La amenaza hacker

Deepak Daswani

Prólogo de Mikko Hypponen

Todo lo que empresarios, directivos, profesionales y particulares deberíamos saber para protegernos adecuadamente

Un hacker experto en ciberseguridad nos explica cómo evitar ataques, robos, estafas y otros peligros en la era de la revolución digital

Lectulandia

La tecnología nos ha traído toda clase de comodidades, pero también una serie de riesgos que hasta hace poco eran desconocidos para la mayoría de la gente. En los últimos tiempos, las noticias sobre incidentes de ciberseguridad son cada vez más habituales: a diario se roban millones de cuentas de correo, datos de tarjetas de crédito, credenciales de banca online y se cometen toda clase de delitos informáticos. Todo ello ha motivado que cada vez seamos más conscientes de los riesgos implícitos que conlleva nuestra dependencia de la tecnología.

En este libro, sucinto y práctico, Deepak Daswani, ingeniero y experto en ciberseguridad, analiza en detalle los riesgos a los que estamos expuestos y explica cómo podemos hacerles frente, evitándolos cuando es posible o minimizando su amenaza.

Con ejemplos y anécdotas recabados de su experiencia personal, un firme dominio técnico y una gran capacidad para transmitir con claridad, La amenaza permite comprender, incluso a quienes no disponen de conocimientos técnicos, los entresijos de la relación entre el mundo físico y el virtual.

Proporciona, además, un dominio básico para advertir las oportunidades y los riesgos del mundo digital, así como los recursos necesarios para promover buenas prácticas y fortalecer la seguridad y la privacidad en la red, tanto en nuestro uso particular como en las empresas en las que trabajamos.

Una obra, en definitiva, dirigida a todos aquellos que necesitamos conocer y saber cómo se originan las amenazas a las que todos estamos expuestos, en nuestra vida privada y en la profesional.

Lectulandia

Deepak Daswani

La amenaza hacker

ePub r1.0
XcUiDi 15.05.2019

Título original: *La amenaza hacker*
Deepak Daswani, 2018

Editor digital: XcUiDi
ePub base r2.1

A mis padres, por educarme, inculcarme principios y valores
que me han sido siempre la base de mi camino.

A Aarti y a mi *hacker* Lara, por acompañarme en este camino,
compartir y ayudarme a cumplir mis sueños.

Y a ti Ranvir, mi rey

Prólogo

Paso mucho tiempo pensando en nuestros enemigos.

Creo firmemente que la atribución de quién ha sido el atacante es una de las cosas más importantes que una organización puede hacer para protegerse. Es decir, descubrir quién está dispuesto a atraparte. Esto no es tan sencillo como podría parecer; diferentes tipos de organizaciones son blanco de diferentes tipos de atacantes. Y no tendremos ninguna esperanza de defendernos si no entendemos quiénes son los atacantes.

Los atacantes actúan por motivos muy variados, usan diferentes técnicas y eligen diferentes objetivos. Para las organizaciones es muy diferente defenderse contra un grupo cibercriminal que opera en línea tratando de obtener acceso a datos valiosos, como números de tarjetas de crédito, que proteger sus redes contra ataques de denegación de servicio distribuido lanzados por un colectivo hacktivista, o protegerse contra un ataque de espionaje lanzado por un Estado o nación hostil. Los sistemas de algunas organizaciones incluso podrían ser blanco de extremistas o grupos terroristas.

La buena noticia es que no todas las organizaciones son atacadas por todos los atacantes. La mala noticia es que nadie más puede conocer a tus atacantes potenciales tan bien como tú mismo. El trabajo de atribución del atacante es difícil de externalizar.

Todos tenemos recursos y presupuestos limitados para defender nuestras redes. Comprender al enemigo nos permite enfocarlos hacia donde más importa.

Y cuando estamos tratando de luchar contra los *hackers*, uno de nuestros mejores recursos son precisamente los *hackers*. Ya ves, necesitamos *hackers* buenos para atrapar a los malos.

Te deseo buena suerte en tu lucha contra los *hackers* malos.

MIKKO HYPPONEN

Chief Research Officer / Director de Investigación y un *hacker* bueno
F-Secure

Introducción

La amenaza *hacker*

Otra vez ese sonido estruendoso que irrumpe mientras arañábamos los últimos minutos de un descanso reparador, recordándonos que es hora de empezar un nuevo día. Es la alarma del despertador. En realidad, de nuestro teléfono móvil, pues el tradicional aparato que ocupó un lugar indiscutible en la mesilla de noche durante décadas ha sido sustituido por el *smartphone*, que nos ofrece un sinfín de funcionalidades para hacer nuestra vida más cómoda a todos los niveles. Si programamos con él una alarma, nos brinda versatilidad para elegir o modificar el sonido que queremos que nos despierte cada día. Algo que el despertador tradicional no permitía.

Tras el sobresalto inicial, nos estiramos para coger nuestro dispositivo y detener la alarma. Aún con legañas en los ojos, echamos un vistazo rápido a las notificaciones mientras nos incorporamos para ver si hay algún mensaje importante en alguno de nuestros chats de WhatsApp o Telegram, filtrando aquellos que provienen de ese grupo en el que siempre hay cientos de mensajes que no aportan nada. Probablemente, es lo último que hicimos también por la noche, justo antes de dejar el dispositivo en la mesilla y encomendarnos a los brazos de Morfeo.

Mientras nos preparamos y desayunamos, repasamos el timeline de Twitter para seguir la actualidad del mundo o cualquier novedad en nuestro sector profesional. Complementariamente a esto, también echamos un vistazo a las actualizaciones de nuestros contactos de LinkedIn y las publicaciones de nuestros amigos en Facebook.

De camino al trabajo, tanto si tomamos el transporte público como nuestro vehículo particular, quizá escuchemos alguna radio en línea desde nuestro teléfono o con nuestra lista favorita de Spotify para enchufarnos de energía y comenzar el día con buen pie.

Una vez en la oficina, dejamos a un lado, pero cerca de nosotros, nuestro querido *smartphone* y arrancamos el ordenador corporativo para leer el correo electrónico y comenzar a trabajar…

Con alguna que otra variación, este podría ser perfectamente el inicio del día de cualquiera de nosotros. En tan solo unas pocas horas de un día cualquiera, ya hemos accedido a un sinfín de servicios que hoy constituyen prácticamente una necesidad esencial para nuestro bienestar. Forman parte de nuestro día a día, están integrados en nuestra rutina y si no los tenemos, los echamos en falta.

Todo esto es posible gracias a la evolución de la tecnología. Un desarrollo que pone a nuestro alcance un mundo hiperconectado, inimaginable hace pocos años. Un universo de ceros y unos que nos han llevado a vivir en una sociedad digital en la que cada uno de nosotros maneja una media de tres dispositivos al día para acceder a ese mundo virtual que denominamos ciberespacio.

Como es de imaginar, esta penetración de la tecnología en nuestras vidas tiene como contrapartida la exposición a una serie de riesgos que hasta la fecha eran desconocidos o menospreciados por la gran mayoría de la gente. Quizá porque hasta ahora muchos no eran conscientes del vínculo que existe entre el mundo físico y el virtual. Y piensan que lo que sucede en este último no tiene trascendencia o impacto real sobre nuestra vida. Y, como podemos deducir a tenor de los acontecimientos ocurridos durante los últimos años en materia de incidentes, nada más lejos de la realidad. En las sociedades desarrolladas, nuestra vida digital y nuestra vida física están enormemente solapadas. Lo que sucede en una, tiene un impacto directo sobre la otra, y viceversa. Solo casos muy excepcionales de grupos de seres humanos que todavía viven aislados del mundo actual y de la tecnología se salen de este esquema, y representan un porcentaje ínfimo de la población.

Por desgracia, nos hemos ido acostumbrando a noticias cada vez más frecuentes en las portadas de los medios generalistas que informan sobre incidentes de ciberseguridad. Si bien hace unos años estos sucesos podían resultarnos novedosos y puntuales, hemos alcanzado un punto en que prácticamente ninguna cosa que leamos al respecto de internet y la seguridad nos puede sorprender. En los últimos años, hemos asistido estupefactos a numerosas revelaciones de incidentes de robo masivo de cuentas de correo, datos de tarjetas de crédito, credenciales de banca en línea u otros servicios. También filtración de información confidencial de organizaciones, ataques al sistema financiero o a las llamadas infraestructuras críticas; sin dejar de lado

el ciberespionaje industrial o los eventos de ciberguerra entre países. Por supuesto, ataques que, pese a no ser novedosos en su *modus operandi*, han generado un revuelo social histórico a nivel global por la manera en que se produjeron, cuyo ejemplo más característico es WannaCry, hasta la fecha el ciberataque más mediático de todos los tiempos.

Como podemos comprobar, el espectro de amenazas a las que nos enfrentamos como consecuencia directa de nuestra dependencia natural de la tecnología es considerable. Son muchos y variados los diferentes vectores de ataque a los que nos vemos expuestos por parte de los cibercriminales u otros actores simplemente por ser usuarios de internet y de la tecnología.

Es por ello que se hace necesario conocer de primera mano y en detalle los riesgos a los que nos exponemos, para así poder hacerles frente, intentando evitarlos si es posible, o al menos procurando mitigar el posible impacto de su amenaza en nuestras vidas. Porque si bien es cierto que lo que hoy es seguro mañana puede no serlo, y que nunca podremos garantizar un nivel de seguridad total, sí es verdad que gran parte de los problemas que sufren los usuarios y las empresas podrían evitarse siguiendo una serie de buenas prácticas y recomendaciones.

Son estas cuestiones las que trataremos de desgranar con detalle a lo largo del libro, incluyendo algunos ejemplos y anécdotas más que elocuentes para comprender el panorama en el que nos movemos. El objetivo es ayudar a comprender mejor los entresijos de este complejo mundo sin tener que disponer de elevados conocimientos técnicos. Sin ahondar en detalles farragosos, pero abordando nociones y conceptos fundamentales. Proponemos una base de conocimiento mínima para ganar conciencia sobre las oportunidades y los riesgos del ámbito digital, y proporcionamos recursos para promover buenas prácticas y fortalecer nuestra seguridad y privacidad en la red.

Además de otros trabajos de carácter más técnico, uno de los servicios que más demandan las empresas a los expertos en ciberseguridad es la formación de su personal no técnico (tanto de alto nivel de dirección como al resto del staff), organizando sesiones de concienciación en materia de ciberseguridad. En ellas nos centramos en repasar los diferentes tipos de amenazas y explicamos la motivación de los ataques, los diferentes actores involucrados, por qué y cómo se originan. Mi experiencia profesional y mi participación en estas sesiones y conferencias a lo largo de los años están sintetizadas en el libro con el fin de ser útil e interesante para el lector.

Es importante conocer los diferentes tipos de ataques posibles, así como la finalidad de cada uno de ellos. Distinguir entre aquellos orientados al lucro económico por parte de ciberdelincuentes y los dirigidos al control de la información por parte de gobiernos, o bien los destinados a reivindicar un ideal abanderado por colectivos hacktivistas.

Resulta clave comprender que todos los ataques son posibles y se originan por errores técnicos o humanos. Asentar los conceptos de «vulnerabilidad» e «ingeniería social» como componentes esenciales de los ataques; diferenciar entre campañas masivas de *malware* y *phishing*; conocer el funcionamiento de las botnets que infectan nuestros equipos como zombis; entender los complejos ataques dirigidos a una organización u objetivo, o saber qué herramientas y prevenciones podemos emplear para hacer frente a cada uno de los escenarios, anticipándonos incluso a gran parte de los peligros serán algunas de las ideas que analicemos en el libro. La desmitificación de muchos tópicos que se han ido consolidando con los años acerca del mundo del *hacking* y la ciberseguridad ocupa también una parte importante de este trabajo.

La idea es que tú, usuario, profesional o empresario, llegues a alcanzar el conocimiento mínimo imprescindible para desempeñar correctamente tu actividad en el ciberespacio con las máximas garantías de seguridad posibles; porque internet es un medio maravilloso, pero a veces hostil. Debemos estar preparados para hacer frente a los peligros que se nos puedan presentar en el mundo virtual, del mismo modo que lo hacemos instintivamente en el mundo físico, mediante comportamientos aprendidos de manera natural a base de repetición. Igual que cerramos la puerta con llave al salir de casa o nos abrocharnos el cinturón de seguridad al emprender la marcha con nuestro coche, debemos adoptar y automatizar unas pautas mínimas de seguridad en el mundo en línea.

Si has comprado este libro, es que el tema te preocupa y estás dispuesto a dedicarle un tiempo. Es el paso más importante.

Aseguremos nuestra identidad digital y nuestros activos tecnológicos cerrando siempre la puerta y abrochándonos el cinturón. Porque la seguridad empieza por nosotros mismos.

1

Hackers, Script Kiddies y el vecino que te roba el *wifi*

Los ríos de información que nos llegan a través de diferentes canales respecto a la figura del *hacker* generan una imagen pública que no siempre se corresponde con la realidad. Sobre la idea del *hacker* giran todo tipo de especulaciones, falsos mitos, debates e incluso dilemas morales. Es inevitable comenzar definiendo este polémico concepto con el objetivo de transmitir su significado real, que para nosotros tiene, de hecho, una connotación positiva.

Sin embargo, esta visión no ha sido compartida tradicionalmente por medios de comunicación u organismos oficiales. Como muestra, el diccionario de la RAE define al *hacker* en su primera acepción como «pirata informático». Fue gracias a la insistencia de nuestro gremio que desde principios de 2018 se incorporó una segunda acepción mucho más próxima a lo que para nosotros es un *hacker*: «Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora».

¿Qué es un *hacker*?

El término *hacker* fue acuñado por primera vez en los años sesenta entre los informáticos del Instituto Tecnológico de Massachusetts (MIT). De ahí que siempre haya estado ligado al ámbito tecnológico. Su traducción literal no es otra que la de «curioso».

Un *hacker* es una persona inquieta, que no se conforma con utilizar la tecnología a nivel de usuario, sino que ansía profundizar en cada detalle. Es una persona apasionada por ahondar en el conocimiento de los sistemas, por superar los límites que la tecnología nos impone, llevándola más allá y

logrando hacer cosas para las que, en principio, no fue concebida. Desde incorporar nuevas funcionalidades que *a priori* eran impensables, hasta romper las barreras de seguridad que tratan de impedir su control. ¿Cómo? Descubriendo vulnerabilidades. Encontrarlas es fruto de horas y horas de aprendizaje, lectura, experimentación e investigación. Eso es realmente un *hacker*, y para todo lo demás existen otras denominaciones.

> *Un hacker no es un pirata informático como dice el diccionario de la RAE, sino todo lo contrario.*
>
> *Erróneamente asociado a la ciberdelincuencia, un hacker es en realidad alguien curioso, inquieto, apasionado por conocer cada detalle de lo que estudia, sea tecnología u otra cosa.*

Esta definición implica diferentes conceptos y aspectos que iremos desgranando, pero difiere radicalmente de la de pirata informático. Los piratas, los que utilizan todo este conocimiento y estas técnicas para hacer el mal, son los llamados ciberdelincuentes, que trataremos en el próximo capítulo. Quizá en el desconocimiento de este último concepto radica la confusión de la gran masa social. Debido a la tradicional estigmatización del término *hacker*, muchos lo utilizan incorrectamente para referirse a piratas o ciberdelincuentes. Afortunadamente, esta tendencia está comenzando a cambiar, como ilustra la decisión de la RAE para incluir una segunda definición del término.

Para quien aún no lo tenga claro, los *hackers* son los buenos, los inconformistas que intentan siempre llegar un paso más allá, motivados por la pasión que les mueve, para alcanzar un objetivo que han trazado en su cabeza y que muchas veces parece imposible.

Gracias a que existen *hackers* tenemos internet y disfrutamos de todas esas maravillas que la tecnología nos ofrece. Cada año podemos comprar dispositivos que los fabricantes tecnológicos nos presentan con nuevas funcionalidades, así como disponer de sistemas más robustos, más seguros, algo fundamental en estos tiempos donde la privacidad es un bien tan codiciado, pese a que muchos usuarios renuncian voluntariamente a ella sin tan siquiera ser conscientes de las implicaciones que tiene. De ello también hablaremos en un capítulo de este libro.

Todas las vulnerabilidades que los *hackers* descubren permiten que nuestros dispositivos, los sistemas con los que se comunican y la tecnología

que los conecta sean corregidos y fortificados. Esto es lo que nos permite a la larga vivir en una sociedad digital más segura para todos.

Cualidades de un *hacker*:

- Pasión.
- Inquietud.
- Perseverancia.
- Sacrificio.
- Ansia de conocimiento.
- Pensamiento lateral.
- Inconformismo.

Cualidades de un *hacker*

Lograr este tipo de mejoras, a veces auténticas hazañas, implica no solo disponer de un alto nivel de conocimiento técnico en la materia, sino de una serie de cualidades innatas que forman parte del ADN de cualquier *hacker*.

Además de cualidades como la inquietud, la curiosidad o la pasión, insuficientes por sí solas, hay otras más. A lo largo del camino, podemos encontrarnos con muchos obstáculos, con horas y horas de trabajo invertidas en una determinada línea de investigación que finalmente desemboca en un intento frustrado más. Con escollos insalvables por falta de recursos, de conocimiento o de tiempo. En estos momentos, la constancia y la perseverancia son también fundamentales.

Si has programado alguna vez, probablemente sabrás que cualquier código que escribimos, por muy simple que sea, casi nunca funciona a la primera. Siempre hay un error a la hora de compilar o hay algo que no está bien. Forma parte del rito. Por otro lado, también es posible que, en alguna ocasión, tras una serie de intentos fallidos por lograr que un programa haga lo que queremos, milagrosamente conseguimos arreglarlo sin saber muy bien cómo lo hemos hecho. Por explicarlo de una manera simple, es «como si lo tuviésemos cogido con pinzas», nunca llegamos a controlarlo del todo.

> *Para no perdernos…*
>
> *«Compilar» es traducir un programa escrito por humanos en lenguaje de alto nivel a un código interpretado por una máquina.*

Los errores o fallos de programación se conocen como bugs.

Esto era muy común a la hora de entregar prácticas de programación en la facultad. Muchas veces, en función del nivel de complejidad y de lo tarde que uno las empezara, podían requerir auténticas gestas, y escribir líneas de código toda la noche antes de la entrega. El resultado eran programas que funcionaban de manera un tanto inestable, a lo mejor ejecutándose correctamente tres de cada cuatro veces. Era habitual cruzar los dedos, mirar hacia arriba e implorar ayuda divina a la hora de presentar la práctica al profesor. En las entregas, muchos alumnos acababan recitando una expresión recurrente y casi mítica: «¡No puede ser, en mi casa funcionaba y aquí no!».

Este ejemplo es válido para exponer dos ideas:

- La primera es que evitar este tipo de situaciones es lo que sin duda alguna diferencia a un *hacker*. No dejar jamás cosas al azar, sin entender del todo cuándo, cómo y por qué se ha solucionado el problema de manera casual o casi accidental. Debemos huir del pragmatismo, aunque se haya logrado el objetivo.
- La segunda es que este tipo de actitudes por parte de los programadores cuando desarrollan cualquier programa son las que abren la puerta a que un *hacker* habilidoso, con ansia de conocimientos y con la constancia necesaria, pueda encontrar la razón de un comportamiento erróneo. Generalmente, gracias a un error (bug), el *hacker* identificará una vulnerabilidad para explotarla y alterar así el comportamiento original del programa. Así es como se comprometen los sistemas, pero son cuestiones que explicaremos con más detalle a lo largo de este libro.

Ejemplos de *hackers* en la historia y en la ficción

A la hora de hablar de *hackers* famosos a lo largo de la historia, probablemente el primer nombre que sale a la palestra es el del mítico Kevin Mitnick, perseguido en la década de los noventa durante tres años por el FBI. Hablaremos de él en el capítulo dedicado a la ingeniería social. Otros referentes del *hacking* a nivel mundial son Mikko Hypponen, reconocido por su amplia labor de investigación en el campo del malware y de la seguridad con numerosos galardones y distinciones; Fermín Serna, *hacker* español que trabaja en el equipo de seguridad de Google y en su día lo hizo para

Microsoft; o Charlie Miller, famoso por descubrir importantes vulnerabilidades, como las que permitían tomar el control de un vehículo en movimiento. Hay muchos otros *hackers* que quizá no suelen identificarse como tales. Bill Gates y Steve Jobs, referentes y responsables del éxito de Microsoft y Apple, o el creador del sistema operativo Linux, Linus Torvalds, son también *hackers*. Lo son en realidad todos los que transgreden los límites y van más allá, siempre con el objetivo de crear algo nuevo.

Otra de las cualidades que sin duda caracterizan a un *hacker* es su capacidad de resolver problemas complejos a través del pensamiento lateral. Para quien no haya oído jamás este concepto, se trata de la habilidad natural para encontrar soluciones ingeniosas a la hora de abordar un problema aparentemente irresoluble, a través de caminos alternativos. Uno de los mejores ejemplos para entender lo que es el pensamiento lateral se encuentra en el mundo de la ficción. Michael Scofield, protagonista de la serie Prison Break, ilustra cómo el *hacking* puede ir mucho más allá del teclado y la pantalla.

En esta adictiva y espectacular trama conspiratoria con elevadas dosis de intriga, Scofield, un genio con una mente brillante, abandona su exitoso trabajo como ingeniero de estructuras para embarcarse en una trepidante misión: ayudar a su hermano a escapar de la cárcel, ya que este ha sido condenado injustamente a raíz de una conspiración que se origina en las esferas más altas del Gobierno de Estados Unidos.

Para ello, Scofield planifica con minuciosidad todos los pasos para poder entrar en la cárcel y lograr su cometido, lo que implica acciones tan ingeniosas como la de tatuarse el plano de la prisión en su cuerpo en aras de disponer en todo momento de los mapas de las dependencias del recinto.

Como suele suceder en las series, el plan inicial del protagonista se va torciendo a medida que avanza la trama. A pesar de que cuenta con una hoja de ruta perfectamente trazada en la que ha cuidado todos los detalles, depende de muchos factores y agentes externos que se suceden y actúan en la historia. Es entonces cuando Michael Scofield hace gala del pensamiento lateral para resolver situaciones muy complejas capítulo tras capítulo. Momentos irresolubles para la mayoría de los mortales, pero no para este genio que encuentra siempre un recurso inesperado.

Estas cualidades innatas de Scofield se reflejaban desde la infancia. Su madre cuenta cómo de pequeño se dedicaba a romper todos los juguetes y aparatos que caían en sus manos para volver a repararlos o convertirlos en

nuevos. Aunque algunas de sus acciones trasciendan lo tecnológico, Michael Scofield es caracterizado como un *hacker* en toda regla.

> *Michael Scofield, protagonista de Prison Break, era un hacker.*
>
> *McGyver, capaz de crear cualquier artilugio a partir de objetos variopintos, era un hacker.*
>
> *Cualquiera puede ser un hacker en su campo de especialización o en su vida.*

Cuando la motivación no es otra que la de aprender, innovar y crear, en contraposición al beneficio económico que suele imperar a menudo, podemos encontrar *hackers* en muchas disciplinas o campos de la vida. Por eso es más acertado pensar en el concepto de *hacker* como una actitud, antes que como una persona. Cualquiera puede ser un *hacker* en su área de conocimiento o en su propia vida si adopta en ella ese talante.

Lammers y script kiddies

La sensación de satisfacción que se obtiene al alcanzar cada hito en esa búsqueda de conocimiento constante es muy superior a cualquier otro tipo de remuneración que cualquiera pueda imaginar. Pero solo se obtiene cuando uno llega a la consecución del objetivo, sea cual fuere, adoptando la vía del conocimiento y del trabajo duro. Sin buscar atajos, sin omitir etapas ni hacer trampas.

De nada sirve arreglar un programa si no sabemos cómo lo hemos hecho, o comprometer la seguridad de un sistema con herramientas automatizadas si no tenemos ni idea de lo que hacen dichas herramientas. No pasa nada por usar herramientas de terceros. Compartir conocimiento forma parte de esta cultura. Es totalmente lícito y todos lo hacemos, siempre y cuando nos hayamos tomado la molestia de documentarnos, de conocer y asimilar los conceptos técnicos que sustentan dichas herramientas, así como de controlar su funcionamiento a un nivel exhaustivo.

Lo que no procede es descargarse herramientas llamadas «de botón gordo» y ejecutarlas para que hagan todo el trabajo sin tener ni idea de lo que realmente hacen, para posteriormente vanagloriarse de ser un superhacker ante los demás. Esta actitud, totalmente contraria a la de un verdadero *hacker*,

es tan habitual en el mundillo, que tiene su propio apelativo: lammer, o script kiddie (el chico que ejecuta scripts).

> *Script es un término que hace referencia a un programa, generalmente sencillo, escrito en un archivo de texto.*

Un script kiddie generalmente es fácil de reconocer si se interactúa con él. Es aquel que en un foro o un chat preguntará directamente por la solución o respuesta a un problema sin pensar en la posibilidad de buscarla por sus propios medios. Es aquel que rehúye la teoría y busca directamente la herramienta que resuelve el problema, hecha por otro. Es quien ejecuta esa herramienta sin haber siquiera leído el manual, y cuando esta no hace lo esperado, lo primero que hace es preguntar en lugar de ir a la fuente.

Precisamente, el hecho de autoproclamarse como *hacker* ante los demás es lo que caracteriza a un potencial lammer o lúser en muchas ocasiones. El apelativo *hacker* reúne una serie de cualidades que giran en torno al respeto, la devoción y la admiración; bien distintas a las más mediáticas y difundidas. Ganarse este apelativo no es nada fácil. Supone un orgullo y un privilegio dedicarse a ello. Sin embargo, sería algo ambicioso y soberbio definirse a sí mismo como *hacker*, aunque no lo neguemos cuando una persona ajena nos defina así.

> *Un verdadero hacker no suele autoproclamarse como tal.*

Estos matices pueden parecer menores, pero cobran mucha importancia en un sector donde el ego está más acentuado aún que en otros lugares. El amplísimo campo de investigación disponible, y los potenciales descubrimientos lo convierten en una práctica muy competitiva donde por desgracia la búsqueda del reconocimiento de los demás se prodiga demasiado. Al final, nadie te da o te quita el título de *hacker*, es una cuestión de actitud.

Hackear al vecino que me robaba el *wifi*

Un ejemplo real e ilustrativo de lo que es un script kiddie está en esta historia que publiqué en su día en el blog de mi amigo Chema Alonso, El lado del mal. En aquella ocasión, la expliqué con pelos y señales desde un punto de

vista técnico. Para lo que nos interesa aquí, la he desprovisto de datos técnicos innecesarios.

Corría el año 2013, y yo tenía configurada la red *wifi* de mi casa a propósito con cifrado WEP. Estaba haciendo pruebas de los diferentes ataques posibles en este tipo de redes mientras escribía el libro Hacking en redes *Wifi* y Radiofrecuencia con el equipo de Mundo Hacker, liderado por otro gran *hacker* amigo, Antonio Ramos. El cifrado WEP es tremendamente inseguro y se identificó como tal desde 2001. Desde entonces, han aparecido multitud de herramientas «de botón gordo» que permiten obtener la contraseña de la red *wifi* en cuestión de minutos, sin necesidad de conocimiento técnico alguno.

Al tener configurada la red de manera insegura, era consciente de que algo malo podría pasar. Durante aquellos días, revisaba concienzudamente las conexiones a mi red en el panel de administración del router, por si de repente alguien se unía a la fiesta.

En las redes abiertas de hoteles, cafeterías o aeropuertos, el tráfico que generamos puede ser monitorizado por cualquiera.

> *«WEP» es un estándar de cifrado antiguo, declarado inseguro desde hace más de una década.*

Como regalo traído del cielo por los Reyes Magos, la tarde del seis de enero apareció un dispositivo más, con nombre «Rober1», que se unía al registro de conexiones, junto con mi ordenador, el móvil, y la PlayStation (que en aquellos maravillosos días aún tenía tiempo para encender).

Enseguida supe que tenía un intruso en mi red, posiblemente un vecino del edificio. Si así era, la seguridad de mis dispositivos estaba comprometida. ¿Sería un *hacker* haciendo pruebas o un ciberdelincuente, un verdadero pirata? Todo dependía de sus intenciones. La tercera posibilidad era que se tratara de un script kiddie con la única intención de obtener acceso gratuito a internet.

La solución pragmática consistía en modificar la configuración de la red a un cifrado más seguro (WPA2), asignarle una contraseña robusta y terminar con el problema. Pero la posibilidad de *hackear* al intruso, identificarlo y realizar una práctica en un escenario real me pareció un reto interesante. Pese a que suponía dedicar tiempo y esfuerzo, merecía la pena.

