21

Cuando la realidad supera a la ficción

Aprender nociones avanzadas sobre seguridad operacional, anonimato o privacidad no es una tarea fácil. La mayoría de las personas no se encuentran en una posición que les obligue a preocuparse por adquirir estos conocimientos. En los casos en los que adquieren paulatina o repentinamente una posición donde estas disciplinas cobran relevancia, pueden aprender lo que necesitan a partir de otras personas en su misma situación o delegar este conocimiento contratando algún servicio de protección personal. Pero adquirir ese conocimiento a posteriori puede resultar peligroso. **En el mundo digital la seguridad operacional no funciona retroactivamente.** Además, como ya mencionamos en el capítulo anterior, la literatura sobre buenas prácticas en este campo podría ser considerada un manual para no acabar en la cárcel. Es esperable que los delincuentes de éxito no cuenten sus secretos, pero cabría esperar que personajes como los presentados en el capítulo anterior sí compartieran con el mundo sus lecciones aprendidas. La realidad es que, en la mayoría de los casos, los buenos tampoco comparten sus estrategias de ciberdefensa.

A lo largo de los años en el mundo civil, mucho de lo que parece haberse aprendido en términos de seguridad operacional, anonimato y privacidad está basado en las pocas historias que han salido a la luz. Estas pueden tratar sobre operaciones militares que han ido mal, evidencias de misiones de espionaje y contraespionaje, filtraciones de topos a la prensa o procesos judiciales donde se detalla cómo las fuerzas de seguridad consiguieron detener a un criminal y cuáles fueron sus errores. La mayoría de los secretos a aprender están ocultos entre las

líneas de estas historias. En ocasiones los buenos exhiben orgullosos los detalles de sus técnicas a la hora de encontrar al sospechoso de un crimen [205], en otros casos, se mofan de algún error clamoroso que cometió [206]. Otros delincuentes esquivaron condenas y sus historias pueden esconder detalles interesantes y menos obvios sobre qué hicieron bien. Extraer aprendizajes prácticos de todos estos ejemplos puede resultar difícil sin estar en la sintonía adecuada. El objetivo de este capítulo es despertar esa sensibilidad en el lector presentando una selección de hechos históricos.

Los metadatos de Milán y Beirut

En febrero de 2003 como parte de las campañas posteriores a los atentados de las Torres Gemelas, un operativo de la CIA secuestró en Milán a Abu Omar, un sospechoso de pertenecer a grupos terroristas [207]. La operación se realizó utilizando prácticas clandestinas de captura y extracción diseñadas para sortear las leyes italianas [208]. Esta operación no pasó desapercibida para las autoridades locales, quienes consiguieron identificar a 22 agentes encubiertos de la CIA que participaron en el secuestro únicamente partiendo del testimonio de una mujer que pudo ver cómo Abu era introducido contra su voluntad en una furgoneta.

El testimonio de esa mujer proporcionó un lugar, una hora y una fecha al equipo italiano que investigó la desaparición. A partir de esta información los investigadores solicitaron los datos de las torres de telefonía móvil de la zona y comenzaron a analizar los metadatos. Estas fuentes aportan información muy detallada tanto de las llamadas y movimientos de las tarjetas SIM de cada línea telefónica, como de los dispositivos donde están insertadas (usando los llamados códigos IMEI[209]). Mediante el análisis de estos datos asociados a las zonas de interés que rodeaban el trayecto diario de Abu, pudieron identificar 30 teléfonos que únicamente hablaban entre sí y que formaban un grupo aislado. A partir de información de otras torres, analizaron por dónde se movían los dispositivos e identificaron los posibles hoteles donde sus

propietarios dormían tras observar los lugares donde los teléfonos se mantenían en reposo por las noches.

