltiples teléfonos puedes reducir el riesgo de filtrar datos por error o comportamiento inesperado creando múltiples perfiles en tu dispositivo Android. Esto no te protegerá contra el malware, pero ofrece alguna protección.

Uno de los casos de uso más comunes de los teléfonos múltiples es para organizar un sindicato. Algunas empresas obligan a instalar aplicaciones para la gestión

remota como forma de proteger la propiedad intelectual corporativa o mitigar las brechas de seguridad. Estas aplicaciones son software espía y pueden controlar completamente tu teléfono. Aparte de esto, muchas empresas requieren una aplicación de chat específica para comunicarse. Deberías evitar organizarte en dispositivos de la empresa o con su software espía instalado, además de evitar el chat de la empresa para intentar organizar un sindicato.

Teléfonos para manis, desechables y quemables

Mucha gente entiende la importancia de sus teléfonos y saben que pueden ser rastreados por ellos o que su pérdida o compromiso pueden ser devastadores. Los activistas (y no solo ellos) usan toda una serie de tácticas para ayudar a reducir su riesgo incluso si no pueden definir bien ese riesgo o por qué sus contramedidas funcionan.

Algunas personas tienen teléfonos para manis o desechables que se llevan a acciones o cuando cruzan fronteras. Estos aparatos tienen el mínimo de datos privados en su interior y se consideran inseguros (debido a la posible instalación de malware) si las fuerzas de seguridad han tenido acceso a ellos. Estos teléfonos no se usan con fines de anonimato. Podrían compartir SIM con el teléfono habitual del usuario y podrían usarse de forma que la geolocalización los vincule con la vivienda del usuario. Los teléfonos para manis tienen menos datos y cuentas disponibles para la policía si ésta los captura. No hay necesidad de que un teléfono para manis o desechable sea un teléfono simple. En muchos casos son smartphones porque esto permite al usuario usar mapas y comunicaciones encriptadas de extremo a extremo.

Algunos activistas usan erróneamente la frase "teléfono quemable" para describir teléfonos de mani, desechables o cualquier teléfono simple.[20] Un teléfono quemable toma el nombre del hecho de que es de un sólo uso y después es destruido. Son el tipo de teléfono adecuado cuando el usuario necesita tener comunicación móvil durante el tipo de acción que lleva a una enorme y certera investigación como respuesta.

Para que un teléfono sea quemable necesita cumplir estos criterios:

1. El teléfono debe ser comprado[21] utilizando dinero en efectivo.
2. La SIM usada en el telefono quemable debe ser comprada usando dinero en efectivo.
3. El teléfono y la SIM deben ser compradas por un usuario que no tenga otros teléfonos o aparatos rastreables encima en el momento de la compra.
4. El teléfono y la SIM sólo deben ser usados el uno con el otro.
5. El teléfono nunca debe ser llevado a localizaciones asociadas con el usuario a no ser que esté apagado y dentro de una bolsa de Faraday.

[20] Parece que la gente usa la frase "teléfono quemable" porque suena super ilegal y mega criminal y no porque estén describiendo realmente las propiedades de un teléfono quemable.

[21] El robo de teléfonos con una SIM activada generalmente es poco recomendable ya que cada robo crea una localización que puede ser vinculada con la acción, los teléfonos tal vez no puedan ser desbloqueados y el dueño quizá tiene el aparato añadido a una lista de denegación de servicio y no podrían ser usados para hacer llamadas o usar datos.

6. El teléfono nunca debe ser usado en presencia de otros teléfonos que no sean quemables u otros aparatos que puedan ser rastreados hasta el usuario o sus socios.
7. Cualquier cuenta en el teléfono debe hacerse anónimamente, debe usarse sólo en ese teléfono y no volver a usarse jamás.
8. El teléfono debe ser usado exactamente en una sola acción.
9. El teléfono debe contactar únicamente con otros teléfonos quemables o terceras partes no relaccionadas (por ejemplo una oficina o adversario objetivo de la acción).
10. El teléfono y la SIM deben ser apagados después de la acción y destruidos inmediatamente.

Un factor que complica las cosas es que algunos teléfonos o tarjetas SIM necesitan activarse llamando a un número específico o accediendo a la web del proveedor. A veces estas webs bloquean conexiones a través de Tor. Usar un teléfono no quemable para activar la SIM es, obviamente, una vulneración de su seguridad. Quizá necesites buscar un teléfono de pago o usar la ingeniería social para hacer que un extraño en una estación de tren te deje su móvil por unos minutos.

Cuando decimos que un teléfono quemable puede ser usado para una acción quiere decir "una sucesión de actividades acotadas en el tiempo." Esto puede significar una acción directa que tiene lugar a lo largo de dos horas, pero también la planificación y coordinación en el mes anterior a una acción además de la acción en si.

Si se tiene especial cuidado, un grupo de afinidad cerrado puede reutilizar sus teléfonos quemables para acciones recurrentes. En este caso los teléfonos tienen que ser usados de forma de lotes cerrados que no se sobrepongan unos sobre otros en los diferentes ciclos.

Una norma que no es obligatoria, pero sí bastante recomendable, es que los teléfonos quemables no deberían comprarse inmediatamente antes de una acción. Esto crea la posibilidad adicional de que los vídeos grabados por las cámaras de seguridad estén aún accesibles en el momento de la acción.

Intentar ofuscar la existencia de un ciclo cerrado entre los teléfonos puede ayudar a prevenir la detección del grupo de afinidad. Uno de los pasos a seguir sería no activarlos todos en poco tiempo. La activación gradual es menos detectable cuando el Estado analiza los datos. También hacer unas cuantas llamadas desde localizaciones aleatorias a números que la gente llama comúnmente, pero **no hablar** si alguien contesta, o llamar a números con largos períodos de espera como bancos o aseguradoras, llamar a tiendas locales antes de que abran o después de que cierren… Aunque todas estas llamadas falsas tal vez sean innecesarias ya que muchos usuarios en algunas regiones nunca hacen llamadas y simplemente usan su plan de datos para todo.

Debido al cuidado con el que un teléfono quemable debe ser adquirido y usado, es muy poco probable que valga la pena usar uno. Si creéis que vuestra acción necesita un teléfono quemable, seguramente deberíais encontrar la manera de hacer