Sea como fuere, no tenía ninguna información del atacante y además se acercaba la hora de salir de casa para celebrar el día de Reyes con mi familia. Rápidamente, desconecté todos los equipos de mi red y le dejé todo el ancho

de banda al vecino. Eso sí, monitorizando el tráfico de mi propia red con una antena conectada a uno de mis equipos. Al tratarse de una red *wifi*, los paquetes de datos emitidos por cualquier dispositivo conectado a ella viajan en el aire, por lo que pueden ser capturados por cualquiera. Algo que es muy habitual en redes abiertas de hoteles, aeropuertos o centros comerciales.

Al llegar a casa por la noche, comencé a analizar el tráfico capturado durante esas horas. La información disponible en la captura advertía que, efectivamente, había un vecino que estaba utilizando mi red. Su equipo tenía un sistema operativo Windows, con nombre de equipo «Rober1», y en principio había estado utilizando la red para navegar por internet. Los sitios webs más visitados durante esa primera sesión de navegación eran los siguientes:

- http://vanitatis.com: una página de prensa rosa que hasta entonces yo desconocía.
- http://devilwearszara.com: una página de tendencias de moda.
- http://fotoplatino.com: una página de tendencias de moda y peinados.
- http://elpais.com/gente: la sección más rosa de El País.

Con una captura de tráfico se puede acceder a toda la información que un usuario genera en una red, por lo que, además de analizar rápidamente los sitios webs más visitados, también reconstruí las imágenes transferidas en esa primera sesión de navegación. Algunas de las imágenes mostraban a Miley Cirus y otros famosos en la gala de los Óscar, así como fotos de peinados y vestidos varios.

El tipo de contenido visualizado por mi vecino me hacía pensar más en una usuaria con conocimientos básicos de internet que en un *hacker*. Por su historial de navegación supuse que se trataba de una mujer.

Seguí analizando con más detenimiento el tráfico que generaba Rober1. Encontré una petición al sitio web de ASUS para descargar una actualización, donde se podía incluso visualizar el modelo de equipo con el que se conectaba a mi red. Así que, visto que parecía no tener muchos conocimientos en materia de ocultación o anonimato, todo apuntaba a que se trataba de una script kiddie que buscaba conexión a internet gratuita.

Con el objetivo de identificarla, empecé a pensar en diferentes vectores de ataque. Una posibilidad era la de interceptar el tráfico entre el equipo de los vecinos y el router en tiempo real, una vez conectado a mi red. Este tipo de ataques se conocen como ataques Man in the Middle, por aquello de colocarse en medio de la comunicación entre dos dispositivos. Pero esto requería, entre

otras cosas, que ambos estuviésemos presentes al mismo tiempo, lo que ocasionaba tener que estar permanentemente atento al momento en que mi vecina se fuese a conectar.

> *Los ataques Man in the Middle se llaman así porque el atacante se pone en medio de la comunicación entre dos puntos, generalmente la víctima y el router por el que navega en internet.*
>
> *Este ataque engaña a los dos dispositivos, suplantando en cada uno la identidad del otro mediante el envío de información falseada, para redirigir el tráfico de ambos a la máquina del atacante.*
>
> *Una vez interceptada la comunicación, es capaz no solo de acceder al contenido que visualiza, sino también de modificar tanto lo que envía como lo que recibe.*

En un par de ocasiones pude coincidir con ella, pero el éxito de estos ataques dependía de muchas circunstancias. Al ver que no podía resolver mi problema de esta manera, comencé a trabajar en una aproximación diferente y algo más compleja.

Mientras tanto, seguía monitorizando continuamente el tráfico que la vecina iba generando en mi red y lo analizaba para poder obtener información que me permitiese identificarla: un nombre, un usuario, una contraseña, una dirección de correo…

Llegado a este punto, ya tenía un patrón de comportamiento. Sabía que mi presunta vecina se conectaba dos o tres veces al día y que sus sesiones de navegación eran de aproximadamente quince minutos. En todas esas sesiones, solía consultar las páginas de prensa rosa y tendencias, pero también algunas nuevas que no aparecieron las primeras veces, y que me llamaron la atención:

- elimperiodelaley.blogspot.com.
- quieroserjuez.blogspot.com.
- vidadeunaopositora.blogspot.com.
- sufridoraenejercicio.blogspot.com.
- quenovoyaserlasecretariadeunjuez.blogspot.com.

Sí, has deducido bien: opositora a juez robando *wifi*. «Marca España».

Además de estas sesiones de navegación, a lo largo del día se sucedían otras muy cortas, de apenas unos pocos minutos de duración. Por el tipo de contenido que generaban, presuponía que ya no correspondían a mi vecina, sino a su pareja. Las páginas visitadas eran las siguientes:

- sport.es (sección El Balón Rosa, protagonizada por las novias de los futbolistas).
- marca.com.
- tenerifedeportivo.com.

Dejando a un lado los tópicos sobre el fútbol y los hombres, es interesante tener en cuenta cómo podemos obtener mucha información de una persona anónima por el tráfico que genera en una red.

> *«Dime por dónde navegas y te diré quién eres».*

El historial de navegación que generamos en una red dice mucho de nosotros y de nuestra personalidad.

Un domingo, después de consultar fugazmente su lista de diarios deportivos de referencia, Rober1 visitó también la página de unos cines cercanos a nuestro domicilio en Santa Cruz de Tenerife para echar un vistazo a la cartelera. Al cabo de unas horas, pude concluir que en última instancia no acudió a ver la película que estaba barajando o que, si finalmente lo hizo, decidió ir solo o con algún amigo, pero no con su pareja. A la hora que se proyectaba la película, ella estaba conectada a mi red viendo páginas de moda y blogs de oposiciones a juez. Probablemente haciendo su habitual descanso de quince minutos.

El colofón a esta serie de sucesos fue comprobar que en alguna ocasión accedieron a su cuenta de banca en línea desde un *wifi* ajeno usurpado, lo que evidenciaba la falta de conocimiento técnico y el desconocimiento de las consecuencias que pueden acarrear estos actos.

HTTP versus HTTPS

Hasta ahora os he contado que disponía de la información de todos los sitios webs visitados por mis vecinos, pero aún no he mencionado otros portales casi esenciales en cualquier sesión de navegación de un usuario estándar, como pueden ser Gmail, Facebook, Twitter o LinkedIn. ¿Por qué no había recopilado información referente a estos servicios?

Afortunadamente, este tipo de servicios y muchos otros que manejan información personal de usuarios son ofrecidos para acceder a ellos desde nuestro navegador mediante el protocolo HTTPS, que se representa con la imagen de un candado en la barra del navegador. Este protocolo cifra la información transmitida por el medio físico utilizando por debajo otros protocolos, como TLS o SSL. Esto quiere decir que, aunque alguien escuche el tráfico en una red como yo lo estaba haciendo, y como alguien podría hacer en cualquier red *wifi* pública a la que os conectéis, los paquetes que vayan cifrados con estos protocolos son ininteligibles. Es por eso que hasta ahora estaba viendo en claro el tráfico de los sitios web de moda, blogs de oposiciones a juez o diarios deportivos que mis vecinos visitaban regularmente. Puesto que el acceso a estos portales se realizaba mediante HTTP convencional. Sin embargo, hasta el momento no había podido obtener nada relacionado con sus redes sociales y servicios de correo que me permitiera identificarlos.

Lo que tenemos que saber:

- HTTP: protocolo de transferencia de hipertexto.
- HTTPS: protocolo de transferencia de hipertexto segura. Asegura la información mediante protocolos de cifrado transparentes al usuario, como SSL y TLS.

Con el objetivo de romper de alguna manera esta barrera del cifrado, estaba trabajando en una aproximación distinta al Man in the Middle. Los vecinos se conectaban a mi red mediante la conexión *wifi* habilitada por mi router ADSL, por lo que en lugar de intentar atacarlos cuando estuviesen, pensé en cambiar la estructura de mi red, ya que al fin y al cabo yo tenía el control sobre la misma. Ellos se seguirían conectando a través de la conexión *wifi* que ofrecía mi router. Pero quien de verdad haría las funciones de router sería mi equipo. Es decir, todo el tráfico que ellos generaran pasaría por mi equipo. Este lo transferiría al router y luego lo llevaría de vuelta al equipo de los vecinos. En lugar de un esquema de Man in the Middle, estaba implementando un Machine in the Middle. Seguiría accediendo al tráfico de mis vecinos como hasta ahora, pero podría hacer algo más. Para evitar dejar indisponible la red cuando ellos fueran a utilizarla, tenía que ser sumamente cuidadoso a la hora de «cacharrear», como se dice vulgarmente, desplegando mi nueva topología de red durante las horas que no estuviesen conectados. Si por algún error en el proceso dejaba mi red inoperativa cuando ellos la fuesen

a utilizar, podrían pensar que se había caído y dejar de conectarse, y todo mi trabajo habría resultado en vano.

La diferencia con respecto a la escucha pasiva de tráfico radicaba en que, si ahora dicho tráfico pasaba por mi equipo, además de interceptarlo podría modificarlo en tiempo real, exactamente lo que pretendía hacer. Mediante el uso de una determinada herramienta muy conocida para ataques en redes, interferiría el tráfico de mis vecinos para alterar el código fuente de las páginas web que recibían. En realidad, son unos y ceros. Cuando esos unos y ceros se traducían en enlaces a sitios web con HTTPS, la herramienta suprimía la S de «seguro», dejando los enlaces a los mismos sitios, pero utilizando el estándar HTTP, por lo que el tráfico se transmitiría sin cifrar, igual que el de las páginas de moda o los diarios deportivos.

Acceder a su cuenta de Facebook

Solo un día después de haber habilitado este esquema de funcionamiento, sucedió lo que esperaba. En el primer descanso que mi vecina se tomó en su sesión de estudio, además de acceder a sus habituales páginas de moda y a los blogs de oposiciones, entró en su cuenta de Facebook, como seguramente habría hecho anteriormente. La diferencia era que esta vez había conseguido que enviara sus credenciales de inicio de sesión mediante HTTP. En términos sencillos, ya tenía en mi poder su usuario y contraseña de Facebook.

En ese momento a uno se le pasan muchas cosas por la cabeza: entrar en su cuenta, echar un vistazo a sus mensajes privados, publicar alguna aberración en su muro… Más allá de lo que habría sido puro vandalismo informático, lo importante, y que sí hice, fue identificarla a ella y a su pareja. ¿Cómo? Buscando la parte pública de su perfil mediante su dirección de correo, que es el usuario de Facebook. Pude confirmar que, en efecto, se trataba de una pareja de abogados, y, además, que no los conocía personalmente. No me había cruzado nunca con ellos en el portal o en el ascensor, por lo que seguramente se habrían mudado hacía poco. Supongo que por eso decidieron conectarse a mi red mientras no tuvieran la suya.

Una vez identificados, les envié un correo electrónico desde una cuenta anónima de Gmail. En él les informaba de que estaba al corriente de su actividad delictiva desde el primer momento y les exponía toda la información que había ido recopilando acerca de su tráfico. Tampoco quise cebarme mucho con ellos, ya que era normal pensar que detrás de una red *wifi* insegura como la que ellos habían vulnerado seguramente habría un usuario

sin ningún tipo de conocimientos, y no un *hacker* que pudiese invertir los papeles.

No obstante, en ocasiones podemos encontrarnos con redes o sistemas configurados a propósito como inseguros a modo de señuelo para que sean comprometidos por los malos y acabar cazando así a estos ciberdelincuentes. Este tipo de trampas se conocen como Honeypots.

El amigo informático

Mi mensaje debió de calarles hondo, ya que a las pocas horas obtuve una respuesta muy educada a mi correo en el que reconocían su error y se disculpaban por su actitud. Admitían que eran conscientes de la ilegalidad de sus actos (aunque no hacía falta ser abogado para ello), pero no de las implicaciones que su actividad podría tener a nivel técnico. Como explicaban en su correo, fue «un amigo informático el que nos dijo que así podíamos tener conexión a internet gratis».

En este caso no llegó la sangre al río, pero si en lugar de conmigo se hubiesen topado con alguien que tuviese intenciones maliciosas, además de comprometer su cuenta de Facebook y quizá revocarles el acceso, las consecuencias podrían haber sido mucho más graves. Con un poco de paciencia, podría haber accedido, por ejemplo, a sus cuentas bancarias sin que tuvieran la más mínima idea. A lo largo de este libro iremos viendo algunas de las técnicas que pueden aplicarse con relativa facilidad y que los ciberdelincuentes utilizan para vulnerar la seguridad de los usuarios.

Lecciones aprendidas de esta historia y recomendaciones

El relato de los vecinos y el *wifi* es una historia real y habitual que ilustra los peligros a los que nos exponemos a la hora de conectarnos a redes *wifi* públicas o ajenas, así como las recomendaciones que debemos tener en cuenta en estos casos.

En primer lugar, conviene dejar claro los siguientes aspectos:

- En las redes *wifi* públicas de hoteles, cafeterías, aeropuertos o centros comerciales, todo el tráfico que generamos puede ser monitorizado por cualquiera.
- Esto se aplica tanto si la red es abierta como si dispone de cifrado WEP, WPA o WPA2 y tiene contraseña, pues todos los que se conectan a ella conocen la contraseña.

- Monitorizar el tráfico HTTP que generamos en estas redes es trivial, no ocurre así con el tráfico HTTPS que está cifrado.
- Aun así, existen formas de romper la barrera de cifrado HTTPS, como la que utilicé para comprometer la cuenta de Facebook de mi vecina.
- A día de hoy, esta técnica es más difícil de implementar que en el momento en que esta historia tuvo lugar, hace ya cinco años.
- No obstante, sigue siendo posible encontrar la manera de aprovechar la inseguridad inherente a este tipo de redes y comprometer la seguridad de los usuarios.

Así pues, debemos tener claro qué medidas adoptar a la hora de conectarnos a redes *wifi* tanto públicas como ajenas:

- Podemos utilizar sin problemas estas redes para consultar información, leer noticias, acceder a sitios web… pero debemos extremar la precaución a la hora de utilizar servicios personales.
- A pesar de que tanto Facebook como Twitter, LinkedIn o nuestro banco nos proporcionan una interfaz segura mediante HTTPS, y que, a día de hoy, estos ataques son más difíciles de llevar a cabo, es recomendable evitar usar estos servicios desde redes *wifi* públicas.

> *Una VPN es una red privada virtual. Se trata de una tecnología que nos permite conectarnos remotamente a una red local doméstica o corporativa desde cualquier punto de internet.*

Esto hace que las comunicaciones desde dicho punto hasta esa red vayan cifradas y no puedan ser monitorizadas por cualquiera, lo que permite obtener seguridad en cualquier red *wifi* donde nos conectemos.

- Si utilizamos un dispositivo corporativo y nuestra empresa dispone de conexión VPN, es imperativo utilizarla siempre que nos conectemos a una red *wifi* pública. En ese caso, podremos utilizar todos los servicios que queramos sin problema.
- Si somos responsables de la seguridad de una empresa y, debido a su tamaño o modelo de negocio, no dispone de VPN, es recomendable implantar una para garantizar la seguridad de las comunicaciones de aquellos trabajadores con movilidad, que viajan y se conectan a redes *wifi* públicas.
- A nivel personal también es posible utilizar una solución VPN para poder garantizar nuestras comunicaciones. En ese caso, podremos

utilizar todos los servicios que queramos sin problema.

- Si como usuarios no tenemos a nuestro alcance configurar una conexión VPN por falta de conocimiento o recursos, es posible contratar este servicio a un proveedor. Existen multitud de alternativas en el mercado que, a precios asequibles, nos permiten contratar servicios de VPN para poder navegar seguros en cualquier red a la que nos conectemos.

Por supuesto, sobra decir que no debemos conectarnos jamás de manera ilícita y sin permiso a redes *wifi* ajenas, aunque alguien nos proporcione las herramientas para lograrlo. Además de ser inmoral e ilegal, como hemos podido comprobar, puede poner en grave riesgo nuestra seguridad.

2

Ciberataques y lecciones aprendidas: una historia de *hacking old school*

Como hemos visto, *hacker* no es sinónimo de pirata informático. Los *hackers* investigamos técnicas ofensivas y defensivas, descubrimos vulnerabilidades y las reportamos. Es cierto que a veces nos movemos en la delgada línea que separa el bien del mal, pero nuestra motivación es generalmente la de aprender y compartir conocimiento con la comunidad. Los que utilizan su conocimiento para hacer el mal y beneficiarse a costa de comprometer la seguridad de usuarios y organizaciones se denominan, como ya hemos adelantado, «ciberdelincuentes».

Con el paso de los años, nos hemos ido aclimatando al escenario actual que vivimos en materia de incidentes tecnológicos. Los ciberataques son ya una realidad que forma parte de nuestro día a día, hasta el punto de que pocas cosas nos pueden sorprender. Son muchas las noticias que nos llegan a través de los medios de comunicación con una frecuencia casi semanal relacionadas con ataques de diversos tipos y técnicas. Hablamos de robos de millones de cuentas o euros con total ligereza, y de incidentes de ciberespionaje entre países o incluso ataques a centrales eléctricas o sistemas de control industrial.

Un dato significativo que refrenda esta situación es el que arroja el informe de riesgos globales elaborado por el World Economic Forum. Desde hace unos años, los ciberataques y los fallos en infraestructuras críticas no solo se catalogan como riesgos con entidad propia, sino que tienen el dudoso honor de encontrarse en el top 5 de la clasificación, al nivel de otros riesgos comúnmente aceptados como relevantes, tales como el envejecimiento de la población o el cambio climático.

> *El cibercrimen es la actividad delictiva más lucrativa en la actualidad: ocasiona pérdidas de cerca de 500 000 millones de dólares en la economía mundial.*
>
> *Los ciberataques y los fallos en infraestructuras críticas están en el top 5 de los riesgos identificados por el World Economic Forum.*

A día de hoy, el cibercrimen mueve más dinero en el mundo que el narcotráfico, el contrabando de armas o la trata de blancas. Para hacernos una idea, se estima que el cibercrimen tiene un impacto en la economía mundial de alrededor de unos 500 000 millones de dólares al año, según un informe elaborado por el conocido fabricante McAffee.

Estos datos, junto con otros que iremos viendo, confirman que el cibercrimen representa un problema real. Frente a lo que algunos piensan, no se trata de insuflar miedo entre la población para generar negocio. En el sector de la ciberseguridad, al igual que en muchos otros, existirán comerciales que engorden las cifras o profesionales de la venta de humo, pero esto es inevitable y además independiente de la realidad de los delitos en el entorno digital.

Algunos tópicos que se han asociado tradicionalmente a este entorno carecen de veracidad. Un ejemplo claro, que afortunadamente ya no se escucha tanto como antes, es la idea de que son los propios fabricantes de antivirus los que crean los virus. Nada más lejos de la realidad.

Todo este complejo entramado de ataques e incidentes del mundo digital no puede reducirse tan solo a los virus informáticos. Vivimos en un estadio tecnológico en el que la realidad supera a la ficción, donde casi cualquier cosa que podamos imaginar en cuanto a ataques digitales puede ser perfectamente plausible. Es un escenario en el que los guionistas de novelas, series y películas lo tienen bastante complicado para sorprendernos con ataques o incidentes novedosos que superen a los que ya se producen, día a día, en el mundo real. Conocer cada uno de ellos con más detalle nos permitirá hacerles frente de la manera adecuada.

Un acontecimiento que avala esta afirmación es el ciberataque mundial más mediático jamás vivido hasta la fecha de publicación de este libro. Hablamos, como no puede ser de otra manera, del famoso WannaCry, un ataque que afectó a compañías punteras en el mundo entero y que sin duda alguna cambió el punto de vista de la opinión pública sobre la ciberseguridad.

Dedicaremos un capítulo completo a describir con detalle las peculiaridades que lo hicieron diferente, así como la intrahistoria que lo rodea.

La industria del cibercrimen

Existen tres motivaciones principales para los ciberataques que se acometen sobre usuarios y organizaciones:

- El lucro económico.
- El control de la información.
- Hacktivismo.

Aunque algunos incidentes puntuales pueden haber sido originados por otra motivación, por lo general estas son las causas fundamentales que originan los ataques. Por otra parte, cada una de estas motivaciones lleva asociados actores claramente diferenciados. Los iremos desgranando tanto en este como en próximos capítulos.

- El lucro económico es la finalidad única y exclusiva del cibercrimen, como es evidente.
- El control de la información es lo que mueve a los gobiernos y a sus agencias de inteligencia, que centran sus esfuerzos en intentar monitorizar las comunicaciones. ¿De quién? Tanto de sus propios ciudadanos, de elementos hostiles o potencialmente hostiles, así como de otros Estados. Supuestamente, en aras de garantizar la seguridad nacional. Puede haber también otros actores motivados por la obtención de información, como empresas u organismos que desarrollan su actividad en sectores como el químico, el petrolífero o el energético, donde el I+D+i y la propiedad intelectual son fundamentales.
- El hacktivismo constituye la motivación de los activistas, que utilizan la red, en lugar del mundo físico, para manifestarse y lograr notoriedad con sus acciones. Pese a que incurren en delitos, su objetivo no es el robo de información ni de dinero, sino reivindicar una causa o idea.

Como puedes imaginarte, de las tres enumeradas, la motivación económica es la que está detrás de la gran mayoría de ataques. Los ciberdelincuentes se han dado cuenta de que el uso malintencionado de todas las técnicas del *hacking* puede ser muy rentable, y con el paso de los años se ha creado una industria en la sombra, altamente especializada, que se dedica a rentabilizar el negocio del cibercrimen a nivel profesional.

No se trata de individuos encapuchados aislados en un garaje como algunos puedan imaginar. Hablamos de organizaciones estructuradas, con su jerarquía, sus departamentos, sus equipos multidisciplinares y hasta reclutadores de recursos humanos en algunos casos. En definitiva, organizaciones cibercriminales que basan su actividad económica en campañas masivas de extorsión, fraude y todo tipo de delitos tecnológicos. Existen diversos ejemplos de organizaciones cibercriminales que, con el paso del tiempo, han sido desarticuladas y procesadas, como la del grupo que se encontraba detrás del famoso «Virus de la Policía». Se trataba de una banda compuesta por doce integrantes, la mayoría de origen ruso, país que alberga muchas de estas organizaciones. El fabricante Kaspersky, conocido por investigar diversos grupos cibercriminales responsables de campañas de ataques como esta y otras muchas acaecidas entre 2013 y 2015, concluyó en un informe que las organizaciones detrás de este tipo de campañas estaban formadas por una media de entre diez y cuarenta personas.

> *Defacement: es el acto de modificar el aspecto original de una página web por una falsa, típicamente con mensajes reivindicativos o tono burlesco.*

El contexto en el que nos encontramos ahora es completamente diferente al que teníamos hace poco más de una década, donde los ataques no tenían ni el alcance crítico ni la magnitud de los actuales. En aquella época, uno de los mayores peligros para una organización podía venir de un *hacker* independiente que intentara comprometer los sistemas de una infraestructura real para poner en práctica sus habilidades. En este caso, su objetivo no era otro que el de aprender y demostrar que era más listo que los responsables de seguridad. Una vez que el *hacker* conseguía entrar, podía no hacer nada, dejar un flag (una especie de bandera o señal para demostrar simplemente que estuvo ahí, a modo de trofeo) o quizá dedicar una burla a los administradores del sistema, sustituyendo, por ejemplo, el aspecto del sitio web de la empresa por una página adulterada que incluyese algún tipo de mofa. Esta última acción, que sigue utilizándose a día de hoy, se conoce como defacement. En función del grado de intervención y de la naturaleza del ataque, podría causar (o no) cierta repercusión en la reputación de la organización o en la carga de trabajo del departamento de IT en ese día en concreto, aunque probablemente no iría más allá. Al final se trataba de un *hacker* en busca de conocimiento, no

de organizaciones cibercriminales como las que existen hoy día, dedicadas a robar información o activos económicos a gran escala.

Una historia old school. Un ataque de hace una década

Como ejemplo de un escenario en el que un *hacker* pone a prueba sus habilidades contra sistemas reales, he aquí una historia verídica que jamás ha salido a la luz y de la que fui protagonista.

Tuvo lugar hace ya bastantes años. No siempre me dediqué profesionalmente al *hacking* y la ciberseguridad, entre otras cosas porque viviendo en Canarias no existía la posibilidad por aquel entonces. Sí que trabajaba como ingeniero informático, pero en otras áreas del sector TIC. De hecho, tuve que abandonar mi zona de confort y mi querida isla de Tenerife para poder cumplir el sueño de trabajar al máximo nivel en este sector. Fue en 2013, cuando decidí mudarme a León con mi familia para ejercer como Security Evangelist del Instituto Nacional de Ciberseguridad (INCIBE), tras ser seleccionado junto a otros 18 *hackers* de entre más de 600. Pero esto sucedió mucho después.

Años atrás, trabajaba en el Departamento de Ingeniería de GRAFCAN, y me dedicaba al desarrollo de *software* en el ámbito de la ingeniería geográfica. El *hacking* era un *hobby* al que le dedicaba mis ratos libres para aprender, y, en el fondo, sigue siendo así en la actualidad, aunque ahora sí trabajo en el sector de la ciberseguridad. Esto atañe por igual a todos los compañeros de profesión. El anhelo constante de tiempo libre para aprender es una de las mayores preocupaciones para cualquier *hacker*. Incluso aunque nos dediquemos profesionalmente a la ciberseguridad en nuestro día a día. Salvo en casos excepcionales, las habilidades que debemos aprender para seguir creciendo técnicamente hemos de adquirirlas en casa finalmente, en esos ratos libres de los que no disponemos jamás, y que generalmente obtenemos robándole horas a otros menesteres como el sueño.

> *La expresión Hacking ético hace referencia al proceso para intentar encontrar fallos de seguridad en un sistema a demanda de la propia organización objetivo.*

Un domingo por la mañana me desperté inquieto en casa, más temprano de lo habitual. Tras tomarme un té para despertar los sentidos, me fui al ordenador para intentar poner en práctica algunas de las técnicas que se utilizan en las

primeras etapas de un proceso de auditoría de seguridad o «hacking ético». Se denomina así al proceso para intentar atacar los sistemas de una organización con el objetivo de identificar posibles vulnerabilidades que puedan ser explotadas, y concebido como un servicio demandado por la propia organización mediante el establecimiento de un contrato y bajo consentimiento mutuo. Es por ello que se añade el adjetivo de «ético».

También suele usarse este apelativo cuando un *hacker* o investigador descubre por cuenta propia esas vulnerabilidades sin ninguna motivación delictiva, y las reporta de manera altruista a la compañía afectada para que sean remediadas, sin exigir nada a cambio. Básicamente, este calificativo se utiliza para distinguir estas actuaciones de las perpetradas por los ciberdelincuentes, cuyas intenciones son bien distintas. Independientemente del contexto y la motivación de quien lleva a cabo este proceso, la metodología y las técnicas utilizadas son las mismas, tanto para hacer el bien como para el mal. Ahora bien, ¿cuáles son los pasos?

Fase 1: reconocimiento o information *gathering*

El primer paso es recolectar toda la información posible de un objetivo para después intentar encontrar sus debilidades. Esto implica el descubrimiento a ciegas tanto de su infraestructura tecnológica (dominios, sitios web, servidores, direcciones IP, tecnologías utilizadas…) como de sus recursos humanos (nombres de usuario, direcciones de correo, números de teléfono, perfiles en redes sociales…). Cualquier dato puede ser de interés. Si no es posible encontrar una puerta de entrada a través de sus sistemas, quizá haya que buscarla a través de sus usuarios. A la hora de planificar un ataque, cuanta más información se reúne en esta fase inicial, más posibilidades existen de comprometer el objetivo.

Las técnicas que me disponía a probar aquel domingo estaban encaminadas a identificar servidores con servicios concretos accesibles desde internet, ofrecidos por la organización objetivo. Se persigue reconocer todos los servicios que la compañía ofrezca desde internet, con vistas a la identificación de posibles vulnerabilidades en estos servicios.

El rango de direcciones IP que estaba examinando pertenecía a un grupo bancario nacional de reciente creación, constituido por cuatro cajas de ahorros, entre las que se encontraba también la Caja General de Ahorros de Canarias. El grupo bancario se constituyó en 2010 y se disolvió en 2012, cuando fue absorbido por otra importante entidad financiera. No obstante, en

aquel entonces, los servidores que estaba inspeccionando estaban registrados a nombre del grupo constituido, no a los de ninguna de las entidades que lo conformaban.

> *La mayor parte de los sitios web que visitamos a día de hoy son técnicamente «aplicaciones web», porque no son páginas estáticas como las que visitábamos en los orígenes de la red, sino que ejecutan código y proporcionan funcionalidades interactivas.*

Husmeando entre los diferentes servidores del grupo, di con lo que parecía ser el panel de administración de un servidor web Jboss. Se trata de un servidor de internet ampliamente utilizado en aquella época para ejecutar aplicaciones web desarrolladas en Java, un conocido lenguaje de programación. Técnicamente se llaman aplicaciones web porque ejecutan código en un servidor, pero para los usuarios finales, son sitios web. De hecho, la mayor parte de los sitios web que visitamos a día de hoy a diario son aplicaciones.