De esta forma los agentes del operativo fueron identificados utilizando exclusivamente metadatos generados por sus teléfonos móviles. Una investigación posterior reveló que, aunque los agentes habían sido entrenados para desconectar periódicamente de la red los dispositivos utilizando unos sobres a modo de jaulas de Faraday[210], en su lugar habían utilizado bolsas de Doritos pensando que proporcionaban el mismo nivel de aislamiento electromagnético [211]. Además, aunque algunos de los agentes utilizaban tarjetas SIM limpias cuando llamaban al cuartel general para recibir órdenes, al reutilizar los dispositivos móviles donde se insertaban estas tarjetas SIM las fuerzas italianas pudieron conectar las SIM limpias con las otras que participaron en la operación a través de los códigos IMEI de los dispositivos. Estas comunicaciones con oficiales del entramado diplomático de EEUU en Italia permitieron demostrar la conexión gubernamental de la operación.

Este no es el único ejemplo. Otras operaciones en suelo extranjero se han expuesto también a partir de los metadatos telefónicos. En 2011 el grupo Hezbolá reveló en la televisión pública la identidad de 10 oficiales de la CIA que operaban de manera secreta en suelo libanés [212]. En la inmensidad de los flujos de comunicaciones telefónicas, buscaron teléfonos que tuvieran comportamientos anómalos. Por ejemplo, dos teléfonos que únicamente hablaran el uno con el otro, una vez al mes, durante 2 minutos, o una vez a la semana durante 30 segundos. Esto les permitió comenzar a cerrar el círculo sobre potenciales sospechosos dentro de la inmensidad del mar de llamadas telefónicas del país.

Estas historias demuestran la criticidad que los metadatos pueden tener para nuestra privacidad, y cómo pueden hacer irrelevante la necesidad de acceder al propio contenido de nuestras llamadas. Nuestros patrones de movimiento y actividad dicen mucho sobre nosotros. Y nuestros teléfonos están constantemente enviando esa información a la red.

La era Post-Snowden

La creencia de que los gobiernos siempre han podido acceder a información privada de sus ciudadanos se acompañaba con la confianza en que esto únicamente sucedía bajo unas reglas del juego justas y legales. La revolución digital trajo consigo que muchos de nuestros datos privados acabaran cruzando fronteras y jurisdicciones, pero siempre habíamos mantenido una cierta confianza en que nadie podía acceder libremente a nuestra información privada sin el permiso de un juez o algún otro amparo legal. Todas estas creencias se hicieron trizas en el año 2013 tras las denominadas *Revelaciones de Snowden* [213].

En junio de 2013, Edward Snowden, un contratista que trabajaba para la agencia de seguridad nacional de EEUU (la NSA), filtró más de cincuenta mil documentos clasificados a un grupo de periodistas en Hong Kong. Diversos medios de comunicación de todo el mundo obtuvieron acceso a los documentos y comenzaron a publicarse detalles sobre la existencia de una red de vigilancia mundial en la que participaban los países miembros de la alianza de los *Five Eyes* (Australia, Canadá, Estados Unidos, Reino Unido y Nueva Zelanda). La información contenida en estos documentos cambió para siempre la visión pública de los esfuerzos de los gobiernos para obtener visibilidad sobre toda la actividad digital dentro y fuera de sus fronteras.

Algunas de las herramientas utilizadas por estos programas de vigilancia global cuyos detalles trascendieron fueron las siguientes:

- PRISM era un conjunto de herramientas que permitían acceder a datos de grandes proveedores como Google y Apple. A tan solo un puñado de clics de distancia los analistas de la NSA tenían a su disposición, por ejemplo, el acceso al buzón de correo de cualquier usuario de Gmail. Si bien estaba estipulado que para poder acceder era necesaria una orden judicial, el acceso a las cuentas de personas que no eran ciudadanos estadounidenses no lo requería y únicamente exigía incorporar un mensaje justificando la necesidad de acceso. Así,

una herramienta diseñada por los proveedores para facilitar el pinchazo dirigido de correos de ciudadanos bajo una orden judicial permitía abusar de accesos indebidos a las cuentas de ciudadanos extranjeros sin ningún contrapeso legal.