Evidentemente, el panel de administración del servidor requería la introducción de las credenciales de acceso para poder entrar. Lo primero que un *hacker* suele hacer al encontrarse con un panel de administración es probar la combinación de usuario y contraseña por defecto, es decir, la que viene predeterminada a la hora de instalar por primera vez un *software* o un dispositivo. Es posible que hayas hecho lo mismo a la hora de intentar configurar dispositivos como los routers de ADSL o fibra óptica que nos suele instalar nuestro proveedor de internet.

Fase 2: identificar un servidor vulnerable

La combinación «admin/admin» para los campos de usuario y contraseña me facilitó acceso completo al panel de administración de aquel servidor. ¡No me lo podía creer! Alguien perteneciente a la compañía había dejado un servidor accesible a internet sin modificar la contraseña por defecto para el usuario administrador. Como es posible entrever, esto constituye un error abismal, pues para encontrar esta contraseña basta con consultar la documentación de instalación del servidor, disponible a golpe de consulta en Google.

Recomendaciones:

- Modifica siempre la contraseña por defecto al instalar cualquier *software* o configurar un nuevo dispositivo.

- Nunca abras a internet un servidor con aplicaciones en desarrollo que no han sido correctamente testeadas.

Una vez dentro, pude echar un vistazo a las diferentes aplicaciones web existentes en el servidor. No parecían estar desplegadas para su uso, sino más bien aún en desarrollo. Tras una primera ojeada, daba la sensación de que se trataba de un servidor en el que alguien estaba trabajando para implementar una nueva aplicación y que por descuido o error estaba ya accesible desde internet.

En este punto, un atacante con intenciones maliciosas podría realizar muchas acciones. Si la motivación fuese la de causar daño, una posibilidad más que obvia sería la de borrar o corromper las aplicaciones que estaban configuradas. Esto, como poco, obligaría a los desarrolladores a comenzar de nuevo el trabajo si no dispusieran de una copia de seguridad. Otra aproximación más interesante sería la de intentar buscar una manera de ejecutar comandos en ese servidor web con el objetivo de controlarlo y poder descubrir otras máquinas de la red o saltar a otro punto. Como mi motivación era la de aprender y valorar hasta dónde podía llegar, me propuse intentar tomar este camino.

Para lograrlo, necesitaba lo que se conoce en el argot como una shell, es decir, una consola que te permite ejecutar comandos en el servidor. Un ejemplo de consola es el cmd en Windows, también llamado «Símbolo de sistema» (heredado del prehistórico MS-DOS), que posiblemente hayas abierto alguna vez.

> *Las web shells constituyen una manera ingeniosa de poder ejecutar comandos en una máquina de manera remota a través de un navegador, como si estuviésemos frente a una consola.*

Yo tenía acceso al panel de administración del servidor web, no a la consola. Había una posibilidad para lograr tener algo parecido a una consola mediante la instalación de lo que se conoce como una web shell («consola web»). El concepto es sencillo. Ya que tenía la capacidad de administrar el servidor, podría crear una nueva aplicación web ligera, una sola página accesible desde el navegador, con el formulario más sencillo de todos: un campo donde introducir un texto, otro donde recibir texto y un botón de «Enviar». ¿Con qué objetivo? En el campo de entrada de texto, introduciría los comandos que querría ejecutar en el servidor para poder controlarlo, que a su vez se

ejecutarían al pulsar el botón de «Enviar» y posteriormente mostrarían el resultado de dicha ejecución en el otro campo de texto. De esta manera, tendría una especie de consola accesible desde el navegador. De ahí el nombre de web shell.

Fase 3: explotar la vulnerabilidad y controlar el servidor

El siguiente paso consistía en crear esta aplicación web, a través de Java, que era la tecnología ofrecida por el servidor. Años atrás, desarrollé bastantes aplicaciones web utilizando este lenguaje de programación, aunque hacía ya un tiempo de eso. Con los lenguajes de programación sucede algo parecido a lo que pasa con los idiomas: aunque los conozcas, si dejas de practicarlos con asiduidad, pierdes fluidez a la hora de hablar o escribir. Tampoco supone un problema, puesto que, para programar, lo que realmente importa es conocer los conceptos y nociones que hay detrás. Luego, dominar la sintaxis y el uso del lenguaje influye en el tiempo que se tarda en escribir el programa para que funcione correctamente.

Además, para ayudarnos tenemos un montón de recursos disponibles en la red. En algunos casos podremos encontrar programas hechos por otros que hagan justo lo que nosotros necesitamos, o bien fragmentos de código que nos faciliten la tarea. Sea como fuere, es de vital importancia que en cualquiera de los casos entendamos y conozcamos al detalle el funcionamiento y entresijos del programa que vamos a ejecutar, sobre todo si el código que lleva escrito no es totalmente nuestro, puesto que nos podríamos llevar alguna sorpresa. Recordemos lo comentado en el primer capítulo acerca de los script kiddies.

Invertí un tiempo en refrescar lo que necesitaba para escribir mi propia web shell en Java. Al cabo de un rato, ya la tenía lista. Se acercaba el momento de la verdad. ¿Lograría llegar un paso más allá y controlar de verdad el servidor al que había accedido? Como en la vida misma, en el *hacking* nunca se puede dar nada por sentado. Aunque tracemos adecuadamente nuestra estrategia, es posible que surjan inconvenientes, que en algunos casos podremos solventar y en otros no.

Subí la web shell al servidor creando una nueva aplicación web. Acto seguido, abrí el navegador para acceder a la página en concreto y pude visualizar el formulario que había programado. Escribí mi primer comando en el campo de texto, crucé los dedos y le di al botón de «Enviar» mientras contenía la respiración. ¡Voilá! ¡Había funcionado! Tras unos milisegundos, en el otro campo de texto veía el resultado de aquella primera instrucción que

había ejecutado: un comando sencillo de Linux llamado «ls» (equivalente al famoso «dir» presente en los sistemas Windows, desde MS-DOS) que muestra por pantalla la lista de ficheros y carpetas presentes en el directorio actual.

La sensación de satisfacción, felicidad y éxtasis que uno experimenta en ese preciso instante es difícil de transmitir con palabras. Es una sensación que quizá, a diferencia de otras en la vida, nunca deja de ser igual de intensa que la primera vez, aunque pasen los años.

Tras el primer «ls», empecé a probar otros comandos con la intención de inspeccionar el contenido del servidor y ver qué margen de maniobra tenía a la hora de manipularlo. Pese a que la web shell te permite ejecutar comandos en el servidor, no deja de ser un programa *ad hoc*, construido sobre la marcha, por lo que no es exactamente igual que una consola tradicional. Aunque tampoco supone mayor problema, simplemente se trata de acostumbrarse a trabajar con ella para hacer lo que queramos. Un momento clave vino al ejecutar el comando whoami que nos devuelve la información del usuario que está ejecutando la sesión actual. Esto, que puede parecer algo obvio cuando trabajamos en nuestro ordenador con nuestro usuario, no lo es tanto a la hora de trabajar con servidores. Mucho menos a la hora de comprometer servidores ajenos, como puedes imaginar. Además, en sistemas como Linux, los servicios como los servidores web, FTP, correo u otros, tienen usuarios específicos que limitan sus permisos en el sistema, precisamente por motivos de seguridad. Me quedé perplejo al ver que en este caso la sesión a la que yo tenía acceso pertenecía al usuario root, el usuario con máximos privilegios en Linux, también conocido como «superadministrador». El dios todopoderoso del sistema.

> *Como responsables de seguridad de una organización, se ha de comprobar que los servidores no están siendo desplegados con permisos de superadministrador.*

Fase 4: postexplotación frustrada

Estaba emocionado. Eso significaba que podría hacer prácticamente cualquier cosa con el servidor: acceder a todos los rincones del sistema (incluidos ficheros de configuración con jugosas contraseñas de servicios y datos de usuarios), así como crear nuevos usuarios, habilitar una puerta trasera para

volver a entrar en el futuro, o hacer cualquier cosa que puedas imaginar. Podría incluso bajar en el servidor *software* específico para auditar el resto de equipos de la red interna en busca de otras vulnerabilidades. Las posibilidades se multiplicaban, aunque como ya he comentado, mi intención no era otra que la de aprender y ver hasta dónde podía llegar. No pretendía ocasionar ningún daño, ni realizar ninguna acción maliciosa. De hecho, la idea en esta fase de postexplotación era eliminar la web shell y cualquier rastro de mi presencia en el servidor una vez hubiese terminado de realizar mi práctica de *hacking* en un escenario real.

Desafortunadamente, esto no llegó a pasar. Cegado por las infinitas posibilidades que el acceso como root me ofrecía, empecé a ejecutar diferentes comandos a toda velocidad. Estaba tan inmerso en los siguientes pasos que iba a dar, que, envuelto por la euforia, perdí la noción del espacio-tiempo. Olvidé por un instante que no estaba en una consola normal, sino en una web shell.

> *Es fundamental controlar todos los detalles durante una intrusión y no perder jamás el foco.*
>
> *Los resultados de un descuido en medio de un hack pueden ser catastróficos.*

¿Qué fue lo que sucedió? Que metí la pata de la manera más absurda. Hice precisamente lo que no tenía que hacer. Como tenía acceso root, empecé a jugar para ver si era capaz de controlar los servicios de la máquina. En vez de elegir cualquier otro, el primero que casualmente se me ocurrió fue el del propio servidor web que me estaba dando acceso a través de la web shell. Por un instante olvidé dónde estaba, pensando que disponía de una consola normal. Lo que hice no fue parar el servidor web, sino mandar hacer un restart, es decir, reiniciarlo. Le di al botón de «Enviar» y acto seguido me di cuenta de mi error. La aplicación web se quedó colgada y el servidor dejó de responder. Yo mismo lo había mandado reiniciar. Toda la explosión de júbilo y alegría se disipó en un milisegundo. La mayor metedura de pata de la historia. Había conseguido acceso a una máquina y me lo había revocado yo mismo. ¿Cómo había podido ser tan incauto?

De todas formas, aún quedaba esperanza. Había mandado reiniciar el servidor, no pararlo. Si todo iba bien, al cabo de unos segundos era posible que se reiniciara correctamente. Yo volvería a tener mi web shell operativa para continuar donde lo dejé y al menos podría limpiar el rastro.

Lamentablemente, esto no fue así. Esperé un tiempo prudencial para intentar volver a acceder. Luego un minuto, luego dos. Toda esperanza de recuperar el acceso se esfumó. El servidor se había parado, pero no había vuelto a iniciarse correctamente, por lo que la máquina quedaba totalmente desconectada desde la red.

En este momento, me invadieron no solo la frustración y el enfado conmigo mismo, sino también el miedo. Como mi intención inicial era simplemente la de investigar técnicas pasivas de escaneo e identificación de activos, sin realizar ningún tipo de intrusión, no estaba utilizando ningún mecanismo de ocultación para camuflar mi dirección IP. En este sentido, es habitual utilizar máquinas intermedias de salto, conocidas como proxy, o nodos de la famosa red TOR, a la que se hace referencia como la «internet oscura» o Dark Web y de la que hablaremos más adelante.

Analizar el escenario

Al navegar directamente utilizando la conexión a internet de mi domicilio, estaba totalmente expuesto. Si simplemente hubiese hecho lo que pretendía en un principio, es decir, eliminar desde la consola tanto la web shell como los registros de acceso al servidor (conocidos como logs), las probabilidades de que alguien pudiese detectar mi presencia habrían sido muy bajas.

> *Se denomina logs a los ficheros que registran eventos en un sistema, tales como accesos, errores, notificaciones o cualquier suceso que se quiera registrar.*

Sin embargo, al intentar reiniciar el servidor, me había puesto en la situación totalmente contraria. Ahora, sí o sí, alguien iba a darse cuenta de lo que había pasado. En concreto, la persona que administrase el servidor cuando fuese el lunes siguiente a trabajar. Esta era la situación en la que me encontraba:

- Lo primero que haría el administrador del servidor sería ver por qué se había parado, y acto seguido intentaría restablecerlo.
- Comprobaría los logs del sistema para ver si se había producido algún error, así como los de acceso al servidor web (esos que yo pretendía borrar).
- En estos últimos, podría ver un montón de conexiones desde mi IP.

- Incluso saltándose estos dos pasos, al reiniciar el servidor web, se daría cuenta de que había una aplicación más además de las ya configuradas: la que yo había creado con la web shell.
- Tras dedicar un rato y ver el código, incluso si no supiese previamente lo que es una web shell, lo descubriría en ese mismo instante.
- Entonces sí que iría a ver los logs de acceso, que registrarían mi IP como la última que accedió al servidor antes de detenerlo.
- Además de esto, habría evidencias de mi acceso a la web shell, lo que probaría que estaba tratando de controlar el servidor remotamente de manera ilegítima.

Un sudor frío recorrió mi cuerpo cuando dibujé rápidamente en mi cabeza este diagrama de flujo que conducía hasta mi domicilio. Ya no podía hacer nada más que rezar para que el responsable del servidor lo ignorase por cualquier motivo remoto o lo investigase sin demasiada profusión, o que optase por no reportarlo a los responsables, puesto que si yo había conseguido entrar fue por un error suyo que le señalaría y desacreditaría como técnico. Recordemos que fue él quien dejó un servidor expuesto a internet con credenciales por defecto. También cabría la posibilidad de que lo dejasen pasar al ver que no iría a mayores.

No me quedaba otra que intentar tranquilizarme, dejar pasar el tiempo y esperar que no ocurriese nada. En este caso, la mejor noticia sería la ausencia de noticias. Sobre el papel puede parecer fácil, pero la verdad es que lo pasé mal durante unos días, ya que me era imposible pensar en otra cosa.

Transcurrida una semana, decidí llamar a un amigo que trabajaba en el Departamento de Nuevas Tecnologías de la Caja General de Ahorros de Canarias, donde fuimos compañeros en mi primer trabajo. La probabilidad de que pudiese proporcionarme algo de información al respecto era remota, puesto que esta entidad estaba aún en proceso de incorporación al grupo bancario, y por el momento mantenía su independencia a todos los niveles, tanto en imagen corporativa como en infraestructura o servicios. Además, es necesario recordar que el rango de direcciones IP que yo había analizado correspondía al grupo bancario, no a la Caja.

Curiosamente, no solo estaba al tanto del incidente, sino que resultó que, por alguna de esas extrañas casualidades, a pesar de que el servidor web que yo vulneré se encontraba publicado en la red del grupo bancario, eran ellos, el personal de la Caja, los que estaban trabajando con él. Por supuesto, mi amigo no sabía que estaba hablando con el autor de los hechos. Ni por asomo podría imaginarlo, pero casualmente me comentó que habían tenido un incidente de

seguridad. Me explicó que estaban muy preocupados porque «un intruso logró acceder a sus sistemas» y «no sabían cómo lo había hecho, qué información pudo extraer ni qué motivaciones tenía». Según me dijo, los responsables de seguridad «estaban intentando mover los hilos para poder saber a quién pertenecía la IP del atacante».

Podéis imaginar mi cara al oír y procesar toda esta información. Por un lado, me entró el pánico y, por el otro, no pude evitar poner en cuarentena algunos comentarios, debido a la incongruencia de los mismos, aunque es verdad que, en situaciones como esta, el boca a boca puede tergiversar el mensaje que se transmite. Estas fueron mis primeras conclusiones:

Como había supuesto, el responsable del servidor obvió comentar al resto que lo había dejado configurado con las credenciales por defecto. De ahí la preocupación al no saber a qué se enfrentaban ni cómo había entrado el intruso. De lo contrario, habrían conocido perfectamente el origen del incidente.

Para hacer esta historia aún más surrealista, el responsable del servidor era casualmente otro amigo mío, para mí el mejor técnico de los que trabajaban allí. Paradójicamente, el único que tenía conocimientos e interés por el *hacking* y la seguridad informática. De hecho, ese interés fue lo que nos hizo entablar amistad durante el año que pasé trabajando con ellos. Por aquel entonces yo acababa de salir de la facultad, y él llevaba más de doce años trabajando en el departamento. Era mucho mayor que yo. Se empeñaba en llamarme «pequeño saltamontes» cada vez que me corregía o enseñaba algo. La verdad que para mí él siempre fue un *hacker* en esencia, aunque quizá un poco acomodado con el paso de los años. Quizá por eso había obviado contar a los demás lo que realmente sucedió. Si además llegaba a saber que había sido el pequeño saltamontes quien le había sacado los colores, el ego del *hacker* que llevaba dentro no habría podido soportarlo. En el fondo, me moría de ganas de llamarlo y contárselo, pero preferí contenerme, ya que de no tomárselo bien, la situación sería totalmente irreversible.

Por otro lado, lo de «mover los hilos» para llegar a mí a través de la IP no era tan sencillo. Esto es información restringida a la que solo algunos trabajadores del proveedor de servicios de internet (ISP) tienen acceso y que generalmente se trata con la máxima confidencialidad. No se facilita a nadie, solo a Fuerzas y Cuerpos de Seguridad del Estado siempre que exista un requerimiento judicial. Según mi amigo, ellos «tenían buenos contactos», pero me permití la licencia de dudarlo. Ya sabemos cómo mucha gente tiende a exagerar las cosas para darse protagonismo.

No sé si hablar con él me dejó más tranquilo o todo lo contrario, pero al menos me reveló esta curiosa casualidad. Ni por asomo habría podido imaginar que un servidor que escogí al azar de un rango de direcciones perteneciente a un grupo bancario que tenía su sede en Madrid pudiese estar administrado por un excompañero de trabajo que vivía a pocos metros de mi casa y que además tenía inquietudes por el *hacking*. Ellos tampoco podrían imaginar que aquello que ellos veían como «un sofisticado ataque», para el que montaron un gabinete de crisis, era simplemente una práctica de alguien a quien conocían muy bien, que llevó no más de media hora.

Esta historia concluyó sin trascender ni tener más consecuencias. Supone un ejemplo ilustrativo del primer escenario que describimos: el de un *hacker* independiente que consigue comprometer los sistemas de una infraestructura real solo para poner en práctica sus habilidades, y que, en cuanto a la evolución en materia de ataques, nada tiene que ver con el mundo que nos encontramos hoy.

Lecciones aprendidas de esta historia y recomendaciones

A raíz de esta historia, es posible extraer una serie de aspectos para tener en cuenta y evitar que nos pueda pasar algo parecido en nuestra organización, o incluso como usuarios particulares si tenemos algún sitio web o portal publicado en internet:

- A la hora de instalar cualquier *software* de gestión, servidor o aplicación en general debemos cambiar siempre el usuario y la contraseña por defecto.
- Esto es extensible a la hora de configurar los routers ADSL de nuestro domicilio u oficina, así como cualquier otro tipo de equipamiento de red: puntos de acceso, repetidores, PLC, cámaras de vigilancia…
- Nunca debemos publicar en internet nada que no esté preparado para estar en explotación o producción. Si aún está en fase de desarrollo, el acceso debe estar limitado a la red interna de la organización.
- A la hora de configurar servicios que están expuestos a internet, debemos evitar que estén siendo ejecutados con permisos de administrador o root.
- Si no disponemos de conocimiento para asegurar este tipo de cuestiones, debemos recurrir a un tercero que audite nuestros servicios antes de publicarlos al exterior.
- Independientemente de lo anterior, como responsables de seguridad de una empresa, es importante contratar auditorías de seguridad o *hacking*

ético periódicamente o cada vez que haya cambios considerables en nuestra infraestructura. De esta manera, identificaremos y remediaremos las vulnerabilidades existentes antes de que un *hacker* o un ciberdelincuente pueda explotarlas.

- Por otra parte, como responsables de seguridad, si somos víctimas de un ataque, debemos llegar al fondo de la cuestión: intentar determinar la causa y origen del incidente, la vulnerabilidad que ha sido explotada, el alcance de los activos comprometidos, así como la información sensible que pueda haber sido manipulada o alcanzada ilegítimamente. Todo esto forma parte de la respuesta a incidentes, concepto que desarrollaremos en próximos capítulos.

3

Vulnerabilidades, exploits y programas de recompensas para *hackers*

En los capítulos previos hemos asentado algunos conceptos esenciales para poder adentrarnos de lleno en el conocimiento detallado de los diferentes tipos de amenazas a los que estamos expuestos en el ciberespacio.

Para saber cómo protegernos a la hora de navegar por la red y evitar ser víctimas de los ciberdelincuentes, en la medida de lo posible, es fundamental conocer los diferentes tipos de ataques que existen, así como las técnicas que se utilizan para acometerlos. Solo así podremos estar realmente en disposición de tomar las medidas oportunas en cada caso y mitigar el impacto de un posible ataque exitoso.

Pero mucho antes de profundizar en esto, debemos aclarar una cuestión esencial más, que quizá muchas veces se pasa por alto a la hora de abordar estos temas. ¿Cómo se producen todos estos ataques? ¿Cómo logran los ciberdelincuentes penetrar en los sistemas, robar información o provocar todos estos incidentes que nos hemos acostumbrado a presenciar? ¿Es magia? ¿Son magos?

Suelo dejar unos segundos a los asistentes a mis conferencias tras plantear esta reflexión inicial antes de responder, para enfatizar la relevancia que tiene esta cuestión para entender todo lo demás. La comparación con el mundo de la magia responde a las similitudes que existen entre ambas disciplinas. De hecho, tradicionalmente los *hackers* han estado envueltos en un halo de misticismo similar al que rodea a los magos.

> *En el hacking, al igual que en la magia, no existen poderes sobrenaturales.*

Los ataques se producen a causa de un error técnico o humano.

Los trucos de magia son posibles gracias a un error de atención del espectador.

La respuesta es sencilla: todos estos ataques ocurren a causa de un error. No existe magia, en absoluto. O en cierto modo sí que la hay, porque en cualquier espectáculo de magia que se precie, los trucos asombrosos con los que el prestidigitador cautiva a la audiencia responden también a una ilusión; un fallo de atención por parte del público, que no repara en el detalle que da sentido y explicación racional a lo que ocurre en el escenario. El mago induce el error, desviando la atención de los espectadores a un punto en el que sus movimientos pasan desapercibidos, y que permite llevar a cabo esa acción aparentemente sobrenatural. Así es como consigue crear la ilusión.

En el mundo del *hacking* ocurre lo mismo. Los sistemas quedan comprometidos porque en origen hay siempre un fallo, sea técnico o humano. Veamos algunos ejemplos:

- Un programa mal diseñado que permite alterar su flujo de ejecución en determinadas condiciones.
- Un servicio que se deja abierto en internet sin contraseña.
- Un servidor con la contraseña por defecto (como sucedía en la historia del capítulo anterior).
- Un usuario que establece su fecha de nacimiento como contraseña de su correo electrónico o que configura las preguntas de seguridad con respuestas que cualquiera podría conocer.
- Un usuario que cae en la trampa o engaño del ciberdelincuente, que le induce a pinchar en un determinado enlace o instalar un programa espía.

Los vectores de ataque y las posibilidades son considerables, y cubriremos cada uno de ellos a lo largo de todos los capítulos del libro. Aun así, he considerado interesante enumerar brevemente algunos de ellos para afianzar la idea de que la única explicación posible a los diferentes ataques y situaciones que podamos presenciar pasa siempre por la existencia de un error. Este error en el mundo de la ciberseguridad se conoce como «vulnerabilidad».

La asombrosa tecnología que manejamos diariamente y de manera compulsiva en nuestras frenéticas vidas se compone de un entramado de

estándares, protocolos, redes, electrónica de comunicaciones, dispositivos… Un sinfín de piezas que se ensamblan y permiten crear ese ecosistema de conectividad, servicios, aplicativos y funcionalidades al que los usuarios estamos cada vez más acostumbrados.

> *La tecnología está desarrollada por seres humanos, que pese a ser brillantes, pueden cometer errores.*

Algo en lo que quizá la gran mayoría no suele reparar es que todos estos estándares, protocolos, dispositivos, así como los aplicativos que corren en los mismos, han sido diseñados y desarrollados por ingenieros, analistas, programadores… En definitiva, geeks, como se denomina ahora a los amantes o especialistas de la tecnología. Pese a tratarse de mentes brillantes, su condición de seres humanos no les exime de cometer errores a la hora de hacer su trabajo. Por esta razón, tanto los estándares o protocolos que se utilizan para interconectar redes y equipos, como el *software* que corre en dispositivos tecnológicos de cualquier tipo, incluyendo ordenadores, dispositivos móviles, impresoras o routers, son susceptibles de incluir errores o fallos, tanto en su diseño como en su implementación.

Dependiendo del tipo de error, la gravedad del mismo y el componente o ámbito al que afecta, puede tener menor o mayor repercusión en el correcto funcionamiento de los sistemas a los que involucre, así como representar o no un peligro para los mismos. A este tipo de error, que puede poner en riesgo el comportamiento natural de dicho sistema, logrando que se comporte de manera diferente a la convencional o esperada, es al que se hace referencia cuando se habla de vulnerabilidad.

Vulnerabilidades y exploits

La vulnerabilidad hallada en un dispositivo, sistema o tecnología no implica por sí sola que estos hayan sido comprometidos. El programa que se encarga de aprovechar o explotar una vulnerabilidad para comprometer la seguridad del recurso en cuestión se conoce como exploit, de ahí su nombre.

Generalmente, el descubrimiento de una nueva vulnerabilidad por parte de un investigador de seguridad lleva asociado el desarrollo o escritura de un exploit que permite aprovecharla, aunque esto no siempre tiene por qué ser así. En muchos casos, se pueden identificar vulnerabilidades que requieren de determinadas condiciones específicas para poder ser explotadas, y que

dificultan la elaboración del exploit. También puede ocurrir que el posible impacto o valor del exploit no compense el esfuerzo que el investigador tendría que invertir en su desarrollo. Esto puede depender de muchas variables: desde el sistema, programa o tecnología a la que impacta, hasta el número de dispositivos que pudiesen estar afectados o las posibilidades para la explotación de la vulnerabilidad.

> *Las vulnerabilidades son clasificadas dependiendo de su criticidad.*
>
> *El CVSS asigna una puntuación entre 0 y 10, dependiendo de diferentes variables.*

Este último aspecto es un factor que debemos tener en cuenta. Como puedes suponer, no todas las vulnerabilidades son iguales, ni los exploits que las aprovechan funcionan del mismo modo. Dependiendo del tipo y de las condiciones del error, una vulnerabilidad puede ser más o menos crítica. De hecho, las vulnerabilidades suelen clasificarse por su impacto y criticidad utilizando diferentes métricas. La clasificación más extendida es la CVSS (Common Vulnerability Scoring System). Se trata de un sistema que asigna una puntuación entre 0 y 10, que permite evaluar el impacto de cada vulnerabilidad en función de una serie de métricas y variables que van en la línea de los ejemplos enumerados en el párrafo anterior.

Ejemplos de vulnerabilidades y nivel de criticidad

Un ejemplo de vulnerabilidad con baja puntuación de CVSS, y por tanto escasa criticidad, podría ser el representado por un error en el código de la aplicación que corriese en cualquier sitio web de internet. Un fallo que, al mostrar al usuario una página de error por pedir un recurso no disponible, revelase información sobre directorios o rutas internas del sistema donde están alojados los ficheros que conforman dicha web. Esto es algo que muchos lectores habrán experimentado alguna vez. Suele ser muy habitual cuando copiamos mal un enlace o cometemos algún fallo tipográfico al introducir una dirección en la barra del navegador. Generalmente, estamos acostumbrados a ver páginas de error que incluyen el famoso código «HTTP 404», que se traduce como «recurso no disponible». En el hipotético caso de una aplicación con una vulnerabilidad de este tipo, en la página de error 404 podrían aparecer también nombres de directorios, ficheros y rutas internas que

no deberían ser visibles para el usuario, porque proporcionan información sensible sobre la estructura interna del sistema. A este tipo de vulnerabilidades de bajo impacto se las denomina «informativas».

En el otro extremo, una vulnerabilidad con una alta puntuación de CVSS podría ser un error en el código de un programa que permitiese alterar el flujo de ejecución natural de dicho programa. En palabras simples, tomar el control del programa. Si además esto se puede hacer de manera remota, sin necesidad de tener que estar autenticado en el programa (para lo que se requeriría de una cuenta de usuario), y si la forma de explotar el error es sencilla, el valor de CVSS va incrementándose hasta llegar al 10, pues las condiciones para la explotación de la vulnerabilidad son muy favorables. Es el caso ideal. La vulnerabilidad soñada por todo *hacker* o por un ciberdelincuente.

Un ejemplo de este caso sería un servidor FTP vulnerable que cualquiera pudiera controlar remotamente, debido a un error en el código que recoge el usuario y la contraseña en la fase inicial de autenticación, cuando alguien intenta acceder al servidor. No haría falta disponer de cuenta legítima para acceder al servidor FTP, sino que cualquiera podría aprovecharse de esta vulnerabilidad, porque el error estaría en la validación de la cadena de texto que introducimos en el campo de usuario o contraseña. Esta vulnerabilidad tendría una puntuación de 9,5 o 10. Si, por el contrario, el mismo error estuviese en una sección del código posterior, por ejemplo, en la que habilita la funcionalidad de transferir ficheros, esto implicaría que para llegar a esa sección del código, el usuario tendría que estar previamente autenticado en el servidor FTP. Es decir, que para explotar la vulnerabilidad tendría que tener acceso legítimo al sistema mediante una cuenta de usuario. Esto reduciría enormemente las posibilidades de explotación y, por tanto, la puntuación CVSS de la vulnerabilidad, puesto que ya no podría ser explotada por cualquiera de manera remota, sino solo por un limitado número de personas que tuviesen cuenta de usuario en el servidor FTP. Del mismo modo, podría ser motivo de desaliento para el investigador sumergido en la siempre tediosa tarea de desarrollar un exploit para esta vulnerabilidad.

Reporte de vulnerabilidades

Por otra parte, que se descubra y reporte una vulnerabilidad no implica que el exploit se publique para que todo el mundo pueda utilizarlo alegremente. Más aún cuando el desarrollo de exploits es un campo complejo que requiere de mucha especialización. Existen auténticos especialistas que dedican la mayor

parte de su tiempo a desarrollar exploits para vulnerabilidades previamente identificadas por otros investigadores.

> *En el mundo del hacking, existen muchas áreas de conocimiento, por lo que se tiende a la especialización.*
>
> *El desarrollo de exploits es un área que requiere de un nivel de dedicación extrema.*

Hay portales como ExploitDB que recogen exploits publicados por estos especialistas para todo tipo de tecnologías, dispositivos y programas. Si bien en estos portales se encuentran exploits que se hacen públicos para algunas de las vulnerabilidades que se van descubriendo, existen muchísimos otros que no se publican o se mueven solo en determinados círculos de confianza, por motivos evidentes.

> *En algunos casos, los exploits que se hacen públicos incluyen errores en el código a propósito, para evitar su uso por parte de script kiddies.*

En muchos casos, los exploits que se exponen públicamente en estos portales suelen ser lo que se conoce como «pruebas de concepto». Es decir, demuestran que la vulnerabilidad existe y que se puede aprovechar, pero requieren que quienes lo vayan a utilizar realicen determinadas modificaciones sobre el mismo. A veces se publican con algunos errores de programación a propósito, o incluso trampas que puedan comprometer la máquina de quien los ejecuta. Como puedes imaginar, esto se hace para asegurar que quien hace uso de estos exploits es realmente alguien digno de hacerlo, que tiene cierto nivel de conocimientos y no se trata de un script kiddie.

A estas alturas, puedes inferir que, si descubrir una vulnerabilidad es importante, desarrollar o disponer del exploit para la misma lo es aún más. Es lo que realmente permite sacar provecho de la vulnerabilidad para atacar y comprometer los sistemas. Desde la perspectiva ofensiva, si se identifica un sistema como vulnerable, pero no se dispone del exploit para sacar provecho de la vulnerabilidad, poco se puede hacer.

Los exploits, valiosas armas para la guerra en el ciberespacio

Los exploits son la puerta de entrada para atacar los sistemas y obrar la magia. Son las armas que se utilizan en las guerras que ahora se libran en el ciberespacio. Es por eso que tienen un valor económico que se puede cuantificar en función del impacto que puedan tener, así como de la dificultad que pueda implicar su descubrimiento y desarrollo.

Hasta ahora hemos tratado los conceptos de vulnerabilidad y exploit asumiendo un contexto en el que las vulnerabilidades ya han sido descubiertas y reportadas. No obstante, antes de llegar a este punto, existen diversas alternativas que se plantean a los investigadores respecto a qué camino seguir desde el mismo instante en que dan con una nueva vulnerabilidad. Conviene explicar dichas alternativas con cierto detalle, ya que las decisiones tomadas en este punto inicial condicionan el curso de los acontecimientos, dando lugar a diversos escenarios.

Publicación de vulnerabilidades: revelación completa o responsable

La primera de las alternativas a la hora de descubrir una nueva vulnerabilidad es la de simplemente no publicarla. No comunicar su descubrimiento y no compartirla con nadie, o hacerlo solo con un reducido conjunto de allegados, en grupos privados a los que solo es posible pertenecer si se aporta conocimiento adecuado, respetando un código de extrema confidencialidad. Esto es algo muy habitual en la comunidad *hacker*, donde siempre han existido círculos privados de élite en los que los investigadores comparten sus hallazgos.

El otro camino es el de hacer pública la vulnerabilidad, para lo que hay también diferentes itinerarios. Existen dos políticas radicalmente opuestas respecto a la publicación de vulnerabilidades en el mundo de la ciberseguridad: la revelación completa o *Full* disclosure y la revelación responsable o Responsible disclosure.

La primera de ellas, como su propio nombre indica, aboga por exponer al mundo toda la información relativa a la vulnerabilidad sin comunicarla previamente al fabricante del producto o *software*, publicando todos los detalles técnicos e incluso el exploit, para que pueda ser usado por cualquiera, incluidos los script kiddies. Es la política más radical y agresiva. Como todo, tiene defensores y detractores. Con este criterio se consigue que todo el mundo disponga de la información a la vez para actuar en consecuencia e intentar proteger sus sistemas, aunque al mismo tiempo se provee de

munición a cualquiera para atacarlos. Por otro lado, se deja expuestos a los proveedores o fabricantes sin haberlos avisado previamente, lo cual motiva que deban actuar bajo presión, de manera reactiva y con celeridad para poner fin al problema mediante la publicación de un parche.

La Responsible disclosure, sin embargo, aboga por una revelación más comedida, que no exponga los sistemas de los usuarios ni genere caos. El objetivo es avisar previamente al proveedor o fabricante del sistema, con el fin de darle la oportunidad de trabajar en la creación de un parche que pueda remediar la vulnerabilidad. En ocasiones, el aviso se realiza a través de terceros actores que coordinan el proceso para facilitar la comunicación entre ambas partes. Si el proveedor se muestra receptivo, reconoce el problema, y está en disposición de resolver la vulnerabilidad, dando también el mérito al investigador que la ha descubierto, este espera un tiempo prudencial para la publicación. Es un período de tiempo variable y depende de cada investigador y de la reacción del proveedor en cada caso. Se suele dar un período mínimo de treinta días a partir del contacto inicial, y se extiende hasta noventa días si el proveedor muestra interés y si está realmente trabajando en la solución del problema. En este escenario, cuando finalmente se revela al mundo la vulnerabilidad, se publica también el parche por parte del proveedor, con lo que los usuarios no habrán quedado desprotegidos. Por otro lado, a la hora de publicar la vulnerabilidad, no suelen darse todos los detalles técnicos y, por supuesto, aún menos se publica el exploit.

No obstante, puede darse el caso de que el proveedor no reaccione positivamente al aviso, sino que ignore al investigador, haga caso omiso sin reconocer la vulnerabilidad como tal, o incluso adopte una postura retadora. Si se da este caso, el investigador procede a adoptar la política de revelación completa y publica los detalles de la vulnerabilidad sin que esta haya sido remediada. La única diferencia con la *Full disclosure* es que en estos casos el investigador no publica el exploit, ya que de hacerlo dejaría expuestos los sistemas de todos los usuarios ante ataques de cualquiera, al no disponer de parche o solución por parte del proveedor. Recordemos que las intenciones del investigador en una política de Responsible disclosure son las de actuar de manera ética, responsable y protegiendo en última instancia a los usuarios.

Clasificación de vulnerabilidades

Cuando las vulnerabilidades se publican, además de una puntuación CVSS, se les asigna un identificador para poder clasificarlas. Al igual que para el caso

de las métricas, existen diferentes sistemas de clasificación y denominación de vulnerabilidades. El estándar *de facto* es el Common Vulnerabilities and Exposures (CVE). Su funcionamiento es sencillo. A cada vulnerabilidad se le asigna un identificador, o CVE, que se compone de dos números: el primero de ellos es el año en el que se descubre y publica la vulnerabilidad, y el segundo representa el orden de dicha vulnerabilidad entre las identificadas ese mismo año, por lo que se va incrementando conforme estas se van reportando. De este modo, al conocer el CVE de cualquier vulnerabilidad, es posible inferir rápidamente cuándo fue reportada. Un ejemplo de código CVE es el «CVE-2017-0143», vulnerabilidad que fue utilizada para elaborar el WannaCry, el ciberataque más mediático de la historia, que abordaremos en detalle en próximos capítulos.

El CVE es el sistema de clasificación de vulnerabilidades más utilizado, aunque hay otras alternativas. Por otra parte, los fabricantes pueden mantener también su propia nomenclatura para organizar los parches contra las vulnerabilidades reportadas sobre sus productos. Tal es el caso de Microsoft, que publica actualizaciones de seguridad periódicas incluidas en el «Microsoft Security Bulletin», a las que también añade dos dígitos para el año y otros dos para el orden correlativo de la actualización. De hecho, el parche para la vulnerabilidad CVE-2017-0143 utilizada para WannaCry estaba incluida en el MS17-10. Seguro que recordarás estas siglas, recogidas en muchísimos artículos que se hacían eco de la noticia, allá por mayo de 2017.

Lo que tienes que saber

- Como usuario:
    - Mantén siempre actualizados tus sistemas y las aplicaciones que tengas instaladas en ellos, utilizando siempre los parches de los fabricantes.
    - Activa las actualizaciones automáticas para poder estar al día y protegido frente a nuevas vulnerabilidades que sean descubiertas.
- Como responsable de empresa:
    - Es necesario realizar auditorías periódicas de seguridad de la infraestructura y de los activos tecnológicos para determinar las vulnerabilidades que puedan existir.
    - Igualmente conviene estar al tanto de las vulnerabilidades descubiertas para las tecnologías implantadas en la organización, así como de las soluciones ofrecidas por los fabricantes.

- El sistema de clasificación de vulnerabilidades nos permite determinar aquellas vulnerabilidades más críticas para centrar recursos y esfuerzos en remediarlas a la mayor brevedad posible.

Bug Bounty: programas de recompensas para investigadores de vulnerabilidades

Conscientes de la importancia de contar con el apoyo de la comunidad investigadora, hace ya algunos años que las principales empresas tecnológicas y los fabricantes comenzaron a adoptar una estrategia que motivase a los investigadores para decantarse por la revelación responsable de vulnerabilidades. Posiblemente hayas oído hablar de los famosos Bug Bounty, aunque quizá no conozcas exactamente su significado. Se trata de los programas de recompensas económicas que las empresas establecen para *hackers* por reportar vulnerabilidades.

Cuando un investigador reporta una vulnerabilidad a empresas que cuentan con estos programas, recibe a cambio por parte de la compañía una retribución económica proporcional a la criticidad e impacto de la vulnerabilidad, que, dependiendo de la compañía, puede ir desde los 20 000 dólares por una vulnerabilidad crítica hasta los 100 dólares por una de bajo impacto. En algunos casos, la recompensa mínima puede llegar a ser una camiseta de *merchandising* específica o de edición limitada que acredite el mérito del investigador, o incluso simplemente un reconocimiento en el Hall of Fame de la compañía como agradecimiento por su contribución. Aunque es evidente que esto no satisface a nadie del mismo modo que una retribución económica, desde el punto de vista del currículum es prestigioso para los investigadores atesorar este tipo de reconocimientos, más cuando vienen de empresas del calibre de Google, Amazon, Facebook, Microsoft, Yahoo o Apple.

Los primeros programas Bug Bounty vinieron de la mano de Netscape a mediados de los años noventa y de la Fundación Mozilla, que inició el suyo en 2004. Posteriormente, se unieron gigantes tecnológicos como Google en 2010, Facebook en 2011 y Microsoft en 2014. A día de hoy, es una tendencia en auge a la que cada vez se van sumando más compañías, ya no solo de base tecnológica.

> *La recompensa por reportar una vulnerabilidad a través de un Bug Bounty puede ir desde una camiseta hasta 20 000 dólares.*

En su día, fue una aproximación bastante disruptiva, concebida por muchos como una práctica muy arriesgada. Exponer una compañía a ser atacada continuamente por *hackers* a la caza de recompensas podría parecer en principio una mala idea desde el punto de vista de su seguridad interna. Pero con el paso del tiempo, estas compañías han concluido que precisamente el hecho de disponer de estos programas permite que los *hackers* descubran los posibles agujeros y los reporten para ser corregidos antes de que lo hagan los ciberdelincuentes. También evitan que vulnerabilidades en sus productos puedan ser publicadas en modo *Full* disclosure, con el consiguiente daño reputacional que esto podría ocasionar. Cuando hablamos de fabricantes y empresas del mundo tecnológico, la confianza de los usuarios en la seguridad de sus productos es esencial. Es por esto que con el paso del tiempo se ha generado un ecosistema que permite tener satisfechos a investigadores y empresas. Por otro lado, desde el punto de vista económico, muchas empresas han considerado que estos programas de recompensas son en la práctica mucho más rentables que invertir periódicamente en auditorías y test de seguridad para sus sistemas y productos. Con este paradigma, han de desembolsar solo cuando existen vulnerabilidades y siempre dependiendo de la criticidad e impacto de las mismas.

Si te encargas de gestionar la seguridad de una organización, es interesante considerar algunos aspectos al respecto de lo comentado:

- Sea cual sea el tamaño de tu compañía, quizá sería interesante valorar la posibilidad de crear un programa Bug Bounty de cara a tener tus sistemas constantemente auditados.
- Como muchas empresas no tienen experiencia en este tipo de programas, existen compañías, como Bugcrowd, en las que poder delegar la creación y gestión absoluta de estos programas.
- Incluso en caso de no contar con programas de este tipo, si un *hacker* o un investigador reporta una vulnerabilidad, es recomendable prestar atención a la información que nos ofrece y agradecer al menos su contribución.

En la línea de la última afirmación, a lo largo de estos años he descubierto y reportado algunas vulnerabilidades a diferentes instituciones y empresas.

Dependiendo del caso, la experiencia ha resultado satisfactoria, intrascendente o incluso decepcionante. Algunas organizaciones han agradecido el gesto y han dedicado recursos a remediar las vulnerabilidades comunicadas. Otras, han agradecido al menos el gesto sin invertir ni un segundo en analizar la información comunicada ni ser conscientes de la repercusión que el hallazgo en cuestión podría tener. En otros casos, los responsables de la organización simplemente no han hecho nada.

Vulnerabilidades críticas identificadas en la web del Club Deportivo Tenerife

En este sentido, a continuación os cuento un caso digno de comentar que he expuesto con pelos y señales en alguna conferencia, una vez que la vulnerabilidad fue corregida, aunque no precisamente por la buena voluntad del interlocutor de la organización en cuestión.

En el año 2012, la página web del Club Deportivo Tenerife estaba desarrollada utilizando ASP, tecnología de Microsoft que en aquel momento ya empezaba a considerarse obsoleta. Tan solo con un vistazo rápido, alguien con experiencia podía ver que existían numerosas vulnerabilidades. No obstante, también era fácil determinar que, quizá a causa de haber recibido ataques en el pasado, los responsables de fortificar el sitio web habían colocado lo que se conoce como un WAF (Web Application Firewall). Se trata de un cortafuegos que se coloca como puerta de entrada a la web y que filtra todas las peticiones realizadas por los usuarios, cortando aquellas que puedan representar un intento de ataque. Las técnicas utilizadas para explotar las vulnerabilidades más habituales en aplicaciones web implican el uso de determinados caracteres o palabras concretas. Cuando un WAF detecta que alguna petición de un usuario incluye algunas de esas palabras o caracteres, la interpreta como maliciosa y cierra directamente la conexión. Así es como funciona.

En lugar de corregir las vulnerabilidades en el código de la aplicación web mal desarrollada (lo que implica mayor complejidad y tiempo de desarrollo), optaron por esta solución que generalmente suele funcionar muy bien en la mayoría de los casos.

De hecho, la presencia del WAF impedía cualquier intento de explotación de las vulnerabilidades que creía ir detectando en la web del club, por lo que poco podía rascar. Aun así, estaba empecinado en la posibilidad de que existiera alguna situación en la que pudiera explotar alguna vulnerabilidad,

burlando la seguridad del WAF. Tenía la intuición de que era posible, y un día, de manera casi accidental, lo logré. Aún recuerdo la sensación que experimenté en el momento. Pura adrenalina. Había conseguido entrar en la interfaz de administración del portal web del C. D. Tenerife. La forma de hacerlo fue realmente ingeniosa. Fue una de esas ideas felices que forman parte de esto del *hacking*. Una demostración más de que en este mundo, las skills y el pensamiento lateral son determinantes a la hora de identificar vulnerabilidades. Quizá, otro que se propusiera hacer lo mismo, aun con los mismos conocimientos, habilidades o experiencia, igual no daría con la manera de hacerlo por mucho que lo intentara. Es lo bonito, y a la vez en muchas ocasiones frustrante, de este complejo mundo.

La manera en la que exploté la vulnerabilidad me permitió acceder como administrador con máximos privilegios al backend de la web. Entre otras cosas, podía ver los usuarios de los administradores de la web con sus contraseñas… ¡en texto plano! Esto es algo que jamás se debe hacer. Cuando se almacenan contraseñas de usuarios en una base de datos, normalmente se utilizan lo que se conoce como hashes, cadenas que representan cualquier contenido (típicamente una contraseña) utilizando una combinación ininteligible de números y letras de considerable longitud. Se calculan aplicando funciones matemáticas irreversibles, de forma que a partir de la contraseña se puede siempre obtener el hash, pero nunca al revés.

- Backend: interfaz de administración, típicamente no visible de un sistema.
- Hash: representación codificada y cifrada de un contenido para poder almacenarlo con seguridad.

De entre todos los usuarios que podían administrar la web, había algunos con contraseñas tan débiles como «123», «123456», o «7788». También algún caso en que las contraseñas eran iguales que el propio nombre de usuario, como «esteban/esteban».

Visto lo visto, quizá habría sido más fácil probar combinaciones de usuarios con credenciales débiles que explotar una vulnerabilidad.

Además de ver los usuarios, podía controlar por completo la web. Podría haber alterado el aspecto, cambiado las fotos de los jugadores de la plantilla o incluso haber creado nuevas noticias que sembraran el caos entre los aficionados. Con el seguimiento y la popularidad que el equipo tiene en la isla, anunciar el cese del entrenador o la contratación de un nuevo fichaje habría tenido una repercusión mediática considerable. Además, teniendo

acceso al panel de gestión de usuarios, no solo conocía sus contraseñas para poder volver a entrar cuando quisiera, sino que podía modificarlas o revocar el acceso a cualquier usuario legítimo de la web. De este modo, en el caso de publicar, por ejemplo, una noticia falsa, nadie podría volver a actualizarla. Como puedes imaginar, las posibilidades eran infinitas, pues el acceso era total.

Como mi motivación no era la de incurrir en ninguna actividad delictiva o maliciosa, sino la de investigar y probar los límites de la tecnología, lo primero que hice fue ponerme en contacto con el director de comunicación del equipo blanquiazul. Al tener amigos en común, conseguí su teléfono y lo llamé de inmediato. Me atendió amablemente y al contarle quién era y lo que había descubierto, no me hizo mucho caso. Me comentó que «andaba liado». Sugirió que le llamara nuevamente pasadas unas semanas porque el equipo se hallaba inmerso en la vorágine de la competición. Así que, pasado un tiempo, volví a contactarle y su respuesta fue similar. En todo momento me agradeció mi buena voluntad. Pero apenas se esforzó en escuchar en detalle lo que tenía que decirle para poder valorar el alcance de las vulnerabilidades. En esta ocasión, la prioridad era la campaña de abonos. Me instó a llamarle de nuevo, pero desistí y le deseé buena suerte para mis adentros. Si algún día tenían un incidente de seguridad, quizá se acordaría de que alguien le advirtió del problema.

Unos años después, el destino quiso que descubriera otra vulnerabilidad aún más crítica, de manera casual, accediendo a la web como usuario, no como investigador. Fue en el verano de 2015, a mi vuelta de León. Tras dos años ejerciendo como Security Evangelist de INCIBE al máximo nivel, decidí que era hora de volver a mi tierra y continuar mi carrera profesional allí. A pesar de haberme alejado un poco de la afición por el fútbol (ya que no disponía de tiempo ni energía para más *hobbies* que el *hacking*, que convertí en mi profesión), decidí renovar mi carnet de abonado al Club Deportivo Tenerife.

Al acceder a la web, comprobé que la apariencia y la tecnología usada había cambiado un poco respecto a la versión de 2012. No reparé en si la vulnerabilidad descubierta más de tres años atrás aún seguía vigente o no. Posiblemente, al cambiar parte de la web, ya no existiría. Mi intención era la de renovar el carnet de socio, así que a ello me disponía. Enseguida me percaté de que la sección relativa a la campaña de abonos mostraba una apariencia similar a la versión que recordaba de años atrás. Páginas desarrolladas en ASP, aún más obsoleto en 2015 que en 2012. Y es que,

indagando un poco, descubrí que eran las mismas que se usaban en 2012, 2011, 2010, 2009… Cada verano habilitaban esa sección, que se utilizaba simplemente para tramitar las renovaciones y altas de abonados desde la web. No tardé mucho en detectar el primer fallo. Nada más comenzar a gestionar mi renovación, probé a incluir una comilla en uno de los campos del formulario para rellenar. La comilla se utiliza para identificar un tipo de vulnerabilidades conocidas como SQL Injection, que permiten inyectar código desde fuera para realizar consultas, modificaciones u otras operaciones sobre la base de datos de la web.

En esta ocasión, no hizo falta romperse mucho la cabeza. La respuesta que recibí en el navegador me confirmó que existía una vulnerabilidad y que probablemente sería sencillo aprovecharse de la misma. Efectivamente. Al utilizar una herramienta muy conocida que automatiza la explotación de este tipo de vulnerabilidades, comprobé que tenía acceso completo a la base de datos de la web. Una base de datos en la se encontraba la información de los más de ocho mil socios que hasta entonces habían tramitado su abono a través de la web. Con el avance de la campaña de abonos, este número se iría incrementando. De cada socio, entre otras cosas, podía obtenerse lo siguiente:

- Nombre
- Apellidos
- Dirección postal
- Dirección de correo electrónico
- Número de teléfono
- DNI
- Contraseña
- Otros datos

Te puedes imaginar lo que pasaba por mi cabeza al ver cómo los datos de todos los socios del club iban deslizándose por mi pantalla negra con letras verdes a un ritmo vertiginoso, al más puro estilo Matrix. Al ver que podía tener acceso a esta cantidad ingente de información, enseguida detuve la herramienta. Mi intención, como siempre, no era recopilar ni almacenar todos estos datos, aunque un atacante con otros fines podría haberlo hecho sin el menor problema. Podrían estar usando esa información para comercializarla, a favor incluso de candidatos a la presidencia del club, para cuando llegasen las elecciones.

A pesar de que no me apetecía en absoluto, dado el precedente de la ocasión anterior, volví a llamar al director de comunicación. Lo que había

encontrado merecía ser reportado. Estamos hablando de datos personales de miles de usuarios, información de carácter muy sensible que debía tratarse con un nivel adecuado de seguridad. No es ninguna broma. Tras presentarme nuevamente y refrescarle la memoria, le comenté que había encontrado una vulnerabilidad que dejaba al descubierto datos personales de miles de socios de la entidad, información que era fácil de explotar y cualquiera con un mínimo de conocimientos podría acceder a aquellos datos. Con diplomacia, me agradeció nuevamente el reporte, a la vez que me dio la siguiente explicación: «La web la cambiamos en mes y medio, así que de aquí a entonces no tiene sentido hacer nada». En esta ocasión, me preguntó si podía hacer algo en deferencia por mi buena voluntad. Le propuse obsequiarme con el abono que pretendía adquirir y amablemente me dijo que eso era imposible, que el club estaba en segunda división y no se lo podían permitir. Sin comentarios. Educadamente concluí la conversación y me prometí que jamás volvería a reportar nada a este individuo.

Una auditoría de seguridad en la que alguien encontrara esta vulnerabilidad, que yo reporté de manera gratuita y voluntaria, habría costado como poco diez veces más que el abono; también la posible multa que el club podría haber recibido de la Agencia Española de Protección de Datos, en el caso de que cualquiera con intenciones maliciosas hubiese encontrado la vulnerabilidad y hubiese filtrado los datos en la red. Si yo hubiese informado previamente de que había reportado estas vulnerabilidades y que el club no había hecho nada por remediarlas, la sanción habría sido considerable. Como tampoco era mi intención provocar ningún daño a la entidad, volví a dar carpetazo al asunto, esperando que en ese mes y medio nadie identificara la vulnerabilidad.

De todos modos, hasta hace bien poco, la legislación al respecto sobre la responsabilidad de las compañías ante un eventual ataque de este tipo tampoco estaba muy clara. Sin embargo, a día de hoy esto es bien diferente. Con la entrada en vigor del Nuevo Reglamento de Protección de Datos de la Unión Europea (GDPR) en mayo de 2018, las organizaciones tienen el deber de demostrar que cumplen con sus principios de protección de datos, monitorizando, auditando y evaluando con regularidad tanto los procedimientos, como las políticas y la infraestructura tecnológica, así como formando a sus trabajadores en la materia.

Deben tomar medidas técnicas activas para proteger a la organización de ataques, robo de datos y violación de información. Las multas a las que se enfrentan en caso de no cumplir con su responsabilidad son considerables.

Así que ya no hay excusas que valgan. Ya no hablamos de prestar atención a alguien que reporte una vulnerabilidad. Han de ser las propias empresas las que activamente se preocupen de auditar sus sistemas en busca de vulnerabilidades para garantizar la seguridad de la información que manejan. Aunque muchas empresas y organismos ya lo venían haciendo, otras tantas no han dedicado suficientes recursos a este fin y tendrán que ponerse las pilas.

Como último detalle respecto de la información almacenada en la base de datos de la web del Club Deportivo Tenerife, pude comprobar que también estaba accesible la tabla de usuarios del backend de la web, aquellos que descubrí en 2012. Para mi asombro, nada había cambiado. Los usuarios seguían siendo los mismos que tres años atrás, con las mismas contraseñas débiles de entonces, almacenadas en la base de datos en texto plano, listas para que cualquiera pudiera acceder a ellas, ahora incluso desde fuera. Escalofriante a la par que cierto.

De esta historia pueden extraerse varias conclusiones de temas diversos y en diferentes niveles de abstracción. Todas ellas son importantes, sobre todo si recae en ti la responsabilidad de gestionar la seguridad de tu empresa:

- Es recomendable el uso de dispositivos de seguridad como firewalls, WAF o herramientas de detección de intrusos proporcionadas por fabricantes, que ofrecen protección ante gran variedad de ataques, pero no son infalibles.
- Es imperativo contratar auditorías de seguridad con empresas o profesionales especializados en ciberseguridad, con habilidades y experiencia contrastadas para evaluar el nivel de seguridad de la infraestructura y los activos tecnológicos.
- Las auditorías adquieren aún más relevancia a raíz de la entrada en vigor del Nuevo Reglamento de Protección de Datos de la Unión Europea (GDPR). Es recomendable documentarse bien al respecto para asegurar el cumplimiento y evitar posibles problemas en el futuro.
- Si algún *hacker* o investigador reporta una vulnerabilidad de manera voluntaria y sin mayor motivación que la de ayudar, es recomendable valorar la información que aporta, pues en muchos casos redundará en un beneficio para la seguridad de la organización.
- En ningún caso se han de almacenar contraseñas de usuarios en una base de datos en texto plano. Tanto si son trabajadores propios como una empresa externa quien desarrolla el *software* de tu organización, asegúrate de exigirles unas mínimas garantías de seguridad. Son muchas las empresas que siguen sin dedicar esfuerzos a fortificar el

software que desarrollan. Es preferible invertir más y contratar a profesionales con experiencia en desarrollo seguro.

- Es fundamental implantar una política para las contraseñas de todos los usuarios de una organización en la que se les exija una complejidad mínima. No pueden existir contraseñas como «123». En el capítulo 6 abordaremos en detalle los requisitos que se han de cumplir para elaborar una contraseña robusta.
- Los usuarios de una organización no pueden permanecer varios años con la misma contraseña, por muy segura que sea. Se han de modificar frecuentemente y esto ha de considerarse a la hora de definir la política comentada en el punto anterior.

> *Nadie puede protegerse de aquello que no conoce.*

4

Exploits Zero Day, el mercado de las ciberarmas y la respuesta a incidentes

A la hora de plantear los posibles escenarios cuando un investigador descubre una vulnerabilidad, aún queda la posibilidad de que el investigador no la reporte al fabricante (con o sin programa Bug Bounty) y que tampoco publique los detalles de la misma. Si nadie salvo el investigador y quizá un selecto círculo de confianza conoce la vulnerabilidad, es como si esta no existiera ante los ojos del mundo. Quien la conozca y disponga del exploit podrá utilizarla libremente para comprometer los sistemas afectados sin que los usuarios puedan hacer nada al respecto. Ya no solo protegerse, sino tampoco saber cómo han sido comprometidos, ni cuál es el origen del ataque, porque nadie puede protegerse de aquello que no conoce. Y, por supuesto, el fabricante no puede proveer a los usuarios de un parche que remedie la vulnerabilidad, pues ni siquiera es consciente de su existencia.