- TEMPORA y MUSCULAR eran programas fruto de la colaboración entre la NSA y GCHQ (el equivalente a la NSA en Reino Unido) orientados a pinchar canales de comunicación físicos (cables) de grandes operadores. La posición estratégica de Reino Unido y otros aliados como puntos de conexión de las rutas terrestres con los cables submarinos de comunicación global permitió la instalación de dispositivos para pinchar las fibras ópticas de estos cables. Otras veces, estos pinchazos tenían lugar dentro de los propios centros de datos de los grandes proveedores de servicios tecnológicos como Google o Yahoo!. Mediante la intercepción de este tipo de canales de comunicación las agencias de seguridad tenían acceso a ingentes cantidades de tráfico sin cifrar o a la capacidad para extraer metadatos de tráfico cifrado de manera selectiva [214].

- XKEYSCORE era una base de datos distribuida que permitía a los analistas explotar de manera muy eficiente la inmensidad de información que otras herramientas habían capturado previamente. Un usuario de XKEYSCORE podía lanzar una pregunta del tipo: «mi objetivo habla italiano, pero vive en siria» o «hazme una lista de todas las personas que han enviado emails con un adjunto cifrado en el último mes». Al igual que PRISM, cuando en los resultados aparecía alguna persona de nacionalidad estadounidense y no se contaba con autorización judicial, el analista únicamente debía introducir una razón por la cual tenía sospechas de que esta persona podía ser una amenaza para el estado. Como casi siempre, bajo la excusa de estar combatiendo el terrorismo, los sistemas se abrían a abusos de todo tipo. La potencia de esta base de datos era tal que permitía establecer huellas únicas sobre determinadas personas y seguir

su rastro por todo el mundo. Estas capacidades condujeron de manera práctica a la captura de cientos de terroristas. Algunos de ellos fueron localizados y espiados gracias a que buscaron en Google su propio nombre, sus apodos, el de un compañero o el título de su propio libro [215].

- Otras prácticas evidenciadas por los papeles filtrados incluían la instalación rutinaria de micrófonos y antenas en edificios objetivo o la intercepción de envíos de equipamiento electrónico para su manipulación, previo reenvío a su destino. En 2024, manipulaciones de este tipo por parte del Mossad para hacer explotar en masa los buscapersonas utilizados por Hezbolá evidencian que estas prácticas continúan siendo utilizadas [216].

- También se mostraba el uso de vulnerabilidades Zero Day para comprometer los dispositivos de sospechosos previamente identificados gracias a XKEYSCORE. En una ocasión, con el objetivo de obtener acceso a los servidores de un proveedor de conexiones a internet (Belgacom), el GCHQ primero localizó mediante XKEYSCORE a uno de los administradores de la compañía con acceso a sus servidores. Después, utilizando LinkedIn como medio de contacto, le envió un enlace que comprometió su dispositivo mediante una vulnerabilidad no parcheada. Una vez su dispositivo podía controlarse remotamente, robó sus credenciales y accedió a los servidores del proveedor de internet para llevar a cabo sus objetivos [217]. Este modus operandi de atacar a administradores privilegiados pudo observarse también en el compromiso de la firma Gemalto, el mayor proveedor de tarjetas SIM del mundo. La obtención por parte de GCHQ y la NSA de las claves privadas utilizadas por estas tarjetas permitió interceptar el tráfico de cientos de millones de teléfonos móviles [218].

- La acumulación en secreto de información sobre

vulnerabilidades sin informar a los desarrolladores afectados se evidenció como una práctica habitual por parte de estas agencias. Bajo el pretexto denominado *Nobody but us* (NOBUS, traducido como «Nadie excepto Nosotros») [219] se identificaba un tipo de vulnerabilidad o abuso potencial de un software cuya utilización se consideraba únicamente al alcance de agencias de seguridad nacional. Esta limitación se daba por una combinación de recursos necesarios (considerados sólo al alcance de grandes presupuestos gubernamentales) y conocimiento del detalle de las vulnerabilidades. El resultado era que cuando una agencia descubría la existencia de uno de estos fallos, lo mantenía en secreto en lugar de informar a los desarrolladores para que lo corrigieran. Quizá el ejemplo más sonado de estas prácticas trascendió con una famosa vulnerabilidad publicada en 2014 bajo el sobrenombre de *Heartbleed* [220]. La gravedad de esta vulnerabilidad obligó al mundo entero a movilizarse para parchear en tiempo record todos los sistemas afectados. Posteriormente, según fuentes internas anónimas, se supo que la NSA conocía y llevaba años utilizando esta vulnerabilidad en sus operaciones [221].