Esto es algo realmente inquietante, sobre todo cuando se trata de vulnerabilidades críticas que pueden ser explotadas en remoto. Lo es más cuando afectan a productos distribuidos masivamente en el mercado, como por ejemplo Microsoft Office o Adobe Reader, o si las vulnerabilidades afectasen a los propios sistemas operativos (Windows, iOS, Android, Linux…). El caos que podría sembrar alguien con la capacidad de atacar masivamente a cualquiera de estas plataformas sería inimaginable, pues todos estaríamos indefensos ante tal amenaza. Estos exploits, que se aprovechan de vulnerabilidades que no son publicadas ni conocidas por el propio fabricante, se denominan exploits Zero Day. Este apelativo hace referencia al tiempo del que se dispondría para generar un parche, contramedida o defensa para un exploit de este tipo: cero días.

Es algo a lo que todos estaremos siempre expuestos y con lo que tenemos que convivir. De hecho, es algo que perturba enormemente a todos aquellos que conocemos los entresijos de este mundo o trabajamos en el sector de la ciberseguridad: saber que siempre existirá la posibilidad de ser comprometidos por el descubrimiento de una nueva vulnerabilidad. Forma parte del espectro de amenazas ante las que, en teoría, no tenemos posibilidad de protegernos.

Agencias de inteligencia, gobiernos y cibercriminales en la puja por Zero Days

Como puedes imaginar, los exploits Zero Day son altamente codiciados, y su valor económico en el mercado es considerablemente elevado. Varía en función de la criticidad de la vulnerabilidad, así como del producto, sistema o tecnología a la que afecte, pero por lo general los Zero Day no están al alcance de cualquiera.

Son, por tanto, grupos y organizaciones que cuentan con grandes recursos económicos los que invierten para adquirir o pujar por estos Zero Day, dependiendo de las diferentes motivaciones que tengan. Organizaciones cibercriminales de cierta entidad los ansían para poder lucrarse económicamente, explotando masivamente a usuarios y empresas de todo el mundo. Otros grandes compradores de exploits Zero Day se encuentran en las agencias de inteligencia y espionaje de gobiernos de todos los países. La motivación es evidente: disponer de un arsenal de ciberarmas capaz de proteger la seguridad nacional, sea para controlar las comunicaciones de sus ciudadanos e identificar amenazas terroristas o bien para intervenir dispositivos de sospechosos que puedan revelar información importante para investigaciones determinadas, o incluso para recabar inteligencia acerca de otras naciones.

> *Las filtraciones de Edward Snowden sobre los programas de espionaje de la NSA y otras agencias, pusieron en conocimiento del mundo la capacidad ofensiva que tienen los Estados gracias al uso de la tecnología y su motivación para disponer de Zero Days.*

Las cosas han cambiado mucho desde los tiempos de la guerra fría. Hoy día, el espionaje a otros países pasa por la explotación de activos tecnológicos,

como vemos en infinidad de películas o series de ficción. En prácticamente cualquier capítulo de la popular serie Homeland, los agentes de la CIA recurren a su equipo de *hackers* de élite para superar obstáculos que ayuden en sus batallas contra otros Estados u organizaciones terroristas. ¿Y qué mejor manera de hacerlo que comprometiendo dispositivos móviles de sospechosos o servidores de otras agencias? Curiosamente, en un capítulo de la trama, aparecía el concepto Zero Day. Un *hacker* había encontrado una vulnerabilidad no conocida en los sistemas de la CIA y lo aprovechó para acceder a información clasificada.

Ya sabemos que en el mundo de la ficción todo parece más sencillo. Las cosas van más rápido y se pierde cierto rigor, pero lo cierto es que los guionistas de Homeland utilizaron el concepto Zero Day para precisar cómo el *hacker* había conseguido vulnerar los sistemas de la CIA. Probablemente la gran mayoría de espectadores no reparó en el concepto o en su significado. No deja de ser llamativo que llegaran a ese nivel de detalle, más propio de una serie como Mr. Robot, dirigida a una audiencia que sí puede esperar ciertos tecnicismos para explicar los ataques que se van sucediendo en la trama.

Por otra parte, sobre las capacidades ofensivas de las naciones y sus agencias de inteligencia también hemos podido conocer más gracias a las revelaciones que Edward Snowden hizo al mundo en 2013 acerca de los programas de espionaje de la NSA. Durante semanas, asistimos perplejos a las filtraciones que se iban sucediendo sobre las poderosas herramientas de las que disponía la agencia de seguridad estadounidense. Teniendo en cuenta este arsenal, podían acceder prácticamente a cualquier dato o comunicación de todos y cada uno de los ciudadanos del mundo. Además de la todopoderosa NSA, las filtraciones de Snowden pusieron en conocimiento del mundo incidentes de espionaje que implicaban también a otras agencias de inteligencia, como la alemana o el popular GHCQ británico.

Muchas de las capacidades ofensivas de las que disponen todas estas agencias son posibles gracias al uso de exploits Zero Day. Algunos son encontrados por grupos de *hackers* que trabajan para las propias agencias. Tanto la NSA como el GHCQ, por citar algunos, cuentan en sus filas con especialistas dedicados exclusivamente a la búsqueda de vulnerabilidades y exploits Zero Day, debido al incalculable valor que tienen para el trabajo de sus contratantes.

El mercado de las vulnerabilidades

Existe un mercado lícito y legal en el que investigadores, agencias y organizaciones de todo tipo comercializan con Zero Days. Algunas empresas del sector de la ciberseguridad se especializan también en la búsqueda y descubrimiento de este tipo de vulnerabilidades para proveer de herramientas ofensivas a los actores mencionados. Un ejemplo de este tipo de empresas con considerable relevancia en el sector puede ser Vupen. De hecho, su fundador es también conocido por crear Zerodium, una plataforma en línea que pone en contacto a investigadores independientes y compradores de Zero Days. Al igual que en otros mercados, en el de las vulnerabilidades también hay espacio para brókers independientes dedicados a mediar entre las partes interesadas a cambio de una comisión.

Dependiendo de la popularidad de la plataforma en la que se descubra un exploit Zero Day, su coste será uno u otro. Es evidente que un exploit para sistemas Windows, desplegados en equipos por todo el mundo, tendrá un coste mucho más elevado que su homólogo para sistemas Mac OSX. Si bien estos últimos están ganando popularidad entre muchos usuarios e incluso empiezan a usarse en el ámbito corporativo, no se acercan ni por asomo a la cuota de penetración en el mercado de los sistemas Windows. La frecuencia con la que puedan descubrirse exploits para la plataforma o producto atacado, directamente ligada a la dificultad que entraña su obtención, influye en su valor y precio. En este sentido, un exploit para comprometer sistemas iOS será muchísimo más valioso que uno para Android, pues tradicionalmente ha sido difícil romper las estrictas barreras de seguridad que Apple implementa para sus dispositivos.

Principalmente en función de estas dos variables, cuota de mercado de la plataforma tecnológica y dificultad para encontrar amenazas potenciales, es posible estimar *a priori* el precio que podrá tener un exploit. Estos precios suelen anunciarse en plataformas como Zerodium, donde se dan cifras orientativas. Pese a que van variando en función del tiempo y la demanda, un Zero Day para Microsoft Office podría estar entre los 50 000 y 100 000 dólares, mientras que uno para Windows estaría entre 60 000 y 120 000. Un exploit Zero Day para iOS podría superar el millón de dólares.

> *El precio que se puede pagar por un exploit Zero Day para iOS supera el millón de dólares.*

Como es de esperar, pese a que existe un mercado lícito en el que se pueden obtener estimaciones de precios, también existe un mercado más

underground, donde agencias y otros compradores se mueven entre círculos de confianza para la compraventa de Zero Days. En dicho mercado, el precio final también presenta variaciones respecto al precio inicial estimado. Nadie sabe a ciencia cierta si el exploit se descubrirá o no. El valor más importante de los Zero Days es que nadie conozca su existencia.

Lo que hoy es seguro, mañana puede no serlo

Con todo lo expuesto hasta ahora, queda claro que en este mundo es imposible determinar o garantizar nada con total seguridad. Cualquier día un investigador puede encontrar un error en un sistema, dispositivo o programa que lo convierta en vulnerable y, por tanto, inseguro. Es por eso que debemos asumir que lo que hoy es seguro, mañana podría no serlo y ser conscientes de ello para actuar en consecuencia.

Esto no quiere decir que debamos bajar los brazos y encomendarnos a nuestra buena suerte a la hora de utilizar la tecnología. Afortunadamente, son muchas las posibilidades que tenemos para llegar a disponer de sistemas confiables y no permanecer indefensos a la hora de navegar por la red. Los exploits Zero Day constituyen solo una pequeña parte del espectro de amenazas. Es cierto que, ante estos, en teoría poco podemos hacer, pero en la práctica la mayoría de los ataques que se suceden lo hacen exitosamente sin la necesidad de este tipo de exploits. Muchos de ellos sí que se podrían evitar, o al menos contenerlos siguiendo las buenas prácticas de seguridad que vamos desmenuzando a lo largo del libro.

Esta última matización acerca de la contención de ataques es más importante de lo que parece. Aunque hace unos años se trabajaba en la ciberseguridad con el objetivo de evitar que los ataques se produjeran, a día de hoy esta aproximación ha cambiado. Evidentemente, se intenta alcanzar un escenario ideal en el que la organización o el usuario jamás fuera comprometido, pero los años y la práctica han corroborado que se trata de un ideal utópico.

La respuesta a incidentes en el ámbito empresarial

Hoy en día se asume que, dada la frecuencia de intentos de ataque y nuestro grado de exposición a los mismos, en algún momento podemos sufrir vulneraciones. Por ello, a la hora de abordar la ciberseguridad, sobre todo a nivel de una organización, se trabaja haciendo hincapié en lo que se conoce como la «respuesta a incidentes», esto es, en la preparación para responder

adecuadamente en caso de que un intento de ataque derive en un incidente de seguridad. Incluye un protocolo de actuación que ayuda a minimizar el impacto ocasionado sobre nuestra organización, y evitar que los servicios críticos puedan verse afectados, que se sustraiga información crítica o sensible que pueda afectar al negocio o recuperar la operatividad lo antes posible. En definitiva, se trata de prevenir el caos y contener el incidente sin que genere un daño irreparable. Son muchas las organizaciones que por no disponer de un adecuado plan de respuesta a incidentes han sucumbido a los devastadores efectos de un ciberataque, en algunos casos hasta el punto de verse abocadas a la quiebra y la desaparición.

Un ejemplo de las medidas que forman parte de un plan de respuesta a incidentes lo encontramos en la gestión de Telefónica de la crisis de WannaCry en mayo de 2017, el incidente de dimensión mundial que abordaremos con más detalle. Debido a la trascendencia que la multinacional tiene en nuestro país, todo el mundo se hizo eco de una medida que en otros casos nadie tendría por qué conocer. Desde la organización, a través de los servicios centrales de megafonía, se ordenó a todos los empleados que apagaran sus equipos, igual que en una película hollywoodiense. Era esencial aislar los equipos afectados, contener el incidente y evitar que el ataque se pudiese propagar afectando a servicios críticos o a infraestructuras de los clientes.

Pese a la agitación y el revuelo mediático que se generó, en la práctica se consiguió solventar la situación sin perder la operatividad; ni tan siquiera una caída del servicio. Ningún cliente sufrió las consecuencias del ataque, ni una línea afectada, ninguna incidencia en infraestructuras de comunicaciones, en instalaciones corporativas, líneas ADSL… Es más, tras el incidente de WannaCry, la imagen de Telefónica ante sus clientes y la sociedad quedó reforzada. Una gestión impecable de la crisis, tanto en términos de contención y resolución del incidente, como en el ámbito de la comunicación y la transparencia, que en estos casos es igual de importante. En esto se basa la respuesta a incidentes.

A la hora de hablar de medidas que forman parte de la respuesta a incidentes, hemos de diferenciar entre medidas reactivas, como en el ejemplo de Telefónica, y medidas preventivas, que son las que se adoptan para intentar evitar que los ataques se produzcan o al menos para reducir su impacto en caso de que se materialicen.

Si tienes como objetivo gestionar la seguridad de una empresa, ten en cuenta los siguientes aspectos:

- Es indispensable la elaboración de un plan de respuesta ante incidentes en la organización para hacer frente con garantías a cualquier situación que se nos presente en materia de ciberataques.
- No solo las grandes organizaciones cuentan con un plan de respuesta ante incidentes.
- Se debe definir un plan acorde a las dimensiones de la organización. Si tu empresa es una pyme, es evidente que la complejidad del mismo, así como la dotación en recursos, será menor que en el caso de una empresa de mayor envergadura.
- La ciberseguridad es un área que requiere de un alto grado de conocimiento, dedicación continua y especialización. Normalmente, las pymes no cuentan con profesionales expertos en esta materia. Un administrador de sistemas o responsable de TI no tiene por qué disponer de conocimientos de seguridad.
- Por ello, es muy habitual y recomendable externalizar la gestión de la seguridad, delegando esta tarea en empresas y profesionales especializados en la materia que apoyen y asesoren a los responsables de la organización.

En lo que respecta a protegernos de las diferentes vulnerabilidades que se van descubriendo, ya hemos comentado que:

- Es esencial mantener siempre actualizado nuestro sistema operativo con todos los parches de seguridad publicados por el fabricante.
- Lo mismo sucede con todos los programas que tengamos instalados en el equipo.
- Esto aplica también a la hora de hablar de dispositivos móviles.
- Actualizar nuestro dispositivo es fundamental, pues es lo que nos mantendrá siempre protegidos de las vulnerabilidades que se vayan identificando por parte de los investigadores y evitará que nuestro equipo sea comprometido.

Ante un escenario tan complejo, no existen recetas milagrosas ni medidas que por sí solas nos eximan de todo lo que pueda suceder, pero aplicándolas en conjunto sí que pueden conseguir sistemas relativamente confiables. Conforme nos adentremos en el detalle de las diferentes amenazas y los escenarios de ataques más habituales, podremos ver las medidas que se han de aplicar de manera específica para cada uno de ellos.

Ahora que ya hemos introducido los conceptos de vulnerabilidad y exploit relativos a los errores desde el punto de vista técnico, toca incidir en otro tipo de errores: los humanos. Más allá de vulnerabilidades o exploits Zero Day,

gran parte de los complejos ataques que se materializan comienzan comprometiendo al eslabón más débil de la cadena: el usuario final. Por ello es indispensable conocer las diferentes técnicas que los ciberdelincuentes utilizan para este fin. Solo así podremos estar preparados para hacerles frente. Las abordamos en el próximo capítulo, dedicado a la ingeniería social.

5

Cómo evitar ser víctima de la ingeniería social

Kevin Mitnick, o Cóndor, es sin duda el *hacker* más famoso de todos los tiempos. Su época dorada se remonta a los años noventa, una época anterior a las redes sociales, los usuarios accesibles a través de multitud de canales, los sistemas de mensajería instantánea y, por supuesto, los *smartphones*. Aunque apenas había sistemas interconectados mediante redes, los que existían adolecían de medidas de seguridad complejas. Por otra parte, al no existir internet, tampoco se disponía de acceso a información técnica o documentación a golpe de clic. Es por ello que el mérito de las hazañas logradas por Cóndor en aquel mundo prerrevolución digital es considerable y por eso Mitnick es una leyenda viva entre los *hackers*.

Uno de sus primeros ataques consistió en colarse físicamente en las oficinas de Pacific Bell para hacerse con listados de claves de seguridad, la combinación de las puertas de acceso de varias sucursales y manuales de documentación técnica del sistema COSMOS, una base de datos que utilizaban la mayoría de compañías telefónicas para el registro de llamadas. No buscaba sustraer dinero, sino documentación. El valor de la información sustraída se estimó en 200 000 dólares. Para poder penetrar físicamente en las instalaciones de la compañía, tuvo que preparar el engaño con antelación y mimo. No solo mediante la dialéctica, sino también adoptando la vestimenta y el *look* de los trabajadores de la organización. Como en las películas de Hollywood, pero de verdad.

Otra de sus grandes hazañas fue *hackear* a la compañía Motorola y hacerse con el código fuente del último modelo de móvil de la firma antes de que este saliese al mercado. Este ataque fue acometido solamente con llamadas telefónicas. Mitnick se dedicó a llamar a los diferentes departamentos de la organización, averiguando los nombres de los

responsables y escalando jerárquicamente de abajo hacia arriba hasta dar con alguien que le enviaría el firmware por correo electrónico. Esta increíble pero verídica historia pude escucharla de su propia boca en el evento Mundo *Hacker* Day 2014, donde participé como ponente y tuve el privilegio de compartir con él mesa y mantel.

Es cierto que, en su día, Mitnick perteneció al lado oscuro, pero tras ser perseguido durante años por el FBI (a quienes también se anticipaba dejándoles cajas de donuts en su apartamento antes de darse a la fuga), sufrió condena en prisión y a su salida optó por continuar su carrera como un *hacker* ético y no como ciberdelincuente. A día de hoy es dueño de una empresa que presta servicios de seguridad a otras compañías.

Si bien los ataques de Mitnick en aquella época tenían un trasfondo tecnológico, no se caracterizaban por una elevada complejidad técnica, sino que se basaban en el engaño y la manipulación o, más concretamente, en la ingeniería social.

Ingeniería social

El concepto «ingeniería social» no proviene del ámbito de la psicología, aunque guarda estrecha relación con esta ciencia que estudia y analiza el comportamiento del ser humano. Esta conjunción de términos tan peculiar tiene su raíz en el mundo del *hacking*, y su aplicación trasciende el ámbito tecnológico. Se trata de la disciplina que estudia con detalle el comportamiento de las personas para identificar vulnerabilidades que puedan ser explotadas mediante la manipulación y el engaño, con el fin de lograr comprometer su seguridad. Dicho de otro modo, la ingeniería social es el arte de manipular a las personas para obtener de ellas lo que queremos. Así de simple, a la vez que contundente.

Las cuatro claves de la ingeniería social de Kevin Mitnick:

1. Todos queremos ayudar
2. El primer movimiento es siempre de confianza hacia el otro
3. No nos gusta decir «no»
4. A todos nos gusta que nos alaben

En vez de intentar aprovechar la vulnerabilidad de una tecnología, dispositivo o programa concreto, el uso de la ingeniería social tiene como objetivo lograr que sea el propio usuario el que facilite lo que el ciberdelincuente persigue: desde la contraseña de su cuenta de correo, de su banca en línea o el número

de su tarjeta de crédito, hasta la instalación voluntaria de un programa malicioso en su propio equipo, o la desactivación de una medida de seguridad. ¿Cómo se logra esto? Se induce al usuario, mediante tretas y artimañas dialécticas, para que sea él mismo quien allane el camino a la hora de vulnerar su seguridad. Generalmente, es la manera más directa, a la vez que efectiva, para lograr comprometer un objetivo. Por ello, no es de extrañar que sea el arma preferida tanto de *hackers* como de ciberdelincuentes. Es lo primero que intentarán a la hora de planificar un ataque o intrusión. Siempre será más sencillo intentar manipular a un usuario que explotar vulnerabilidades en sus sistemas.

La ingeniería social es el arte del engaño o la persuasión. Un arte que ha existido desde que existe la especie humana. En este caso, se aplica al contexto tecnológico, pero si lo trasladamos a cualquier ámbito de la vida, podremos comprobar que muchos de nosotros utilizamos a diario la ingeniería social en nuestro comportamiento cotidiano con diversos fines, quizá sin saberlo:

- Al intentar sonsacar información sensible, privada o confidencial a un familiar, amigo, compañero de trabajo, etc.
- Al tratar de «colocar» un producto o servicio a un cliente que por cualquier motivo no suponga una buena compra.
- Al flirtear para conquistar a una pareja.
- Al saltarnos la cola de un supermercado, cafetería, discoteca o la atracción de un parque temático utilizando encantos propios o la dialéctica.

Basta con dedicar un rato a pensar en la forma como nos relacionamos con la gente de nuestro entorno para darnos cuenta de que tal vez, en algún momento de nuestra vida, nosotros mismos hemos utilizado la ingeniería social para obtener algún tipo de información o privilegio. Aunque no conociéramos el concepto, sí que éramos conscientes del intento de persuasión, seducción o manipulación que intentábamos ejercer sobre otra persona en aras de alcanzar nuestro fin. O quizá podamos reconocernos como las víctimas de este arte, ejercido por aquellos que saben rentabilizar su verborrea o incluso su atractivo físico.

Si el objetivo es uno de los enumerados anteriormente, generalmente carece de severidad y no llega a resultar perjudicial para nadie, pero la ingeniería social, perfeccionada a través del entrenamiento y utilizada de modo premeditado con fines maliciosos, puede tener efectos devastadores. Su

potencial depende esencialmente de la creatividad del atacante a la hora de urdir la trampa para manipular a su víctima. Tradicionalmente, los ataques de ingeniería social han sido perpetrados mediante llamadas telefónicas o correos electrónicos. Sin embargo, a día de hoy, existen cada vez más medios para lanzar señuelos a los usuarios: foros, redes sociales, sistemas de mensajería instantánea… con lo que las posibilidades para el engaño se multiplican.

La ingeniería social está presente en prácticamente todos los esquemas de ataque que se contemplan en la actualidad. Constituye la fase inicial de la ofensiva en la mayoría de los ataques recibidos por parte de empresas e instituciones. El engaño al usuario es la base. Si el usuario no cae en la trampa, el ataque no se materializa. Por eso es importante conocer el concepto y las diferentes técnicas que utilizan los ciberdelincuentes, con el fin de evitar que nuestras organizaciones sean comprometidas mediante esta poderosa herramienta.

Por lo que respecta a usuarios particulares, además de estar expuestos a los mismos ataques que los usuarios de una organización, también hemos de tener en cuenta los diversos esquemas de fraude que circulan por la red y que utiliza la ingeniería social. Los repasaremos más adelante.

Manipulación y personalización: la clave del éxito

Con excepciones, la gran mayoría de las personas pueden ser manipuladas con éxito, sobre todo a la hora de comprometer su seguridad en el ámbito tecnológico. De ahí que muchos de los esquemas de ataque usados por los ciberdelincuentes para cometer fraude y estafa funcionen a pesar de ser genéricos. Se lanzan de manera masiva para intentar obtener el máximo número de víctimas y resultan rentables porque siempre hay quien pica en la trampa. Si, además, la ingeniería social se prepara de manera personalizada para un objetivo en concreto, recolectando previamente información de su entorno y circunstancias y planificando el ataque a conciencia, aumentan muchísimo las probabilidades de que el atacante logre su propósito.

Podemos encontrar también un montón de ejemplos del uso de la ingeniería social en el mundo de la ficción, sobre todo a la hora de ver cómo actúan los agentes secretos en películas o series de espionaje o acción. Uno que me gusta comentar es el de la película Ahora me ves (Louis Leterrier, 2013), en la que un grupo de magos encandila al mundo con una serie de asombrosos trucos. Uno de ellos consiste en vaciar en tiempo real la cuenta bancaria de un magnate que financia uno de sus espectáculos accediendo a su

cuenta de banca en línea, para lo que previamente han utilizado la ingeniería social. Durante un vuelo, conducen la conversación de la víctima de manera que les proporcione información aparentemente irrelevante sobre su infancia: el nombre de sus padres, el de su perro, la escuela en la que estudió… Esta conversación, en principio intrascendente, les permite obtener las respuestas a las preguntas de seguridad configuradas para su cuenta bancaria.

La buena noticia es que en el mundo real esto no bastaría para reiniciar la contraseña de nuestra cuenta en línea, aunque sí la de nuestro correo electrónico. Los bancos aplican diversas capas de protección para garantizar la seguridad de sus clientes, como el envío de un código de verificación a nuestro móvil para confirmar cualquier transacción.

Fraudes y estafas clásicas que utilizan la ingeniería social

La estafa nigeriana

Uno de los ejemplos clásicos de ataques de ingeniería social es la conocida como «estafa nigeriana». Se le denomina así porque en su día la mayor cantidad de las estafas de este tipo provenían de ese país, generalmente a través de correo electrónico, aunque en el pasado también se veían intentos de estafa vía fax o correo ordinario.

La estafa nigeriana más popular consiste en ilusionar a la víctima con una fortuna proveniente de una herencia o una cuenta abandonada. Hay muchas variantes y señuelos. Se manipula a la víctima con el fin de que adelante una suma de dinero si quiere asegurarse el acceso a la fortuna. En algunos casos, solicitan sumas elevadas, pero insignificantes en comparación con la cantidad económica que las víctimas esperan adquirir. Por supuesto, la víctima nunca recibe ninguna fortuna o herencia. Otras variantes clásicas de la estafa nigeriana son las del premio de la lotería que la víctima nunca jugó, o el Mercedes Benz que obtuvo como premio en un sorteo en el que jamás participó.

Recomendaciones para evitar ser comprometidos

Aunque con el paso de los años muchos de nosotros podemos distinguir claramente este tipo de estafas, los ciberdelincuentes evolucionan continuamente en la creación de nuevos señuelos y mecanismos de engaño. Es por ello que siempre podrán crear una variante capaz de pillarnos

desprevenidos. Por esta razón, conviene tener claras unas mínimas pautas lógicas que nos permitan identificar este tipo de fraudes:

- Si alguien nos ofrece una remuneración económica con la que no contábamos, sin nada a cambio o que no esté justificada, probablemente estemos ante un intento de fraude.
- Si no tenemos ningún familiar en ningún país, no tiene sentido alguno que alguien se acuerde de nosotros para cobrar una supuesta herencia abandonada.
- Si no hemos jugado a ninguna lotería o hemos participado expresamente en algún sorteo, es imposible que nos toque un premio.

En definitiva, ningún desconocido en la red nos regalará jamás nada.

Falsas ofertas de empleo

Esta técnica, en la que se solicita un adelanto económico a la víctima para supuestamente asegurar la consecución de un bien de mayor valor, se sigue utilizando en muchos esquemas de fraude en la red a día de hoy. Los más habituales son las ofertas falsas de empleo. En estos casos, se ofrece a la víctima un puesto de trabajo en otra ciudad o país, con una remuneración mayor a la esperada y por encima de la correspondiente a su categoría profesional. Se les informa de que el puesto es prácticamente suyo, y con la excusa de cubrir costes de viaje y estancia de los distintos candidatos implicados en el proceso, se solicita a la víctima un adelanto inicial que le permitirá acceder a una última entrevista de trabajo, justo antes de conseguir el puesto. Una vez confirmados los supuestos flecos pendientes, a los participantes les sería devuelta la cantidad invertida junto con su remuneración salarial. Obviamente, toda la trama es pura ingeniería social. No existe tal puesto de trabajo y la víctima jamás recuperará el dinero adelantado.

Recomendaciones para evitar ser comprometidos

- Pese a que existen los golpes de suerte, por lo general no es habitual que en el mercado laboral se encuentren puestos de trabajo con remuneraciones muy por encima del salario medio que corresponde a una determinada categoría o perfil profesional.

- En caso de que nos ofrezcan cualquier cosa que se salga de lo normal, debemos sospechar.
- Nunca nadie que nos ofrezca un puesto de trabajo nos exigirá un adelanto económico para cubrir gastos de desplazamiento. Bien distinto será que nosotros optemos a un puesto de trabajo que esté en otra ciudad o país y que asumamos por cuenta propia el coste del viaje, pero hablamos de situaciones diferentes.
- Por otra parte, siempre es vital contrastar la información. En este caso, no está de más pedir información de la empresa en la que se ofrece el puesto de trabajo, aunque quien nos contacta se haga pasar por un headhunter o por empresa de reclutamiento.
- En el caso de que tengamos dudas, podríamos contactar con la empresa y preguntar si realmente existe esa oferta de empleo. En ese caso, comprobaríamos que se trata de una estafa.

El comprador extranjero

También están a la orden del día las estafas asociadas a la compraventa de vehículos por internet. Si bien todos hemos pensado alguna vez en la posibilidad de que alguien intente estafarnos cuando vamos a comprar cualquier cosa a través de la red, quizá somos más descuidados o inconscientes cuando somos nosotros los que vendemos. En el caso de la venta de un vehículo, suele producirse el intento de estafa cuando se nos presenta un potencial comprador que reside en otro país. Veamos cómo funciona:

- Damos de alta un anuncio de venta de un vehículo en diversos portales de la red con un precio acorde al mercado.
- Aparece un comprador potencial que generalmente acepta la compra del vehículo sin negociar apenas el precio o probarlo, lo cual ya podría generarnos cierta desconfianza.
- Nos comenta que reside en otro país, de ahí la imposibilidad de quedar para ver el vehículo. Afirma que se dedica de todas formas a la compraventa de vehículos y que tiene experiencia, por lo que sabe que el nuestro está en buenas condiciones.
- Nos informa de que un colaborador suyo que sí reside en nuestro país será quien recoja el coche para enviárselo.
- Al cabo de unos días, nos confirma la ejecución correcta del pago pactado.

- Además de abonarnos la cantidad pactada, nos ha transferido una cantidad extra para cubrir los costes de la logística de envío del vehículo.
- A continuación, nos pide que hagamos una transferencia con este excedente a su colaborador, para que pueda contar con el dinero necesario para mover el vehículo.
- Son varias las alternativas para convencernos de que el pago ha sido realizado: desde un justificante falso de pago a través de PayPal, hasta un justificante de transferencia de un banco extranjero, con llamada telefónica incluida para confirmarnos el ingreso del dinero en nuestra cuenta. Obviamente, todo es falso.
- Si hacemos la transferencia, habremos perdido el dinero y la estafa habrá sido un éxito.

Existen otras variantes que, en lugar de utilizar como excusa el dinero para la logística, alegan, por ejemplo, el pago de comisiones por recibo de transferencia que nosotros, como vendedores, hemos de abonar para poder retirar el dinero. La ingeniería social se aplica de tal modo que resulta extremadamente convincente. En muchos casos, es complicado detectar que estamos siendo víctimas de una estafa.

Recomendaciones para evitar ser comprometidos

Pese a que la historia puede resultar convincente, hay varias maneras de desenmascarar este tipo de estafas o determinar si estamos siendo víctimas de un engaño.

- En primer lugar, el hecho de que un comprador potencial decline ver el vehículo antes de adquirirlo ya suscita sospecha.
- Por otra parte, si verdaderamente tiene un colaborador en España que va a gestionar la compra del vehículo, podríamos pedirle los datos de contacto. No solo un correo electrónico, sino el teléfono, su actividad profesional, la empresa para la que trabaja… y contrastar la información.
- Lo normal es que nos facilite un correo electrónico falso, puesto que no existe tal colaborador. En ese momento ya podríamos determinar que se trata de una estafa.
- Si recibimos un justificante de pago de Paypal, deberíamos entrar a nuestra cuenta de PayPal directamente a través del navegador, sin seguir enlaces insertos en el correo electrónico, pues probablemente

nos llevarán a una réplica de la página que no es auténtica. En ese caso, también concluiríamos que se trata de un engaño.

- Lo mismo es aplicable al recibir una llamada de un supuesto trabajador de un banco extranjero confirmándonos el ingreso de un dinero a nuestro nombre. A veces, aun cuando ni siquiera hemos facilitado nuestro número de cuenta. En caso de tener dudas, deberíamos acudir a nuestro banco para verificar que realmente alguien ha ingresado dinero. Comprobaremos que evidentemente se trata de un engaño.
- Por último, que nos pidan realizar una transferencia cuando somos nosotros los vendedores es algo que no es habitual ni se justifica. Es la última señal que nos debe alertar de que se trata de una operación fraudulenta.

La novia rusa de Facebook

No faltan por supuesto los intentos de estafa que utilizan el señuelo del amor o la conquista, generalmente femenina. Una novia rusa, rumana, brasileña o de cualquier nacionalidad que llama nuestra atención y se ha enamorado locamente de nosotros, o nos pide ayuda para poder cruzar la frontera y venir a nuestro lado. En el pasado, estos intentos de estafa a través de correo electrónico proliferaban. Hoy en día, suele ser más habitual que los ciberdelincuentes creen perfiles falsos en redes sociales como Facebook para utilizar este señuelo, ya que resulta más convincente. Lo que sucede después de que la víctima caiga en la trampa puede variar: intentos de hacer que facilite dinero o incluso esquemas de extorsión si el usuario ha realizado alguna acción que pueda comprometerlo, como por ejemplo el intercambio de imágenes eróticas a través de la webcam.

Recomendaciones para evitar ser comprometidos

Aunque este tipo de engaños pueden ser fáciles de identificar, puesto que llevamos años escuchando sobre ellos, siempre hay quien puede caer en la trampa. Los ciberdelincuentes detrás de este tipo de fraudes generan perfiles falsos cada vez más perfeccionados para interactuar con la víctima. Envían fotos, chatean con sistemas de mensajería y pueden invertir largos períodos de tiempo en convencer a sus víctimas. En este caso, tenemos que ser capaces de identificar lo evidente:

- Nadie se enamora de nosotros sin conocernos. Inmediatamente después de agregarnos, sin haber mediado palabra, nos declara su amor y quiere acudir a nuestros brazos. Esto no tiene ningún sentido.
- El hecho de que nos envíe fotos no quiere decir que sea real.
- Incluso si se conecta con nosotros por videoconferencia a través de la webcam, no implica que sea real, ni que exista. Existen aplicaciones que permiten sustituir las imágenes de la webcam por un vídeo pregrabado, haciendo creer al que está al otro lado que está viendo a su interlocutor en directo.
- Si hemos pasado por alto todos estos indicios, el momento en que nos solicita dinero para costearse un viaje y conocernos debería activar nuestros sistemas de alerta y ayudarnos a detectar que se trata de un fraude en toda regla.

Aplicaciones fraudulentas

Otro vector de ataque en el que los ciberdelincuentes explotan la ingeniería social es en el mercado de las aplicaciones móviles fraudulentas, que se ofrecen al usuario con funcionalidades milagrosas y casi nunca cumplen su fin. En cambio, suscriben a la víctima a servicios de mensajería SMS *premium* o llamadas de tarificación especial. De este modo, monetizan la estafa. No sustraen elevadas sumas de dinero a cada usuario comprometido, pero esto hace que sea más difícil de detectar por parte de las víctimas, quienes en muchos casos no llegan a denunciar la estafa. Esto permite que la aplicación no sea identificada como maliciosa y que los ciberdelincuentes continúen lucrándose económicamente hasta que sean detectados.

Un ejemplo es la aplicación WhatsApp Spy. Ofrecía al usuario la posibilidad de *hackear* mágicamente las conversaciones de cualquier contacto tan solo introduciendo su número de teléfono. Seguro que eres capaz de ver el engaño a la primera de cambio. *Hackear* WhatsApp no es trivial, y si WhatsApp Spy funcionara correctamente, sería totalmente ilegal. Evidentemente, la aplicación no cumplía con su cometido, y en lugar de espiar conversaciones, estafaba al que la instalaba vaciándole su cuenta corriente a partir de una suscripción a un servicio de mensajería SMS *premium*.

La red está llena de estafas similares que cada día se aprovechan de la ingenuidad de los internautas para incitarles a descargar una aplicación fraudulenta que no implementa la funcionalidad ofrecida, y por contra, repercute en la economía de los estafados, sustrayendo pequeñas cantidades

aparentemente imperceptibles, en lugar de grandes sumas de dinero, de modo que en muchas ocasiones el desfalco es difícil de localizar. Este es el gran secreto de la estafa. Ningún usuario va a denunciar si la cantidad que le roban es de 1,50 euros. Más aún en casos como los de WhatsApp Spy, en el que tendría que declarar la descarga de una aplicación ilícita que atenta gravemente contra la privacidad e intimidad de otras personas. Esta aplicación fue creada por un joven de Murcia, que fue identificado y detenido allá por 2013. Se calcula que recaudó cerca de 40 000 euros por el sistema de SMS.

Recomendaciones para evitar ser comprometidos:

- Efectivamente, las aplicaciones milagrosas no existen.
- Por norma, cualquier aplicación que no haya sido descargada en las tiendas oficiales de aplicaciones, como la Apple Store o Google Play, es susceptible de ser fraudulenta.
- Incluso habiendo descargado una aplicación potencialmente sospechosa, tenemos el control sobre la misma a la hora de asignarle permisos. Es cuando podemos identificar aplicaciones maliciosas o fraudulentas.
- Si una aplicación nos solicita permiso para enviar mensajes, hacer llamadas o acceder a internet sin motivo aparente, es probable que estemos ante una aplicación fraudulenta.
- Como ejemplo, a lo largo de los años han surgido muchas aplicaciones «linterna» para iluminar nuestro teléfono móvil, que solicitan estos permisos y que son fraudulentas. Una aplicación de linterna no necesita acceder a internet, enviar mensajes ni hacer llamadas. Además, se trata de una funcionalidad integrada en la gran mayoría de los *smartphones* y que hace innecesaria su descarga.

Consejos comunes a la hora de identificar esquemas de fraude mediante ingeniería social

Hemos señalado aspectos específicos que debemos tener en cuenta para identificar diferentes tipos de estafa. Aun así, existen una serie de patrones más o menos comunes a todas ellas. Conociéndolos, evitaremos ser comprometidos:

- En muchos casos, podremos ver faltas de ortografía o errores gramaticales en el lenguaje que nos ayudarán a darnos cuenta de que

hablamos con un interlocutor que no maneja nuestro idioma y que se dedica a la estafa sistemática.

No obstante, los ciberdelincuentes han profesionalizado mucho la ingeniería social, y en algunos casos estos errores gramaticales o fallos ortográficos pueden no estar presentes. Obviamente esto no quiere decir que no pueda tratarse de una estafa y deberemos estar atentos a otros indicios.

- Generalmente, no nos facilitan datos personales o empresariales reales que nos permitan obtener más información de la que ellos nos dan. El contacto es a través de correo electrónico, redes sociales o sistemas de mensajería. Si probamos a pedirles un número de teléfono para hablar, comprobaremos que nos responden con evasivas.
- Si existe información de contacto de la empresa o de quien sea que está detrás, es limitada. Es la que ellos han creado para engañarnos. En la mayoría de los casos, no existe ningún tipo de información fuera del sitio web o el canal que nos han facilitado.
- Asimismo, la persona de contacto no tiene perfiles de redes sociales como Twitter, Facebook o LinkedIn en los que comprobar su nombre, ver fotos, publicaciones convencionales o interacciones con otros usuarios de su localidad, su país de residencia, su empresa… Es posible que no hayas caído en verificar este tipo de cosas, pero es lo que te permitirá distinguir claramente cualquier tipo de fraude, y esto es extrapolable a cualquier intento de ingeniería social.
- Es esencial buscar toda la información posible que exista sobre la persona en cuestión de cara a contrastar la veracidad de los hechos. En este tipo de situaciones, enseguida identificaremos que algo no concuerda, por lo que podría tratarse de una estafa.
- Como el objeto de la estafa es lucrase económicamente a nuestra costa, nos solicitarán en algún momento una transferencia o envío de dinero, insistiendo mucho en que una vez realizada obtendremos nuestro beneficio.

En algunos casos, intentarán utilizar sistemas de pago no trazables para evitar que el rastro del dinero pueda llevar hasta ellos.

En definitiva, a la hora de recibir cualquier tipo de comunicación en la red que no venga de alguien que conocemos y que nos inspira confianza, siempre debemos:

- Cuestionar por defecto todo lo que nos diga.

- Extremar la precaución a la hora de facilitar información personal o profesional sobre nosotros que pueda exponernos o comprometer nuestra seguridad tanto física como digital.
    - No facilitar nuestra dirección de residencia si no es necesario.
    - No dar detalles sobre nuestra vida privada.
    - No enviar fotos nuestras ni vídeos de alto contenido erótico que no nos gustaría que se difundiesen.
- Contrastar la información que nos facilita la otra persona por otros canales o medios: un número de teléfono, buscar información en la red…
- Utilizar siempre el sentido común. Nadie nos va a regalar nada, nadie da duros a cuatro pesetas y nadie se enamora de nosotros sin conocernos.
- Ante la mínima sospecha o aspecto que no nos cuadre, lo más seguro es abortar la operación que estábamos considerando.
- En caso de haber caído en alguna de estas estafas, no hay que pensarlo dos veces para denunciar lo ocurrido ante las Fuerzas y Cuerpos de Seguridad del Estado que se encargan de velar por nuestra seguridad en este ámbito:
    - El Grupo de Delitos Telemáticos de la Guardia Civil <https://www.gdt.guardiacivil.es>.
    - La Brigada de Investigación Tecnológica de la Policía Nacional <https://www.policia.es/>.

Ataques de *phishing*

Además de en las estafas tradicionales que hemos repasado o en el fraude a través de aplicaciones maliciosas, la ingeniería social está presente en uno de los métodos de ataque estrella utilizado por los ciberdelincuentes a la hora de comprometer usuarios: el *phishing*, un concepto del que la mayoría de las personas han oído hablar alguna vez, aunque no tengan tan claro en qué consiste.

El nombre proviene del término inglés *fishing*, por la estrecha similitud que guarda con la actividad de la pesca. En este caso, son los usuarios en lugar de los peces los que han de morder el anzuelo, y son conducidos a él mediante la ingeniería social.

El objetivo de los ataques de *phishing* es robar a los usuarios las credenciales de acceso a cualquier servicio, típicamente el de usuario y la contraseña. Para ello, los ciberdelincuentes suplantan la identidad de

proveedores de servicios bancarios en línea o bien de proveedores de correo electrónico como Gmail o Outlook, o de redes sociales como Facebook, Twitter, Instagram y Linkedin. ¿Cómo lo hacen?

- Se envía al usuario un correo electrónico modificando la identidad del remitente con una dirección de correo que simula su pertenencia a la empresa o servicio que pretende suplantar.
- Dependiendo de la sofisticación del ataque y el señuelo utilizado, en el correo se pueden solicitar directamente los datos al usuario a través de un formulario o se le induce a pinchar en un enlace que lo lleve directamente a ver una determinada publicación con fotos o cualquier otra cosa que pueda suscitar su interés.
- Este enlace conduce al usuario a una página falsa de inicio de sesión. Una réplica exacta del sitio web original.
- Una vez que el usuario introduce sus credenciales en el formulario de acceso, estas son almacenadas en un fichero o base de datos gestionada por los ciberdelincuentes.
- A continuación, se redirige al usuario al sitio web legítimo haciéndole creer que se ha equivocado al teclear la contraseña.
- Al volver a introducir sus datos, esta vez en la página original del servicio, inicia sesión correctamente y no se percata de que en el proceso le han sustraído sus credenciales.

Este es el esquema tradicional de un ataque de *phishing*. Más allá de la página falsa en la que aterriza el usuario, lo realmente importante es la ingeniería social con la que se le manipula para hacerle caer en la trampa. De esto dependerá el éxito o fracaso del ataque.

Vishing: *phishing* telefónico

El *phishing* es una de las amenazas de internet que más se ha aireado en los últimos años y quizá por eso es de las más conocidas entre muchos usuarios de la red. Es una cuestión recurrente entre los que nos dedicamos a la concienciación de los usuarios, tanto a nivel general desde los medios de comunicación como en sesiones de formación especializada para el personal de las empresas. Aun así, lamentablemente son muchos los que siguen cayendo víctimas de estos ataques, que llevan sucediéndose prácticamente desde que existe internet.

Antes incluso de internet existía el *phishing* en otra modalidad: la de la llamada telefónica. Si por desgracia fuiste objeto de este tipo de fraude,

seguramente te sonará. Se trata de un medio clásico para acometer estafas de diverso tipo mediante el uso de la ingeniería social. Cuando se aplica directamente para intentar obtener credenciales o información sensible de la víctima (usuario, contraseña o numeración de la tarjeta de crédito), estamos ante un ataque de *vishing*, o lo que es lo mismo, *phishing* telefónico.

Incluso con toda la información que existe en la actualidad sobre estos temas, muchos usuarios siguen cayendo en la trampa de los estafadores mediante una simple llamada telefónica. Aunque no caigan a la primera de cambio, acaban sucumbiendo si los atacantes preparan a conciencia la ingeniería social.

Una de las formas que tienen las empresas de protegerse ante un ciberataque es educar a los trabajadores para hacer frente a intentos de *phishing* o *vishing*, puesto que es uno de los primeros métodos que intentarán los ciberdelincuentes para penetrar en la organización.

Esta educación empieza con la formación del personal mediante actividades para conocer y concienciarse de los riesgos existentes, pero también implica preparar, desde la misma organización, campañas de *phishing* o *vishing* contra sus propios empleados, para comprobar su capacidad de resistencia frente a estos ataques.

He participado en muchos ejercicios de este tipo y resulta realmente sorprendente la cantidad de empleados de distintas organizaciones a los que pudimos comprometer mediante *phishing* y *vishing*. Suplantando la identidad de un compañero del departamento de soporte o de IT y mediante un poco de conversación, conseguía que muchos empleados de grandes organizaciones me facilitasen sus credenciales por teléfono. En algunos casos, lo hacían con algo de recelo o duda, porque a veces estaban avisados de la realización de estas campañas, pero es ahí cuando verdaderamente entra en juego la ingeniería social. Si simplemente se tratase de llamar a un usuario, presentarnos como compañeros de sistemas y pedirle sus credenciales, no tendría sentido hablar de «ingeniería». El primer impulso de la mayoría de los usuarios, más cuando se trata de trabajadores de una organización y está en juego su puesto de trabajo, es el de desconfiar si alguien extraño les pide información sensible. Pero, aun así, en muchos casos lograba convencerlos de que era alguien de su propia organización empleando un poco de encanto y las técnicas de la ingeniería social.

El objetivo de estas campañas no es otro que el de hacer a la organización más resiliente frente a estos ataques. Al final de estas simulaciones, los usuarios que habían sido comprometidos eran informados de que se trataba de

un ejercicio por parte de la organización y recibían formación sobre buenas prácticas para evitar futuras amenazas reales. Gracias a este tipo de experiencias, los trabajadores y usuarios quedan concienciados prácticamente de por vida para no volver a caer en estos engaños, tanto en el ámbito corporativo como en sus cuentas personales.

Esta es la manera más efectiva y recomendable que tienen los responsables de seguridad de una organización para protegerse contra el *phishing* o el *vishing*. Es preferible que los trabajadores caigan en señuelos preparados a conciencia por su propio departamento de IT, sin ningún peligro real. En una sociedad cada vez más hiperconectada, este tipo de entrenamientos se vuelven críticos para la seguridad de las personas y la integridad de las organizaciones.

Buenas prácticas para evitar ser víctimas del *phishing* o el *vishing*

Como en los esquemas de fraude mediante ingeniería social, existe una serie de indicios que debemos tener en cuenta para evitar la caída en esquemas de *phishing*. Es fundamental interiorizar estas pautas, ya que el *phishing* generalmente constituye la vía de entrada de los ciberdelincuentes para otros ataques más complejos dentro de las organizaciones:

- Tener clara una máxima: ningún proveedor de servicio (banco, red social, correo electrónico…) ni personal de nuestra organización nos va a pedir jamás por correo electrónico o por teléfono nuestra contraseña. Nunca.
- Lo anterior es aplicable a cualquier dato sensible que deba ser privado: numeración de la tarjeta de crédito, el pin, la tarjeta de coordenadas…
- Incluso en aquellos casos en los que se produjese cualquier incidencia técnica que obligase al proveedor a *resetear* nuestra cuenta, nos facilitarían un enlace para poder restablecer nuestra contraseña, pero nunca nos la pedirían.
- Ante cualquier comunicación, ya sea telefónica, a través de mensajes, correo electrónico o mediante sistemas de mensajería instantánea como WhatsApp, en la que se nos solicite nuestra contraseña, la norma es desconfiar. Lo mejor es ni siquiera responder o colgar el teléfono si nos han llamado.
- A la hora de recibir cualquier correo electrónico que provenga de una red social, de nuestra entidad bancaria o de nuestra propia

organización que incluya un enlace para acceder a la web del sitio, es preferible evitarlo.

- Incluso si se trata de un correo y un enlace legítimos, es preferible abrir el navegador y teclear la dirección del sitio web para asegurarnos de que estamos en el portal original y no en una página falsa con idéntico aspecto.
- En caso de que hayamos seguido un enlace o el propio correo de *phishing* incluya un formulario con la imagen corporativa de la entidad que trata de suplantar, tendremos ocasión de identificarlo antes de que sea demasiado tarde.
    - En algunos casos podremos apreciar detalles del estilo o de la imagen corporativa que nos resulten diferentes y que puedan ser evidencia de que se trata de una réplica del sitio original.
    - Existen intentos de *phishing* más burdos y otros más sofisticados, por lo que incluso si la imagen corporativa es exactamente igual debemos de extremar la precaución siguiendo estas indicaciones.
- A la hora de incluir nuestras credenciales en cualquier página de inicio de sesión de un servicio, debemos verificar siempre la barra de direcciones del navegador para comprobar que estamos en la dirección correcta.
- La mayoría de servicios de cierta entidad que utilizamos a día de hoy, como las redes sociales, los portales de banca en línea, el correo electrónico o la intranet de nuestra organización, nos ofrecerán acceso mediante el protocolo HTTPS, que se refleja mediante la imagen de un candado en el navegador. Debemos verificar que esto se cumpla siempre.
- Si recibimos un correo electrónico de un contacto conocido, pero no lo esperábamos o nos parece raro, debemos contrastar la información, llamándolo o preguntándole si efectivamente nos ha enviado el correo. En ningún caso hay que seguir cualquier enlace o archivo adjunto incluido en estos correos.

6

Una historia de amor: Arturo, María y el Erasmus

La siguiente historia ocurrió allá por el año 2003 o quizá 2004. Por aquel entonces, yo estaba aún en la universidad. Aunque no retuve la fecha exacta, sí recuerdo con detalle los sucesos de esta historia que jamás he compartido en ninguna entrevista o conferencia, porque es una de esas que en realidad no se deberían contar, pero que casi todos los *hackers* han vivido. O tal vez me lo estoy inventando todo y esta historia solo ocurrió en mi imaginación, en un universo paralelo.

—Tienes que ayudarme, por favor, tienes que ayudarme —me repetía Arturo constantemente y de forma obsesiva.

Durante aquella etapa, Arturo era uno de mis mejores amigos, aunque con el paso de los años se ha quedado en un mero conocido con el que a veces me encuentro por casualidad. Supongo que la vida nos ha llevado por caminos diferentes, y que hubo un antes y un después tras lo ocurrido.

Arturo estaba realmente desesperado. No por problemas económicos ni de salud, sino por amor. Con veintipocos años que teníamos, su amada novia había decidido irse unos meses de Erasmus a un pueblo de Inglaterra.

Seguramente no hace falta que siga para que imagines lo que tenía atormentado a Arturo. Invocando al refranero, dicen que «amor de lejos, amor de pendejos»; y, efectivamente, desde que Arturo y su novia María mantenían una relación a distancia, se habían distanciado, a pesar de los esfuerzos de ambos por mantener la pareja a flote. No solo estaba la limitación geográfica, sino las distintas realidades que vivía cada uno: él seguía su rutina en la tranquila y cálida isla de Tenerife, esperando cada día a que llegara la hora de hablar con su novia; ella estaba a miles de kilómetros de casa, rodeada de otros jóvenes estudiantes en su misma condición, conviviendo permanentemente en un ambiente de fiesta, locura y lujuria desenfrenada,

bajo el pretexto de una estancia académica en el extranjero. No tengo experiencia en Erasmus, pero así se sintetizan a menudo los testimonios que he escuchado en múltiples ocasiones.

En fin, la pareja no pasaba por su mejor momento. La vuelta definitiva de María a casa era inminente, y las sensaciones con las que cada uno afrontaba su regreso eran radicalmente opuestas. Arturo aguardaba expectante el momento de reencontrarse con su amada y María se mostraba reticente a la idea, inapetente, con la intención de evitar o prolongar todo lo posible aquel encuentro. Aquello no era ni mucho menos normal, y Arturo lo sabía. Él entendía que un halo de nostalgia y tristeza acompañara a María en su vuelta, pues cuando concluye una etapa tan intensa, se apagan los focos y la adrenalina se esfuma, es normal decaer un poco. Pero eso era una cosa y otra bien distinta la apatía y la desidia que mostraba María ante el reencuentro. Aunque yo no lo sabía entonces, posiblemente la relación se había desgastado con la acumulación de discusiones durante aquella etapa.

—Tiene que haber pasado algo, alguien, no sé… Algo que no me está diciendo.

—Tranquilo Arturo, cálmate —le decía yo—. Espera a verla y sabrás lo que pasa. No merece la pena que te vuelvas loco. (Qué fácil es aconsejar cuando no eres tú el que lo sufre).

—No. Sé que hay algo. Dipu… (el diminutivo natural de mi nombre), ¿tú no podrías entrar en su cuenta?

—¿Eh? ¿Yo? ¿Qué dices, tío?

—Sí, tú estudias Ingeniería Informática, estás terminando, y eres muy bueno en lo tuyo. Seguro que puedes entrar en la cuenta de correo de María o en la de alguna amiga, no sé.

—¡Qué dices, Arturo! ¿Estás loco? Yo no sé hacer eso, y por otra parte, no te olvides de que es completamente ilegal. Vamos, eso creo.

—Tienes que intentarlo por favor. Te aseguro que me estoy volviendo loco. Le he preguntado, le he suplicado y no me queda nada por intentar. De verdad que no te lo pediría si no fuese cuestión de vida o muerte, por favor, ayúdame.

La fibra sensible y la curiosidad

En aquel momento, algo me tocó la fibra sensible. Arturo lo estaba pasando realmente mal, os lo aseguro. No podía ser plato de buen gusto pedirle a su

amigo que intentara *hackear* la cuenta de su novia para facilitarle acceso a toda su intimidad, acceso del que evidentemente, yo también dispondría.

Lo cierto es que si a un Arturo abatido por las circunstancias, le sumamos el reto técnico, intelectual y humano que su petición suponía para mí, se puede imaginar que, tras dudarlo inicialmente y sin darle aún una respuesta, empecé a investigar si era posible hacerlo.

En 2004 no existían aún Facebook, Twitter, ni LinkedIn. No había redes sociales, ni sistemas de mensajería móvil como WhatsApp o Telegram. No se hablaba tanto de *hackers* ni de ciberseguridad, ni de amenazas o riesgos en la red. Estábamos en la época en la que un usuario medio disponía de una cuenta de correo de Hotmail y utilizaba asiduamente el MSN Messenger. El primer sistema de mensajería instantánea que fue tan popular durante un tiempo, y que quizá te tuvo más de una noche en vela.

El objetivo estaba claro: intentar hacerse con las credenciales de acceso a la cuenta de correo de María o de alguna de sus amigas más íntimas, con el fin de revelar información sensible y útil para los propósitos de Arturo.

Durante aquella etapa en la historia de internet, si alguien buscaba en Google o Yahoo cualquier cosa relacionada con robar o *hackear* cuentas de Hotmail, la mayoría de los resultados llevaban a foros de *hackers* donde se intentaba engañar con ingeniería social básica a los script kiddies o lammers que iban entrando. Y lo cierto es que algunos caían a pesar del evidente engaño. A estos script kiddies se les respondía que, para obtener la contraseña de la cuenta que querían comprometer, solo tenían que enviar un correo desde su propia cuenta a una dirección del tipo bot343x453435bvdj3@hotmail.com, que correspondía a la dirección del bot de Microsoft. Indicaban al usuario que en dicho correo debían incluir, a modo de campos separados por tabulación o líneas, la siguiente información:

- La cuenta de correo que querían secuestrar.
- Su cuenta de correo.
- Su contraseña.
- Cualquier otra tontería que distrajese al usuario de lo que realmente estaba sucediendo.

Como puedes imaginar, la cuenta «bot…@hotmail.com» no correspondía al bot de Microsoft. Era una cuenta más de Hotmail creada por alguien del foro. Cuando el script kiddie enviaba la información de sus credenciales, acto seguido su cuenta era comprometida. Era un castigo tanto por ser un script

kiddie como por ser tan ingenuo de caer en la trampa. Otro ejemplo de uso de la ingeniería social.

Volviendo al tema que nos ocupa, yo sabía que la forma más plausible de poder lograr el objetivo que tenía en vilo a Arturo era la de intentar crear una página que replicara la página de inicio de sesión de Hotmail, pero que en realidad no fuera la legítima, y hacerle llegar esta página a María mediante un señuelo. Te suena de algo, ¿verdad?

Si a día de hoy, con la cantidad de información disponible, aún son muchos los usuarios que caen en ataques de suplantación de identidad o *phishing*, puedes imaginar el escenario hace más de diez años. En ausencia de redes sociales, de la red 2.0, y de tantas advertencias acerca de amenazas o sobre seguridad informática (el término ciberseguridad ni siquiera existía), los ataques por *phishing* escapaban al conocimiento de la mayoría de los mortales. Del mismo modo, no existían tantas herramientas ni posibilidades como ahora para poder emprender estos ataques. Así que me puse manos a la obra. Eran mis últimos años en la facultad y aunque apenas había visto nada acerca de desarrollo web, comencé a investigar qué necesitaba para desarrollar la página que suplantara el sitio web de Hotmail.

Una de las frases más repetidas por todos mis profesores durante aquella época, con la que coincido enormemente, y que de hecho cito a menudo en entrevistas o conferencias, es que, durante la carrera, más que centrarnos en aprender una u otra tecnología, debíamos «aprender a aprender». Para mí no hay afirmación más certera aplicable a esta disciplina. Si hay algún sector en el que debemos aprender continuamente, leer, probar, experimentar, errar una y otra vez, así como dedicar horas y horas a la investigación, es el de la informática. Es por eso que solo aquellas personas a las que realmente les apasione esto perdurarán.