Snowden mostró la ubicuidad y profundidad de estos programas de vigilancia, pero también la falta de transparencia y el abuso al que sus herramientas podían ofrecerse. Estas filtraciones mostraron cómo las agencias de inteligencia violaban de manera constante el derecho a la privacidad de personas, sin garantizar las autorizaciones judiciales previas y sin considerar las implicaciones de mantener secretas las vulnerabilidades utilizadas. Con la excusa de luchar contra el terrorismo y los enemigos del estado, otras víctimas como periodistas, activistas o ciudadanos extranjeros se veían rutinariamente espiados sin salvaguardar sus derechos y la legalidad vigente. Aunque estas revelaciones generaron ciertas reformas y debates sociales sobre la necesidad de desarrollar programas de vigilancia más garantistas con los derechos de los ciudadanos, muchos de estos debates todavía siguen

abiertos. Todavía se plantean retos éticos y problemas sin resolver en el ámbito del control al que aspiran los gobiernos sobre el mundo digital.

Radiografías usando lugares, amigos y likes

Incluso cuando agencias gubernamentales no se ven involucradas, el registro masivo de nuestra actividad digital y el análisis de datos a escala tiene un gran impacto en el anonimato y privacidad de las personas. En el pasado hemos conocido algunos eventos relevantes que ponen de manifiesto la fragilidad de nuestro anonimato y privacidad cuando se enfrentan a técnicas modernas de inferencia.

En 2013, un académico de Cambridge llamado Aleksandr Kogan y otros investigadores publicaron una aplicación en Facebook para autoevaluar un conjunto de cualidades de nuestra personalidad. Otros investigadores por aquella época ya se habían dado cuenta de que a partir de datos limitados como cuatro likes era posible inferir datos relevantes sobre las personas tales como su orientación sexual. Con varias decenas de likes resultaba posible averiguar con una alta probabilidad otros atributos concretos de su personalidad [222].

Esta investigación inicial originó que otras personas comenzaran a analizar a escala otros datos disponibles en Facebook y convirtieran este análisis en algo que se podría aprovechar para realizar propaganda política dirigida. Esta operación condujo a lo que se conoció como el escándalo de Cambridge Analytica, una operación en 2016 que pudo influir de manera significativa en el referéndum del Brexit y en las elecciones presidenciales de EEUU de ese mismo año [223].

Otros investigadores han publicado trabajos que muestran cómo únicamente es necesario cuatro localizaciones de una persona para poder identificarla [224]. Estas localizaciones ni siquiera necesitan ser de alta resolución y basta con su localización aproximada en base a lo que reportan las torres de telefonía móvil. Estos resultados son congruentes con lo que ya se pudo observar de manera práctica en los casos previamente comentados de Milán y Beirut. Si bien el acceso a esta información de localización aproximada basada en la red de telefonía

móvil no está al alcance de cualquiera, hoy en día los smartphones proporcionan información de localización de muchas otras formas. Aplicaciones instaladas en nuestro teléfono solicitan rutinariamente permisos de localización, que además de basarse en sensores GPS y tener mucha más exactitud, puede incluir datos de conexiones wifi cercanas. La mayoría de las personas comparte esta información con aplicaciones sin pensarlo mucho, por lo que un ecosistema floreciente de empresas recopila y revende esta información de localización de personas supuestamente anónimas. En muchos casos, estos datos permiten la completa identificación de manera práctica.

Como prueba de ello, otro ejemplo. En 2018 el gobierno de la ciudad de Victoria (Australia) publicó un fichero de datos que incluía información sobre más de 1000 millones de viajes de su red de transporte público. Los identificadores de las tarjetas de los viajeros habían sido anonimizados, pero las personas que examinaron el fichero no tardaron en darse cuenta de que bastaba buscar uno o dos viajes concretos (identificados por origen, destino, fecha y hora) para señalar qué identificador anónimo le correspondía a cada persona. Esto mismo podían hacerlo con otras personas con tan solo conocer datos sobre algunos viajes que quizá habían compartido con ellos, pudiendo entonces extraer del fichero el resto de viajes que esa persona había hecho entre 2015 y 2018 [225].

Anonimizar datos antes de ser utilizados para labores de analítica es la excusa de oro con la que se defiende habitualmente que la privacidad de las personas se mantiene a salvo. La realidad es que casi cualquier conjunto de datos de personas es extraordinariamente difícil de anonimizar bien. Por ello existe una disciplina del campo de las matemáticas dedicada específicamente a transformar datos para que resulte estadísticamente inviable extraer información adicional de ellos que pueda afectar a la privacidad de las personas [226].

Un simple error es todo lo que se necesita

Otras historias que han trascendido nos permiten conocer cómo en ocasiones nuestro anonimato no depende tanto de nuestras habilidades o herramientas como de nuestra disciplina operativa. Muchos criminales han sido pillados por pequeños deslices o por no anticiparse al escrutinio que sus acciones iban a provocar.

En 2011, Héctor Xavier Monsegur, un hacker conocido como *Sabu*, fue arrestado por el FBI. Sabu colaboró con la justicia, manteniendo en secreto su captura y continuando con sus comportamientos habituales mientras conducía al FBI hasta otros colaboradores. Hasta entonces, el grupo conocido como *lulzsec* había sido responsable de numerosos ciberataques con motivación política, incluyendo a Sony y a la CIA entre sus objetivos. De entre todos los errores cometidos por Sabu y sus compañeros, destaca el breve y único instante en el que Sabu olvidó activar su conexión anónima cuando entró al chat donde mantenían contacto con la comunidad de seguidores de lulzsec. Ese momentáneo desliz condujo al FBI a su detención posterior [227]. Con Sabu como aliado pasando información y registros de conversaciones al FBI, otros miembros de lulzsec fueron detenidos por carencias también en su disciplina de seguridad operacional. Aunque mantenían identidades falsas entre ellos, hablaban despreocupadamente del tiempo que hacía en su zona, de su nacionalidad o de otros detalles que finalmente ayudaron a su identificación.

En 2013 un estudiante de Harvard llamado Eldo Kim fue arrestado como sospechoso de enviar un aviso falso de bomba para forzar el desalojo de varios edificios y sortear así un examen al que debía presentarse. Eldo planificó el envío de los avisos utilizando un servicio gratuito de correos electrónicos sin remitente y una conexión a través de la red anónima llamada *Tor*. Esta red impide, teóricamente, la identificación desde el destino de la comunicación de la persona que la utiliza [228] . Sin embargo, la detención de Eldo no se produjo gracias al análisis de posibles debilidades en las herramientas que utilizó.

Su error fue utilizar la red wifi de la universidad para conectarse a Tor, generando así evidencia de que él se encontraba entre los pocos usuarios de dicha red anónima desde el campus. Si bien las autoridades no podían identificar quién había enviado el correo con el aviso de bomba, sí pudieron orientar sus interrogatorios a todos aquellos usuarios de la wifi del campus que habían utilizado Tor a la hora a la que el aviso fue enviado. La sorpresa por ser interrogado y la falta de preparación para ello hicieron a Eldo una presa fácil para los agentes del FBI, quienes consiguieron sacarle una confesión [229].