No tardé mucho en tener lista la página réplica de Hotmail en un servidor web, que corría en el ruidoso ordenador que tenía en mi habitación. Incido en este detalle porque durante aquellos días tuve que tener constantemente encendido el equipo, ya que el servidor con la página debía estar disponible a cualquier hora del día, a la espera de que la víctima cayese en la trampa. Esto incluye también las noches, con la molestia del estridente zumbido del ventilador a altas horas de la madrugada, cuando uno intentaba caer rendido en los brazos de Morfeo. Mi madre me preguntaba por qué no apagaba el ordenador, y yo le contestaba muy seriamente que era para unas prácticas de la facultad, que se trataba de «un proceso importante que requería de alta

carga computacional y que tardaría muchas horas». Bendita ingeniería social. Vale para todo.

La trampa

Todo estaba casi a punto, aunque aún faltaba hilvanar la trampa para conseguir que nuestra víctima mordiera el anzuelo. No me compliqué mucho la vida. Me bastó con abrir una nueva cuenta de correo en Hotmail, con un nombre raro del tipo «service_ microsoft@hotmail.com» y «Servicios de Hotmail» en la información relativa a nombre y apellidos. En aquel entonces esto podía pasar desapercibido para un elevado porcentaje de usuarios.

Desde esta cuenta enviaría a la víctima un correo electrónico similar al que se recibía desde el soporte técnico de Hotmail. En él indicaba a los usuarios que, debido a cuestiones de mantenimiento en sus servidores, tendrían que verificar la información de su cuenta para que esta no quedara cancelada. Nada como la amenaza de quedarnos sin el Messenger, con todos nuestros preciados contactos, para lograr que la víctima invierta unos segundos en verificar su cuenta.

Solo quedaba darle al botón de enviar y cruzar los dedos. A la hora de urdir un ataque dirigido de este tipo, hemos de ponernos en la piel de la víctima y pensar cómo actuaríamos si nos llegase a nosotros un mensaje de este tipo. Cualquier mínimo detalle puede ser relevante y dar al traste con nuestro propósito. Una posibilidad es que el correo llegue cuando no estamos utilizando el ordenador y lo viésemos pasadas unas horas o incluso días. En aquella época no recibíamos nuestro correo de manera instantánea en el móvil. Si junto al correo de verificación de Hotmail recibíamos otros más interesantes de nuestros amigos, parejas o familiares, entonces el correo podía caer en el saco del olvido para siempre. Es por eso que mi aproximación pasaba por enviar el correo a la víctima cuando estimaba que estaría conectada. ¿Y cómo podría yo averiguar esto? Muy fácil. A través del MSN Messenger. Como María y su círculo íntimo de amigas estaban en mi lista de contactos, yo sabría cuándo estaban conectadas para enviarles el correo en ese instante y asegurar así una cuota de visibilidad mayor. En el *hacking* todos estos detalles son importantes.

Esa noche, cuando el icono de María cambió su color a verde esperanza, luciendo el flamante estado de «conectado», dejé pasar un tiempo prudencial, para al cabo de la media hora o así, lanzar la caña. Ya estaba todo en marcha. Ahora tocaba esperar.

Esa noche me fui a dormir expectante, con el zumbido del ventilador recordándome que una importante operación estaba en curso. A la mañana siguiente, me hallaba impaciente por revisar el contenido del fichero «pass.txt» que almacenaba en mi servidor. En él, debería aparecer ahora una línea más con el usuario y contraseña de María si esta había sido víctima del *phishing*. Pero esa línea no apareció. Era un escenario previsible. Pocas veces el éxito es inmediato. Al fin y al cabo, en el correo se le daba un plazo para verificar la información de su cuenta. Había que tener paciencia, aunque esto era difícil con Arturo llamándome continuamente por teléfono, con más insistencia que un comercial de telefonía.

El día se hizo bastante largo. A pesar de mis obligaciones académicas y otros menesteres, mi cabeza estaba en este asunto. Llegó la noche y vi de nuevo a María conectándose al Messenger. Era imprudente, lo confieso, y podría llamar mucho la atención si María ataba cabos, pero esa noche volví a enviarle el correo desde mi cuenta de servicios de Hotmail, con el consecuente riesgo de que lo detectara como correo malicioso, aunque en aquella época esto no era tan habitual como ahora.

Otro intento: la amiga

Mi fichero «pass.txt» siguió con el mismo tamaño los días siguientes, seguía sin obtener las credenciales de María. Si Arturo ya estaba desesperado al comienzo de la historia, os podéis imaginar su estado a estas alturas. En su obsesión por alcanzar la verdad, me instó a cambiar la aproximación, interfiriendo en la cuenta de la mejor amiga de María, la que «era como su hermana».

Si ya era reticente a espiar la cuenta de correo de María, comprometer la de su amiga me parecía algo más flagrante todavía, ya que al contrario de lo que pensaba Arturo, para mí el fin no justificaba los medios. Por otra parte, era su fin, no el mío. Pero lo cierto es ya estábamos metidos en el embrollo. Así que con el ansia por colmar los deseos de mi sofocado amigo y de satisfacer esa necesidad imperiosa de lograr el éxito, aquella noche envié nuevamente el cebo, esta vez a la «hermana» de María.

Sin muchas expectativas, me fui a dormir acompañado del ventilador de mi equipo, intentando apartar el tema de mi mente. Algo bastante difícil cuando te propones un reto de *hacking* de este calibre siendo joven y novato.

En aquella época tenía clases por las tardes y prácticas por las mañanas, así que no tenía que madrugar en exceso. Recuerdo aquel día como si fuera

ayer. Me tocaba presentar una práctica a las doce, así que no tenía pensado salir hasta las 11.30. Mientras revisaba concienzudamente que todo lo referente a la práctica estuviera en orden y que el programa hacía lo que tenía que hacer, recibí la enésima llamada de Arturo.

—¿Qué pasó? ¿Sabemos algo? ¿Has podido mirar algo?

—La verdad es que no lo he mirado tío, iba a echarle un vistazo ahora, pero estaba preparándome para la práctica…

—Entra un momento a ver, igual esta picó…

Yo no tenía muchas esperanzas, y estaba empezando a estar un poco harto de la actitud de Arturo. Aun así, me dispuse a comprobar nuevamente el fichero pass.txt. Fui a la carpeta correspondiente y de repente, todo cambió…

Un subidón de adrenalina

El mundo se paró durante un instante. Sentí, quizá por primera vez, esa sensación de triunfo cuando logras romper una barrera, comprometer un objetivo o alcanzar algo casi imposible. La adrenalina se dispara, las pupilas se dilatan, el corazón se agita, todo se vuelve inerte a nuestro alrededor y una sensación de fuerza, de pasión y de poder recorre todo el cuerpo mientras la mirada permanece inmóvil en la pantalla que evidencia la consecución de nuestro objetivo. No sé si acierto a transmitir lo que se siente en ese preciso instante. Supongo que, dependiendo de la entidad del reto, el esfuerzo dedicado y la necesidad que teníamos de lograr nuestro objetivo, esta sensación puede fluctuar en cuanto a intensidad, pero aseguro que es indescriptible, que hace que todo merezca la pena.

—¡Oye!, ¡oye! ¿Estás ahí? ¿Qué pasó? Dime, dime, ¡Dipu!

—¿Qué?, ¿qué fue? —balbuceé, inmerso en mi nube de emociones. En ese instante, nada ni nadie existía salvo yo y mi pass.txt.

—¿Qué pasó? ¿Ha picado? ¿Tienes la contraseña? ¿Por qué no dices nada?

—Sí, ¡ha picado! La tengo —fui capaz de responder, mientras Arturo me obligaba a volver al mundo terrenal.

—¿Y a qué esperas para dármela? Venga, dámela, di, ¡vamos! ¡Corre!

En aquel momento cometí quizá uno de los mayores errores hasta la fecha. No sé si achacarlo a mi inmadurez, a la inexperiencia en este tipo de situaciones, al ansia por satisfacer a mi amigo o a todo a la vez, pero sin tan siquiera haberme asegurado de lo que habría al otro lado del muro o dedicar unos segundos a pensar en las posibles implicaciones que tendría aquel acto,

le facilité la contraseña como quien da la hora a un extraño. ¡Cuántas veces me habré arrepentido de aquel momento!

Como puedes deducir, el siguiente paso fue entrar en la intimidad de Patricia, la mejor amiga de María. Lo hicimos ambos a la vez. Hoy, con las medidas de seguridad que implementan los proveedores de correo electrónico como Google, Yahoo o Microsoft, es posible que esto hubiese generado algún tipo de alerta por originar conexiones simultáneas desde ubicaciones o dispositivos no habituales, pero en aquel entonces nada de esto se tenía en cuenta.

En la bandeja de entrada había muchos correos. Mis ojos, al igual que los de Arturo al otro lado del teléfono, identificaron de manera automática el cuarto de la lista, un correo que Patricia había recibido justo el día anterior. Provenía, como no podía ser de otra manera, de María.

Ahí estaba. La prueba del delito. Mientras escribo estas líneas vienen a mi cabeza todas y cada una de las palabras de aquel correo, que aún recuerdo como si lo hubiese escrito yo. Palabras que superaban de lejos la mayor losa que una pareja pudiese soportar. Toneladas de dolor para cualquier hombre o mujer que ame, sienta o padezca. Sin duda alguna, estoy seguro de que fue una de las cosas más duras que Arturo haya podido vivir en su vida. Además de confirmar una infidelidad con otro estudiante durante su Erasmus, del que solo ensalzaba sus virtudes, María no expresaba atisbo alguno de arrepentimiento, sino todo lo contrario. El correo incluía referencias a Arturo no precisamente alentadoras. Era más bien una declaración de intenciones para la ruptura, una injustificada oda a la libertad.

—¿Lo estás viendo? —pregunté.

—Sí…

—Bueno, no sé, tengo que prepararme para ir a la facultad. Te llamo luego, ¿vale?

—Ok…

Arturo no era capaz de articular palabra. Por otra parte, no era el momento de decir nada. Hay momentos en la vida en que uno debe estar solo y entendí que aquel era uno de esos, porque cualquier cosa que pudiese haberle dicho en aquellos instantes no habría servido de nada.

Un juicio implacable

Mientras conducía hacia la facultad ensimismado en lo que acababa de protagonizar, reflexionaba acerca de la ironía del destino. No podía parar de

pensar en que había sido como una especie de castigo divino para él. Podría haber sucedido de mil maneras diferentes: podríamos haber tenido acceso a la cuenta de Patricia dos días antes, y ese correo aún no se habría ni enviado; podríamos haberlo tenido unos días después, cuando Patricia quizá lo hubiese borrado; podría incluso haberlo visto yo antes de facilitarle el acceso a Arturo si no me hubiese llamado en ese preciso instante, en cuyo caso probablemente le habría ahorrado el mal trago. Pero no, tuvo que ser así. Así es como estaba escrito.

¿Qué acababa de hacer? ¿Era esto justo para alguien? La pobre Patricia no tenía vela en este entierro y nadie tenía derecho a invadir su intimidad, ¿acaso alguien tenía derecho a invadir la intimidad de nadie? ¿Incluso de la propia María?

No os voy a mentir. Mi juicio sobre ella fue implacable. María no demostró ni un ápice de humanidad, de arrepentimiento, de empatía, de amor o un mínimo de aprecio hacia la persona con la que llevaba tantos años.

Pero Arturo tragó. No hay más ciego que el que no quiere ver. Armado de valor, coraje y con una copia impresa del correo electrónico —algo a lo que yo me opuse en toda regla—, acudió al encuentro de María, dispuesto a acorralarla por sorpresa, esbozando en su mente los capítulos de la mayor batalla dialéctica que la pareja hubiese vivido. Nadie en su sano juicio habría esperado que la discusión durase tan poco. Solo unas horas después, la pareja de tortolitos paseaba de la mano.

La historia no hubiera tenido mayor repercusión si todo hubiese transcurrido en la intimidad de Arturo y María, como tantas otras discusiones de pareja. Pero nada más lejos de la realidad. Arturo había contado con mi ayuda para satisfacer su necesidad de verdad, me había instado a transgredir la ley, la ética y la moral, bajo el pretexto de desenmascarar a su amada. Todo para nada.

Todos podemos cometer errores, somos humanos. Los humanos erramos continuamente, por eso existen el *hacking* y la ciberseguridad. María, sin embargo, jamás admitió su error, y Arturo, ¿qué decir de él? ¿Para qué quería saber lo que había pasado si en el fondo no iba a cambiar? ¿Para qué exponerme así? ¿Qué más tenía que pasar? Nuestra relación jamás volvió a ser igual. Era imposible. Él había perdonado a su princesa sin que ella le pidiera perdón, pero a mí no me haría jamás comulgar con ruedas de molino. No era mi problema. Nunca debió de haberlo sido.

Yo sí que reflexioné una y otra vez acerca de mis errores. Podía ser hábil para utilizar la ingeniería social y vulnerar la seguridad de un objetivo,

encontrando caminos alternativos para resolver los escollos que se me presentaran, pero a la vez tan necio como para dejarme manipular por un amigo en apuros que había perdido cualquier tipo de raciocinio. Tal vez quería demostrarme a mí mismo que era capaz de conseguirlo, y encontré en el problema de Arturo un móvil que justificara un ensayo de ataque en un escenario real.

El bando correcto

En cualquier caso, esta historia me dio una idea de la magnitud o el impacto que la tecnología podía tener en nuestras vidas, a la vez que me dejó claro el camino que no recorrería jamás. Si algún día llegaba a aprender todas las técnicas que me permitieran poner en entredicho la seguridad de una persona, sistema o tecnología, no sería jamás para el beneficio propio o ajeno, sino para todo lo contrario. Trabajaría para evitar que algo así pudiese sucederle a cualquier persona.

Y así ha sido. Con el paso del tiempo, la vida y el camino me han dado la oportunidad de estar en el bando correcto. La divulgación mediante conferencias o colaboraciones con medios, y ahora a través de este libro, me permite ayudar a concienciar a la sociedad acerca de los riesgos a los que se exponen cada vez que utilizan la tecnología y a interiorizar las buenas prácticas que deben adoptar para evitar riesgos.

A día de hoy, Arturo y María siguen juntos y están felizmente casados. Ha triunfado el amor, como en los cuentos de hadas, por decir algo. Tal vez sea eso, que esta historia es solo un cuento de hadas y no llegó a ocurrir realmente.

7

Campañas masivas de malware: ransomware y troyanos

Antes de entrar de lleno en los distintos tipos de amenazas a las que estamos expuestos los usuarios y las organizaciones en internet, conviene hacer una pequeña puntualización.

Hemos de distinguir entre dos tipologías de amenazas claramente diferenciadas: las campañas de ataques que se lanzan de forma masiva destinadas a cualquier usuario que pueda convertirse en víctima potencial y los ataques dirigidos sobre un objetivo concreto. Estos últimos responden al acrónimo de APT (Advanced Persistent Threats) y los abordaremos en próximos capítulos.

Nos centraremos ahora en estos ataques genéricos que no distinguen ni determinan su destinatario, sino que persiguen comprometer el mayor número de víctimas posible. Ya comentamos en el capítulo 2 que la motivación principal de los ciberdelincuentes es el lucro económico a través de la explotación y el desarrollo del cibercrimen a nivel profesional. Como cualquier empresa que se precie, buscan maximizar la rentabilidad y minimizar a su vez los costes de inversión. Desde este punto de vista, el cibercrimen es un negocio ideal, pues una vez diseñadas, las campañas de ataques pueden difundirse de manera masiva y llegar a una gran cantidad de usuarios. En primera instancia, muchos no sucumbirán a la ingeniería social, pero siempre habrá una cantidad considerable de usuarios que sí caerán en la trampa y contribuirán sin quererlo ni saberlo al beneficio de los ciberdelincuentes.

Ransomware

Aunque a día de hoy, con el ransomware como máxima representación de este tipo de ataques masivos, muchos usuarios sí son conscientes de que han sido comprometidos una vez que el ataque tiene éxito, esto no es siempre así. Un ejemplo es el famoso «Virus de la Policía», una de las primeras versiones de este tipo de amenazas que empezaron a pulular por la red alrededor de 2012.

El término ransomware proviene del inglés ransom, «rescate» en castellano, y ware, por *software*, que en este contexto funciona como abreviatura de malware, traducido como «programa malicioso». De ahí la denominación de este tipo de amenazas, por aquello del rescate económico que el usuario ha de abonar por la extorsión a la que se ve sometido.

El Virus de la Policía

Para quien no lo conozca, el Virus de la Policía es un tipo de malware que afectó con virulencia a muchísimos usuarios en aproximadamente veintidós países entre los años 2011 y 2013. Una vez que el usuario era infectado, este virus secuestraba la sesión de su equipo. La actividad de la víctima quedaba detenida por una pantalla con el logotipo del Cuerpo Nacional de Policía y un mensaje alertando al usuario de que su equipo había sido bloqueado a causa de ser consumidor de pornografía infantil. Para poder desbloquearlo, el usuario debía abonar una multa a la policía de entre 100 y 300 euros. Pero por motivos evidentes, para poder liquidar esta multa no se podían utilizar tarjetas de crédito o transferencias. En su lugar, se ofrecían sistemas de pago virtuales difíciles de rastrear como «Ukash», «Paysafecard» o «Moneypak».

Los usuarios que eran capaces de identificar este virus podían recuperar la actividad normal de sus equipos siguiendo el procedimiento de desinfección. Yo mismo lo eliminé de unos cuantos equipos de conocidos y familiares en su día. Pero hubo otros tantos que cayeron en la ingeniería social utilizada por los ciberdelincuentes. En mis conferencias de concienciación, cuando abordamos este caso, siempre cuento la anécdota del vecino de Ramón, amigo y compañero de departamento en la empresa GRAFCAN. Nunca llegué a saber su nombre, pero sí la historia que Ramón me contó con pelos y señales. Este vecino, víctima del Virus de la Policía en su ordenador portátil, no solo cayó en el engaño de los ciberdelincuentes, sino que se asustó de tal manera que se apresuró a deshacerse de su equipo tirándolo al contenedor de basura. Cuando se lo comentó a Ramón, mi amigo fue corriendo a recuperar el equipo antes de que fuera demasiado tarde. Su vecino fue totalmente transparente: «Ramón, sabes que yo pornografía infantil jamás, pero algo de pornografía

normal sí que veo, así que, para no tener problemas con la policía, prefiero tirar el equipo e ir a comprar otro a Media Markt».

Esta historia, que arranca siempre las carcajadas de los asistentes, es totalmente verídica. Es un reflejo de cómo la ingeniería social es capaz de hacer estragos entre los usuarios más crédulos, aunque en este caso, el vecino de Ramón no habría contribuido al lucro de los ciberdelincuentes, sino al de la conocida cadena de establecimientos de electrónica.

Evolución del ransomware

Como acabamos de ver, debido a señuelos como el de la policía, las primeras versiones de ransomware no dejaban claro al usuario si estaba siendo víctima de un ataque. Actualmente, cuando el usuario es infectado por ransomware, no se le secuestra la sesión, sino sus datos. ¿Cómo? El programa malicioso cifra todos los archivos de su disco duro mediante una contraseña que solo poseen los ciberdelincuentes. Para obtener la contraseña y recuperar sus archivos, el usuario debe abonar un rescate económico, mientras los ciberdelincuentes le facilitan las instrucciones concretas para proceder. Para evitar ser rastreados, estos utilizan la famosa red TOR, de la que hablaremos más adelante, y el sistema de pago en bitcoins. Como el usuario medio generalmente no sabe cómo conectarse a esta red ni adquirir bitcoins, los extorsionadores llegan a poner a su disposición un pequeño tutorial con las instrucciones necesarias para iniciarse en el uso de TOR y realizar el pago correctamente. Surrealista.

El principal problema de esta amenaza radica en que cuando un equipo es infectado, es prácticamente imposible recuperar la información cifrada por el ransomware. En las versiones iniciales que usaban el esquema de secuestro de datos, la contraseña era la misma para todos los equipos infectados. Así que, tras la pertinente investigación de los especialistas en ingeniería inversa de malware, era posible dar con la contraseña que permitía recuperar los archivos. Con el paso del tiempo, los ciberdelincuentes han sofisticado su amenaza. Las actuales campañas de ransomware usan una compleja criptografía asimétrica. Esto significa que solo los ciberdelincuentes pueden disponer de la contraseña, única y diferente para cada equipo infectado. La única manera de recuperar los archivos cifrados es restableciendo las copias de seguridad, siempre que las tengamos hechas y bien gestionadas, o pagando el rescate a los extorsionadores.

- La «ingeniería inversa» es la disciplina que se encarga de analizar un determinado programa ejecutable, dispositivo o tecnología, desensamblando todos sus componentes para conocer todos los detalles de su funcionamiento, hasta llegar incluso a obtener el código fuente en aquellos casos en los que sea posible.
- Se denomina así porque es el proceso inverso al tradicional.
- A la hora de desarrollar, generalmente se parte del código fuente y se llega a un ejecutable final.
- La ingeniería inversa se aplica sobre el *software* o malware diseñado por otro para intentar conocer sus entresijos.

Hasta ahora hemos comentado el funcionamiento del ataque una vez infectado un equipo, pero ¿cómo son comprometidos los usuarios? Como casi siempre, mediante la ingeniería social. Por supuesto, existen ataques de ransomware que se materializan mediante la explotación de vulnerabilidades, pero la mayoría de campañas masivas comienzan con un correo electrónico suplantando la identidad de una organización o de una persona en la que el usuario pueda confiar. Incluyen un fichero adjunto que el usuario debe abrir. Una vez que es ejecutado, el ransomware comienza su actividad.

Los ciberdelincuentes utilizan señuelos creíbles para lograr que el usuario no solo abra el correo, sino también el fichero adjunto que permite iniciar el ransomware. He aquí algunos ejemplos de campañas realmente exitosas en los últimos años:

- Envío de un falso borrador de la declaración de la renta suplantando la identidad de la Agencia Tributaria conforme se acercan los plazos de su tramitación.
- Envío de una falsa factura de luz suplantando la identidad de Endesa.
- Envío de un correo con el asunto «Tu factura» y el nombre de un remitente conocido.

Estos cebos, y otros similares que los criminales van desarrollando con el paso del tiempo, hacen que sean muchos los usuarios que muerden el anzuelo y ven cómo en cuestión de minutos todos los ficheros de su equipo se vuelven totalmente inaccesibles a causa del proceso de cifrado.

Por esta razón, desde hace unos años, el ransomware es una plaga que azota sin pudor a usuarios y organizaciones en internet. En particular, trae de cabeza a los responsables de IT o de seguridad de las empresas, tanto pymes como grandes corporaciones. En el entorno corporativo, su efecto es devastador. Tan solo con que uno de los usuarios sea comprometido por abrir

un fichero que no debía abrir, el malware se propaga por toda la red. Lo primero que hace un ransomware actual es cifrar los archivos que están dentro de unidades compartidas de red antes que los del propio equipo de usuario. ¿Por qué? Típicamente, las unidades compartidas en red en un equipo corporativo son carpetas que se encuentran en servidores de almacenamiento de una organización. En dichos servidores, se almacena de manera centralizada gran cantidad de información sensible perteneciente al negocio. Si el ransomware comienza cifrando esa información, los ciberdelincuentes se aseguran una mayor tasa de éxito en su acción. Incluso si los responsables de seguridad consiguen identificar en poco tiempo la amenaza y detener su propagación, el daño se multiplica en estos casos. Al final, son estrategias que utilizan para intentar generar el mayor impacto posible, aumentando las probabilidades de que las víctimas cedan a la extorsión para maximizar así sus ganancias.

Es curioso que muchos usuarios no conocieran el término ransomware antes del WannaCry. Sí sonaban más otros programas parecidos, como Cryptolocker y sus variantes: TorrentLocker, BitLocker, Locky o CBC-Locker.

Recomendaciones ante el ransomware

Algunas de las medidas que deben asumirse para hacer frente al ransomware coinciden con las de otro tipo de amenazas, pues las técnicas utilizadas para comprometer a los usuarios son comunes. Las repasamos a continuación.

Como usuario particular:

- Mantener siempre actualizado nuestro equipo, instalando los parches de seguridad para el sistema operativo y el resto de programas instalados, nos ayudará a remediar las vulnerabilidades que se vayan identificando con el paso del tiempo.
- Extremar la precaución a la hora de abrir documentos adjuntos que provengan de correos electrónicos sospechosos.
- Aunque provengan de un remitente conocido, si no esperamos ningún correo con fichero adjunto, no está de más desconfiar y contrastar primero si el remitente es quien dice ser.
- Utilizar un antivirus comercial de reputación contrastada que se actualice constantemente con las firmas del nuevo malware.
- Asegurarnos de tener correctamente salvaguardada nuestra información mediante copias de seguridad que podamos restaurar en caso de que nuestros equipos se vean infectados.

Como responsable de una organización:

- —Asegurar que se cumplen las medidas anteriores para todos los equipos de la organización.
- —En el entorno corporativo, adquiere más relevancia aún asegurar que los mecanismos de respaldo de la información están actuando correctamente y que será posible restaurar la información en caso de que haya cualquier problema.
- —Existen soluciones profesionales de fabricantes que se pueden implantar para prevenir el ransomware.
- —No obstante, es esencial formar y educar a los trabajadores para evitar que caigan en la ingeniería social utilizada por los ciberdelincuentes a través de:
    - Sesiones de concienciación al personal, con demostraciones de ataques en tiempo real, incluyendo al staff y al Comité de Dirección de la organización. Cuando los usuarios comprueban en directo cómo sus dispositivos son comprometidos a causa de los engaños más habituales, asimilan mejor las buenas prácticas necesarias para no caer en la trampa. Esto redunda en un mayor nivel de seguridad de la organización.
    - Campañas coordinadas de ataques de *phishing* e ingeniería social, para comprobar el nivel real de resiliencia de la organización ante este tipo de amenazas.

Troyanos

Un término que siempre ha formado parte de este mundo, casi desde que comenzamos a utilizar ordenadores y redes, es el de «troyano». De hecho, los primeros troyanos se remontan a los años noventa, así que no es de extrañar que sea un vocablo recurrentemente utilizado para hablar de amenazas y ataques en internet. Sin embargo, pese a que muchos usuarios lo manejen en su vocabulario, no todo el mundo conoce el concepto ni el significado real de la palabra.

Un troyano es un tipo de programa malicioso. Como el ransomware, se engloba también dentro de la categoría de malware. Su nombre alude al mítico caballo de Troya mencionado en la Odisea de Homero. Aquel famoso caballo aparentemente representaba un regalo de los griegos a la ciudad de Troya como signo de su rendición. En realidad, era una estrategia para introducirse en la ciudad. Dentro del caballo iban camuflados soldados

griegos que salieron durante la noche, mataron a los guardias y abrieron las puertas de la ciudad para que el resto del ejército griego se uniera al asedio y Troya cayera definitivamente.

De la misma manera, el troyano se ofrece al usuario como un programa legítimo, con una funcionalidad u objetivo determinado, aunque dentro esconde un código que permite al atacante acceso remoto completo al equipo del usuario. En definitiva, es un programa espía que permite controlar remotamente un equipo de manera silenciosa, como si estuviésemos sentados frente a la pantalla. Dentro de las funcionalidades que permite un troyano, se encuentran prácticamente cualquier acción que podamos imaginar:

- Obtener información del equipo.
- Parar o arrancar nuevas aplicaciones.
- Descargar o subir ficheros.
- Obtener una foto en tiempo real del escritorio de la víctima.
- Capturar todas las pulsaciones del teclado de la víctima.
- Obtener en texto plano las contraseñas de la víctima en el sistema operativo.
- Grabar sonido desde el micrófono del equipo de la víctima.
- Capturar fotos o vídeos desde la webcam.
- Etcétera.

Sí, como estás pensando, prácticamente cualquier cosa que el usuario haga en el equipo puede ser monitorizada por el atacante que se encuentra al otro lado. Todo lo que escribe, lo que hace, lo que descarga. Toda la información contenida en el dispositivo. Existen troyanos denominados RAT (Remote Administration Tool) que permiten realizar todas estas acciones sobre el equipo víctima. Otros solo implementan una de ellas, como los keyloggers, que se encargan de capturar las pulsaciones del teclado de la víctima. También existen los troyanos bancarios, especializados en robar las credenciales de acceso a banca en línea de los usuarios infectados.

Existen diversas vías a través de las cuales un usuario puede acabar siendo víctima de un troyano. Como siempre, la ingeniería social cobra un papel relevante. Más aún cuando la característica principal de un troyano es que se ofrece al usuario como algo que realmente no es. O, mejor dicho, que sí es pero que además es otra cosa. La manera más habitual de introducir un troyano en el equipo de la víctima es añadiendo código malicioso al fichero ejecutable de un programa legítimo para conseguir así camuflarlo adecuadamente. Posteriormente, se distribuye al usuario utilizando el señuelo

apropiado en cada caso o simplemente se sube a internet esperando que alguien lo descargue si no se pretende ir a por un objetivo específico.

Una vez que el usuario abre el fichero, se ejecutan tanto el programa que este espera arrancar como el troyano que silenciosamente ha proporcionado al atacante la puerta de entrada al equipo de la víctima.