En el año 2020, varios agentes de la policía nacional española se infiltraron en varios grupos asociados a los movimientos independentistas catalanes. Los testimonios de algunas de las personas que mantuvieron relaciones estrechas con estos policías pusieron de manifiesto los extremos a los que estas personas llegaron para hacer sus personajes creíbles dentro de estas organizaciones [230]. De estos testimonios también ha trascendido que cuando la misión de estos agentes terminó (lo que se conoce como «extracción»), su desaparición repentina levantó sospechas y motivó una investigación interna en el entorno que habían abandonado. Una de estas investigaciones descubrió que uno de los agentes había revelado su localización de manera involuntaria en uno de sus viajes. Su personaje iba a viajar a Mallorca, pero la localización que pudo verse en el historial de direcciones IP del buzón de correo de la asociación al que tenía acceso desde su teléfono reveló que en realidad había viajado a Madrid. Además, la revisión forense de un *pendrive* que había regalado a un compañero del movimiento objetivo pudo recuperar fotos borradas en las que se veía al agente vestido de policía el día de su graduación en la academia.

Exploits y mitología griega

En 2018 el periodista Jamal Khashoggi fue asesinado en el consulado de Arabia Saudita en Estambul. Tiempo después el Washington Post publicó que la CIA daba por confirmado que la orden de eliminación

vino del príncipe heredero saudí Mohamed bin Salmán [231]. Un año después el National Enquirer publicó la noticia de que Jeff Bezos, consejero delegado de Amazon y dueño del Washington Post, estaba teniendo un *affaire* fuera de su matrimonio. Al parecer el Enquirer tuvo acceso de alguna forma a fotos íntimas de ambos amantes. La reacción de Bezos fue la de hacer todo público y contratar a un investigador forense para averiguar cómo el contenido de su teléfono móvil había acabado en manos del National Enquirer.

El resultado de las investigaciones del experto forense señaló que el móvil de Bezos había sido comprometido tras recibir un mensaje de WhatsApp del propio príncipe saudí. Este mensaje, podría haber aprovechado un Zero Day para implantar malware que permitía extraer información del teléfono de manera silenciosa [232].

Este modus operandi para obtener inteligencia de objetivos específicos abusando de vulnerabilidades (lo que se conoce como *exploits*) para instalar software de monitorización (spyware) se popularizó mucho a finales de la década de los 2010 y comienzos de los 2020. Quizá el fabricante más conocido de este tipo de herramientas ha sido NSO Group, una compañía israelí autora del spyware *Pegasus*. Este producto, proporciona un paquete completo que cubre todas las necesidades que su usuario pueda tener sobre un objetivo concreto, entre ellas el acceder a un conjunto de exploits que aprovechan diferentes vulnerabilidades. Algunos de estos exploits se basan en que la víctima pinche en un enlace recibido por SMS mientras otros pueden únicamente requerir conocer el número de teléfono del objetivo (sin requerir acción alguna por parte de la víctima). La facilidad con la que Pegasus podía ser utilizado y su efectividad se demuestra por los más de 1400 afectados que han podido ser documentados como parte de una querella interpuesta por WhatsApp contra NSO Group en 2019 [233]. La conexión de Pegasus con la historia que rodea al asesinato de Khashoggi y la filtración de Bezos también ha quedado patente tras confirmarse la infección con Pegasus del teléfono de la viuda de Khashoggi meses antes de su asesinato [234].

En los últimos años gracias a la labor investigadora de varios periodistas especializados en la materia, muchos otros ejemplos de este tipo han sido documentados. Las operaciones de vigilancia digital por medio de exploits a activistas o disidentes políticos en diversas partes del mundo son un hecho contrastado. En algunos casos, se han publicado informes detallados sobre las técnicas utilizadas y las vulnerabilidades aprovechadas por los exploits [235]. Otras investigaciones señalan también a miembros prominentes de gobiernos como víctimas de este tipo de ciberarmas. En algunos casos las investigaciones han constatado el acceso a datos sensibles por parte de los atacantes, pero en otros casos, se han cerrado en falso por falta de pruebas o indicios con los que poder seguir investigando [236].