Por este motivo, no es buena idea descargarse de internet aplicaciones y programas por los que normalmente hay que pagar, pero que han sido crackeados y están a disposición de los usuarios de manera «gratuita». Los usuarios buscan habitualmente programas como Microsoft Office, Adobe Photoshop o antivirus comerciales como Kaspersky y McAffee que en teoría son de pago. En algunos casos, es posible que estos programas estén libres de amenaza, pero en muchos otros traerán consigo un troyano (u otro tipo de malware) de regalo. Como suele decirse, nadie da «duros a cuatro pesetas».

Los troyanos son los programas que vemos típicamente en muchas películas o series de ciencia ficción, cuando de manera aparentemente milagrosa el protagonista es capaz de entrar en tiempo real en el ordenador de su víctima, descargar información confidencial, visualizar todo lo que hace y verle a través de su webcam. Por una vez, lo que vemos en la ficción no dista mucho de la realidad. La única diferencia radica, como siempre, en el tiempo que se tarda en obrar la magia. En la gran pantalla se ahorra al espectador la fase de preparación, en la que se identifica y explota una vulnerabilidad o se logra infectar al usuario con ingeniería social.

Recomendaciones para evitar ser víctimas de un troyano

En estos casos, se recomiendan siempre medidas genéricas básicas a la hora de proteger la seguridad de nuestros equipos:

- Actualizar el sistema operativo y todos los programas que tengamos instalados con todos los parches de seguridad a la última versión.
- Utilizar un antivirus comercial de prestigio y reputación contrastados que se actualice con las firmas del nuevo malware.
- No descargar jamás programas de internet crackeados.
- Extremar la precaución a la hora de descargar *software*, haciéndolo solo de sitios legítimos y confiables.
- En lo que a los dispositivos móviles se refiere, instalar aplicaciones que provengan solo de los markets oficiales, como Google Play o Apple Store.

Si te encargas de gestionar la seguridad de una organización, además de asegurar que se cumplen estas medidas, te interesará saber que:

- Algunas soluciones de fabricantes de seguridad, como las herramientas de detección y prevención de intrusos llamadas IDS o IPS, ayudan a detectar este tipo de amenazas.
- Asegurar que los usuarios tienen siempre los mínimos privilegios necesarios para acometer sus tareas con eficacia sobre los activos de la organización ayuda a mitigar los posibles efectos de una infección por un troyano. Si el usuario no tiene permisos de administrador en el equipo, muchas de las funcionalidades no podrían ser utilizadas por los atacantes.

8

Hacktivismo, ataques DDoS, botnets y ataques a contraseñas

Hasta ahora hemos resaltado el lucro económico como la motivación principal de los ciberdelincuentes. También abordamos el interés de los gobiernos y las agencias de inteligencia por el control de la información con los exploits Zero Day.

Otros actores que a lo largo de la historia han tenido un papel importante en el panorama de ataques son los llamados hacktivistas. El acrónimo proviene de la unión de los términos *hacker* y activista.

Se trata de individuos y colectivos que utilizan el *hacking* como medio para el activismo. En lugar de manifestarse en la calle, lo hacen en la red, acometiendo acciones que puedan lograr impacto y notoriedad. A pesar de que realizan actos ilegales y, por tanto, delictivos, su motivación no es criminal. No les mueve el dinero ni el poder que da la información, sino sus ideales. Al menos esa es la teoría.

Anonymous, movimiento hacktivista por antonomasia

Cuando pensamos en hacktivismo, a muchos nos viene a la cabeza el nombre Anonymous y la imagen de la característica máscara que representa a este movimiento. Si bien no es el único, Anonymous representa quizá el hacktivismo en su máxima expresión.

Mucho se ha hablado y escrito en medios de comunicación sobre el origen, los fundamentos y la estructura de este movimiento. Nosotros nos centraremos en explicar los fundamentos de sus principales tipos de ataques u «operaciones», como ellos suelen llamarlos, pero conviene puntualizar solo algunos aspectos confusos sobre su aparición y funcionamiento.

La historia sitúa el nacimiento del movimiento Anonymous en 4chan, un popular foro perteneciente a la clasificación de los llamados imageboard. Se trata de foros centrados en la publicación de imágenes en lugar de textos. 4chan era un foro que versaba sobre diferentes temáticas relacionadas con la cultura japonesa del manga o el anime, los videojuegos, la música o la fotografía. Cualquier persona podía compartir contenido sin necesidad de disponer de cuenta de usuario ni estar registrado. Se podía introducir un nombre, un pseudónimo o dejar el campo en blanco, en cuyo caso el contenido se publicaba como contenido anónimo. Cualquiera que no revelase su identidad, publicaba bajo el nombre «anonymous». No se sabía quiénes ni cuántos eran los que publicaban como anónimos. Esta es la idea que está detrás del movimiento. Porque pese a que existan individuos o grupos que se han identificado o asociado como miembros influyentes de la organización Anonymous en una región o país concreto, en realidad Anonymous no es en sí ninguna organización. No existe una cúpula como tal, aunque evidentemente en las comunidades existan actores más o menos influyentes. Se trata de un movimiento, un sentimiento en favor de la libertad de expresión, de la independencia y la neutralidad de internet. Cualquiera puede utilizar la bandera de Anonymous en un momento determinado para liderar y reivindicar una causa. Todos podemos ser Anonymous.

Este es quizá el matiz que más ambigüedad suscita a la hora de entender el movimiento. Puesto que en muchas ocasiones los medios de comunicación hablan de Anonymous como un grupo concreto, se tiende a pensar en una organización centralizada, con niveles jerárquicos y nexos de unión entre los grupos de cada región o zona geográfica.

Si cualquiera puede formar parte del movimiento Anonymous, suele ocurrir que en su seno existan grupos o individuos con distintas motivaciones e ideales.

La Wikipedia recoge una definición atribuida a Chris Landers, periodista del Baltimore City Paper, que puede contribuir a explicar esta idea a través de una sencilla metáfora:

> *«Anonymous es la primera "superconciencia" basada en internet. Anonymous es un grupo, en el sentido de que una bandada de aves es un grupo. ¿Por qué sabes que son un grupo? Porque viajan en la misma dirección. En un momento dado, más aves podrían unirse, irse o cambiar completamente de rumbo».*

Las acciones llevadas a cabo por Anonymous son denominadas «operaciones», que nacen por una causa determinada refrendada por los ideales que acompañan al movimiento: «Libertad de expresión», «justicia» o «independencia y neutralidad en la red». Cada operación puede centrarse en un objetivo concreto o en varios del ámbito político, social o corporativo. En su historia, hemos visto ataques a grandes empresas multinacionales, a estamentos gubernamentales de diferentes países o incluso cruzadas contra grupos terroristas como el Estado Islámico.

Dependiendo de la operación y los objetivos establecidos, los ataques puedan variar en tipología y finalidad. En algunos casos, se trata de revelar información sensible que cuestione la credibilidad del objetivo, dejándolo en entredicho al exponer las falacias de sus argumentos empresariales, sociales o políticos. En la lucha contra el terrorismo, las acciones se centran en identificar los sitios web y perfiles en redes sociales de propaganda yihadista, para reportarlos a las autoridades y contribuir a su desarticulación. Pero por lo general, los ataques más habituales de Anonymous y otros colectivos hacktivistas son los conocidos como «ataques de denegación de servicio distribuida», identificados por el acrónimo DDoS.

Ataques DDoS

Seguramente has leído alguna vez las siglas DDoS en noticias relacionadas con incidentes de seguridad y hacktivistas implicados. Estos ataques, como su propio nombre indica, tienen como objetivo dejar un servicio indisponible, típicamente el sitio web de una organización o cualquier sistema expuesto en internet. Los usuarios de la web o sistema afectados dejan de tener acceso y aparece como caído o inaccesible.

A diferencia de otro tipo de ataques, en los de denegación de servicio, por lo general, no se penetra en la red o equipos de la organización, ni se accede a información. Se atenta contra la disponibilidad de los sistemas aprovechando la manera en que la tecnología está construida y en los protocolos que utilizamos para acceder a internet. Para poder entenderlo, veámoslo paso a paso con un ejemplo.

Cuando visitamos cualquier sitio web desde nuestro ordenador o dispositivo móvil, lo que hacemos es enviar una petición a un servidor remoto de la organización a la que pertenece la web. Dicho servidor, al igual que nuestros dispositivos, está conectado a internet a través de un canal de comunicación que tiene un ancho de banda. Estamos familiarizados con este

concepto pues a la hora de contratar una conexión a internet para nuestro domicilio u oficina existen diferentes opciones disponibles en cuanto al ancho de banda: 5, 10, 50 o 300 megas dependiendo del tipo de conexión y la tarifa que decidamos contratar. Sucede igual con la conexión de datos móviles. Somos conscientes de que navegando con 4G tenemos mayor ancho de banda que con 3G o 2G. Estoy seguro de que en alguna ocasión has comprobado qué sucede cuando agotamos el ancho de banda si tenemos muchos dispositivos generando tráfico en la red. Si estamos viendo vídeos en *streaming*, descargando películas y jugando en línea… puede llegar un momento en que no podremos ni realizar una sencilla consulta en Google.

El servidor del sitio web al que enviamos la petición inicial también puede sufrir esta saturación. Si en un determinado instante de tiempo recibe muchas más peticiones además de la nuestra, llegará un momento en que su canal de comunicación hacia internet se vea colapsado con más tráfico del que pueda soportar. Alcanzado este pico, el servidor no podrá atender ninguna otra petición puesto que su ancho de banda está agotado, con lo que estará indisponible para cualquiera que intente acceder a él. En términos generales, esta es la manera de efectuar una denegación de servicio.

Hay otra aproximación que pasa por intentar agotar la capacidad de computación del servidor que queremos atacar, en lugar del ancho de banda de su canal de comunicación. En este caso, en lugar de intentar inyectar mucho tráfico, la idea es que las peticiones generadas obliguen al servidor a consumir recursos de CPU y memoria para procesar las peticiones. Posiblemente, también lo habrás experimentado en tu equipo en más de una ocasión. Si has visto alguna vez el mensaje de error que reza «Windows no responde» porque tienes varias aplicaciones corriendo simultáneamente y documentos de ofimática abiertos, sabes de lo que hablo.

Hemos introducido el fundamento técnico que se encuentra detrás de los ataques de denegación de servicio. Sabemos qué pasa por saturar el ancho de banda del canal de comunicación de un servidor o su capacidad de cómputo a base de enviar al mismo tiempo una cantidad ingente de peticiones. Pero ¿cómo se logra esto? La respuesta es sencilla: utilizando todos los equipos que se tengan al alcance. Cuantos más, mejor. De hecho, en la red es posible encontrar fácilmente herramientas distribuidas libremente por Anonymous para sumarse a las operaciones de colectivos hacktivistas y contribuir con los recursos de nuestro equipo a realizar un ataque de denegación de servicio. Dichas herramientas implementan diferentes técnicas de ataque a bajo nivel

que se basan en el fundamento de protocolos como TCP o HTTP. No entraremos en detalle para explicarlas debido a su complejidad.

Recomendaciones para combatir los ataques DDoS

Prevenir los ataques de denegación de servicio es complicado, pues se basan en los protocolos y estándares que utilizamos para acceder a internet. No obstante, como responsables de la seguridad de una empresa sí que hay algunas consideraciones al respecto:

- Gran parte de la prevención ante estos ataques recae en el operador que proporciona servicios a internet, comúnmente llamado ISP (Internet Service Provider). Generalmente, los principales proveedores ofrecen protección ante ataques de este tipo.
- Asimismo, existen fabricantes especializados que proporcionan soluciones al problema de la denegación de servicio. Algunos de los más conocidos son CloudFare, Incapsula, Akamai o Arbor. Funcionan apuntando los dominios a la infraestructura de estos proveedores, quienes aplican sus estrategias para filtrar y separar el tráfico legítimo del dañino y redirigirlo nuevamente a los sistemas de la organización.

Por otra parte, también se dan casos en que los ataques de denegación de servicio pueden llevarse a cabo por vulnerabilidades concretas en aplicaciones determinadas, como ha sucedido en el pasado con algunas versiones de WordPress, el popular gestor de contenidos. Como ya hemos apuntado, es esencial auditar nuestros sistemas para detectar y parchear todas las vulnerabilidades que existan.

Botnets

Otra manera que tienen los hacktivistas y los ciberdelincuentes de obtener equipos para sumarlos a los ataques de denegación de servicio es mediante redes de ordenadores zombis infectados, conocidas como botnets. Se les llama así porque una vez que los equipos pasan a formar parte de estas redes, permanecen durmientes, a la espera. A modo de zombis esperando órdenes. ¿De quién?

Cuando el equipo es comprometido por este tipo de amenaza, generalmente el usuario no es consciente. Puede continuar utilizando el equipo, realizando sus tareas habituales sin ningún tipo de problema. Solo que el equipo, además de responder ante su dueño, lo hace también ante su nuevo

amo, el administrador de la botnet, quien también le asigna sus propias tareas. Lo hace a través de un «servidor de comando y control», equipo que centraliza el control de los equipos infectados por la botnet, enviándoles las instrucciones oportunas en cada caso.

Por lo general, el usuario no detectará un comportamiento anómalo. Es posible que en determinados casos note que el rendimiento de su equipo decae o este se vuelve más lento de lo habitual, pero esto tampoco suele levantar sospechas ni constituirse como indicador de una posible infección. Estamos acostumbrados a que con el paso del tiempo el rendimiento de nuestros equipos se degrade paulatinamente hasta que la situación sea insostenible; es el momento en el que toca formatear o ir directamente a por un equipo nuevo. Si nuestro equipo presenta síntomas de una lentitud excesiva, puede que esté infectado por una botnet.

Las tareas encomendadas a los equipos infectados se orientan por lo común al envío de *spam*, correo fraudulento, así como a la distribución de cualquier otro tipo de campañas masivas de malware y ataques de denegación de servicio.

Recordemos que para efectuar una denegación de servicio es necesario inyectar una gran cantidad de tráfico sobre un objetivo concreto en un instante determinado. Si se cuenta con un ejército de bots o zombis a la espera de órdenes, es posible sincronizar el envío de todas estas peticiones a través de una sencilla instrucción del servidor de comando y control.

El uso de botnets para acometer ataques de denegación de servicio es una de las prácticas más habituales desde hace unos años. La evolución de la tecnología, con el incremento de la capacidad de ancho de banda de los canales y las crecientes medidas de seguridad para contener y mitigar estos ataques, obliga a utilizar muchos equipos para poder llevarlos a cabo.

«Mirai», la botnet que tumbó los servicios de Twitter, Spotify, Netflix o Amazon

Son muchísimos los ejemplos de ataques DDoS sonados a través de diferentes tipos de botnets. Sin duda alguna, uno de los más reseñables hasta la fecha, tanto por el impacto como por la cantidad de tráfico generado, tuvo lugar el 21 de octubre de 2016. Durante aquella tarde de viernes, los servicios de Twitter, Spotify, Netflix, Paypal, Amazon y otras entidades de semejante calibre quedaron inaccesibles para sus usuarios durante cerca de cuatro horas. El ataque no se produjo directamente contra los servidores de estas

organizaciones, sino contra la infraestructura tecnológica de DYN, el proveedor que se encargaba de darles servicio DNS. Este incidente fue catalogado en su día por algunos medios como el ciberataque más grande de la historia (aún no había tenido lugar WannaCry). Este tipo de afirmaciones, «el más grande la historia», pueden suscitar confusión entre los usuarios, porque como ya sabemos a estas alturas, ni todos los ataques son iguales ni tienen la misma motivación, ni el daño ocasionado es el mismo. WannaCry tuvo esta repercusión porque se alcanzó un récord histórico en cuanto al tráfico inyectado sobre la infraestructura de DYN: 1,2 Tbps. No se había visto nada igual hasta la fecha. El récord anterior se había quedado en la mitad, aproximadamente 600 Gbps.

> *El DNS (Domain Name System) es el servicio que se encarga de traducir un nombre de dominio a una dirección IP. Si el servidor DNS de una organización no responde, es imposible conocer la IP de sus servidores, por lo que es como si no existiera en internet.*

Que este ataque consiguiera doblegar los servidores de DYN no debió resultar una tarea sencilla. Un proveedor que da soporte a organizaciones punteras como Twitter, Netflix o Amazon cuenta con una infraestructura de dimensión y seguridad considerables.

¿Cómo se consiguió entonces alcanzar este récord histórico de tráfico? Por supuesto, a través de una botnet. Pero no una botnet cualquiera, sino una bastante sofisticada, que no solo infectaba ordenadores de escritorio, sino también todo tipo de dispositivos del llamado Internet of Things, o internet de las cosas. La botnet infectaba cámaras IP, aparatos vigilabebés o circuitos de videovigilancia, conocidos como CCTV, todos dispositivos vulnerables añadidos a su ejército de bots. Básicamente, intentaba localizar dispositivos que estuviesen mal configurados y con las credenciales por defecto (como el servidor Apache Tomcat del capítulo 2). Son muchos los usuarios que conectan estos dispositivos sin modificar la combinación de usuario y la contraseña que traen de fábrica. Con este arsenal de equipos y dispositivos infectados fue posible alcanzar el récord histórico de tráfico. Pudimos conocer en detalle su funcionamiento porque su orgulloso creador liberó voluntaria y gratuitamente el código fuente de la botnet, a la que denominó «Mirai», que

significa «futuro» en japonés. Como dato anecdótico, lo hizo bajo el alias de «Anna Senpai», por lo visto un popular personaje del anime manga japonés.

> *La botnet «Mirai» es la primera que no solo infectaba ordenadores, sino también dispositivos del internet de las cosas.*

Es necesario señalar que el creador de esta compleja botnet no tuvo por qué ser el autor del ataque de denegación de servicio sobre DYN. La publicación del código se hizo el 1 de octubre, antes del ataque, y pudo ser utilizado por cualquiera. Pasados unos días, un grupo de hacktivistas bastante conocido denominado New World Hackers se atribuyó la autoría de este ataque a DYN, aunque jamás pudo confirmarse si era cierto. El fabricante Flashpoint publicó un informe de investigación del incidente en el que ponía seriamente en duda la veracidad de las afirmaciones de New World Hackers. Según los investigadores, entre los sitios atacados se encontraba también una conocida compañía del sector de los videojuegos, y los indicios encontrados apuntaban a posibles script kiddies utilizando el código liberado por Anna Senpai, y no a un colectivo hacktivista.

Para bien o para mal, la incertidumbre forma parte de este mundo y así ocurren este tipo de casos extraños en los que alguien se atribuye la autoría de un ataque que tal vez no perpetró. Suele suceder con grupos hacktivistas que buscan visibilidad, mientras que otros actores detrás de los ciberataques evitan ser reconocidos a toda costa.

Recomendaciones para evitar ser víctimas de una botnet

Las medidas que deben adoptarse para prevenir las infecciones de botnets coinciden con las del ransomware y los troyanos, pues al tratarse de malware, los usuarios son infectados por las mismas vías. Las repasamos a continuación, incluyendo alguna más, y aplican tanto a usuarios particulares como a responsables de empresa:

- Actualizar el sistema operativo y todos los programas que tengamos instalados con todos los parches de seguridad a la última versión.
- Utilizar un antivirus comercial de prestigio y reputación contrastado que se actualice con las firmas del nuevo malware.
- No descargar jamás programas de internet crackeados.

- Extremar la precaución a la hora de descargar *software*, haciéndolo solo en sitios legítimos y confiables.
- En lo que a los dispositivos móviles se refiere, debemos instalar aplicaciones que provengan solo de los markets oficiales, como Google Play o Apple Store.
- Hay que modificar las contraseñas por defecto de cualquier dispositivo conectado a internet: routers, puntos de acceso, cámaras IP, televisores inteligentes, neveras…
- También hay que actualizar la última versión el firmware (el *software* que maneja físicamente el *hardware*) de todos estos dispositivos.

Otros usos de las botnets: *cracking* de contraseñas y minería de bitcoins

Las botnets aportan además otras funcionalidades interesantes para los ciberdelincuentes, que pasan por el uso de la «computación distribuida». Para los que no conozcan esta expresión, la computación distribuida hace referencia al uso de un gran número de ordenadores para resolver problemas complejos, que requieren una elevada capacidad de procesamiento. Al final, una botnet es justo eso, una enorme red de ordenadores conectados esperando a que les sea asignado trabajo. Se utilizan para el *cracking* de contraseñas o la minería de bitcoins, las famosas monedas digitales que se han puesto de moda en los últimos años.

La minería de bitcoins es un proceso matemático utilizado para confirmar transacciones entre diferentes usuarios y generar nuevas monedas. En cualquier sistema monetario tradicional, son los gobiernos los que imprimen más dinero cuando lo necesitan. En un sistema monetario descentralizado como bitcoin u otras monedas criptográficas, es necesario descubrir nuevas monedas resolviendo un problema matemático que requiere de mucha capacidad de cómputo distribuida. Aquellos usuarios que ofrecen la potencia de sus equipos para poder minar nuevas monedas se denominan mineros y reciben a cambio una recompensa en bitcoins proporcional al trabajo realizado. Es por esto que los ciberdelincuentes aprovechan la potencia de los equipos infectados a través de sus botnets, evidentemente sin el consentimiento de sus dueños, para minar bitcoins y lucrarse económicamente.

Ataques a las contraseñas de los usuarios: fuerza bruta o diccionario

A la hora de comprometer las cuentas de los usuarios, antes incluso de pensar en un ataque de *phishing*, existe la posibilidad de averiguar directamente la contraseña de la cuenta. En algunos casos, esta es la manera más sencilla, pues son muchos los usuarios que siguen estableciendo contraseñas débiles para sus cuentas. Son contraseñas típicas y fácilmente predecibles, como «123456», «password» u otras basadas en datos personales, como el nombre, la fecha de nacimiento, el mes y el año vigentes… Existen varias aproximaciones para intentar obtener la contraseña de una cuenta: a través de un ataque de «diccionario» o «por fuerza bruta».

El ataque de diccionario consiste en generar un conjunto de posibles contraseñas, incluyendo las más usadas y las fácilmente predecibles, así como otras basadas en el nombre, datos personales, entorno, residencia o incluso todo el diccionario de palabras del idioma habitual utilizado por la víctima u objetivo. Cuanto más completo sea el diccionario, más posibilidades habrán de dar con la contraseña correcta.

La segunda alternativa, la llamada fuerza bruta, es mucho más radical. En lugar de intentar utilizar un diccionario, trata de generar directamente todas y cada una de las diferentes combinaciones de números y letras posible para la contraseña, empezando por el mínimo de caracteres permitido en cada caso y llegando hasta el máximo. Esto asegurará que en algún momento llegue a encontrarse la contraseña correcta. Para las de cierta complejidad y determinado número de caracteres ese momento pueda tardar muchos años en llegar. Probablemente, más de los que estemos en la Tierra. Si un usuario tiene una contraseña de cuatro dígitos y utiliza solo letras minúsculas, existen 456 976 combinaciones posibles. Son muchas para introducirlas a mano, pero automatizando el ataque con herramientas específicas, se podrían probar todas las combinaciones en minutos u horas, dependiendo de la potencia de procesamiento y otros factores. Sin embargo, si hablamos de una contraseña de ocho dígitos que tenga al menos una mayúscula, una minúscula, un número y un símbolo especial, y si conseguimos probar unas 100 contraseñas por segundo, se tardarían cerca de 960 000 años para abarcar todas las posibilidades. Sin duda alguna, no tiene sentido intentar atacar una contraseña de esta magnitud por fuerza bruta.

Longitud y complejidad de las contraseñas

Por eso tanto los proveedores de servicio como los responsables de seguridad en las compañías recomiendan u obligan a los usuarios a establecer sus contraseñas con un número mínimo de caracteres, a ser posible entre ocho o diez, y utilizando letras mayúsculas, minúsculas, números y símbolos especiales. Cuantos más caracteres distintos formen parte del conjunto, más combinaciones deberán probarse. Aun así, entre longitud y complejidad, el factor diferenciador es el primero. Con una contraseña de dieciséis dígitos que solo utilizase letras se tardarían cerca de 22 000 millones de años para probar todas las posibilidades. Si además modificamos con relativa frecuencia nuestra contraseña, prolongaríamos hasta el infinito el tiempo necesario para descifrarla.

Evidentemente, para los ciberdelincuentes no tiene sentido intentar atacar por la fuerza bruta contraseñas de cierta entidad que no sean fácilmente predecibles o que no sucumban a un ataque de diccionario. Es aquí donde entra la capacidad que tienen las botnets para el uso de la computación distribuida. Si estimamos que se tardarán equis años en obtener una contraseña por fuerza bruta con un solo equipo, al repartir el trabajo entre 100 000 ordenadores podemos reducir considerablemente el tiempo estimado. Los ejemplos propuestos son estimaciones basadas en estadísticas y dependen del tipo de contraseña que se va a atacar, de la disponibilidad del sistema de autenticación (si es en línea o una máquina en local), así como de la capacidad de procesamiento; pero también de la posición de los dígitos en la combinación elegida por el usuario entre todas las posibles. Si en el ejemplo de ocho dígitos con números, letras y símbolos especiales en vez de probar 100 combinaciones por segundo se probasen 2000 se tardaría en hallarla cerca de 50 000 años. Si se utiliza una botnet con 100 000 equipos, en medio año podrían probarse todas las combinaciones posibles y obtener la contraseña. Podría valer la pena cuando se trata de un ataque dirigido a un usuario privilegiado de una organización. En este sentido, cobra relevancia la importancia de modificar cada cierto tiempo la contraseña para ponérselo más difícil a los ciberdelincuentes.

Recomendaciones para gestionar correctamente nuestra contraseña

Para evitar que la seguridad de nuestras identidades digitales pueda ser comprometida mediante un ataque de diccionario o fuerza bruta, es preciso seguir una serie de recomendaciones a la hora de definir nuestra contraseña:

- Como usuario particular:
  - No utilizar palabras o patrones predecibles.
  - Es posible utilizar fragmentos de palabras o fechas, pero que no sigan ningún patrón ni puedan ser fácilmente deducibles.
  - No incluir en la contraseña nuestro nombre, fecha de nacimiento o cualquier dato que sea público o pueda ser conocido fácilmente.
  - Utilizar contraseñas al menos de ocho caracteres.
  - Mezclar letras minúsculas, mayúsculas, números y símbolos especiales siempre que sea posible.
  - Modificarla al menos dos o tres veces al año.
- Como responsable de empresa:
  - Implantar una política de contraseñas en la organización que asegure y exija que todos los usuarios cumplen las directrices especificadas a la hora de definir una contraseña.
  - Incorporar las medidas técnicas para forzar la caducidad de la contraseña en un plazo de vigencia máximo. Lo recomendado en el entorno corporativo es entre 30 y 60 días.
  - No permitir excepciones en este sentido a ningún usuario de la organización, por muy arriba que esté en el escalafón jerárquico.
  - A menudo son los directivos o dueños de la empresa quienes obligan a los responsables de seguridad a realizar con ellos una excepción y permitirles disponer de una contraseña que no caduque nunca. En algunos casos, utilizan contraseñas débiles y fácilmente deducibles mediante ataques de diccionario.
  - Son precisamente las cuentas de directivos las primeras que los ciberdelincuentes van a intentar comprometer, por tratarse de usuarios con privilegios sobre los activos y los sistemas de la organización.

9

WannaCry, el ciberataque que cambió el mundo

Llega el momento de abordar en detalle el incidente más mediático de los últimos años en materia de ciberseguridad. Hablamos, cómo no, del mítico y popular WannaCry, que pasará a los anales de la historia como el mayor ciberataque que la sociedad haya vivido a escala mundial hasta la fecha. Al menos en lo que a impacto y repercusión se refiere. Seguro que recuerdas aquel día.

El revuelo mediático que provocó WannaCry carece de precedente alguno. Durante algunos días no se habló de otra cosa. La noticia copó las portadas de todos los medios de comunicación a nivel mundial, que realizaron un seguimiento exhaustivo de la evolución del número de infecciones y de toda la información que se iba recabando según avanzaba la investigación.

Veamos qué sucedió y si fue o no diferente a cualquier otro ataque.

La primera noticia: Telefónica víctima de un ciberataque

Todo comenzó el viernes 12 de mayo de 2017, poco antes del mediodía. A esa hora, ninguno de los que trabajamos en este apasionante mundo de la ciberseguridad imaginábamos que sería un viernes más largo de lo habitual. Los que además tenemos el privilegio de colaborar e intervenir en medios de comunicación, viviríamos aquel día una jornada frenética e inusual. En mi caso, pasada la una de la mañana con la pérdida de las llaves del coche debido al estrés y a la agitación de aquellas horas, con entrevistas, consultas, llamadas y el teléfono que no paraba de sonar.

Cerca de las doce de la mañana saltó la voz de alarma. Publicaciones en medios en línea y redes sociales, mensajes en listas de correo, grupos de Telegram y de WhatsApp se amuculaban comentando al unísono la primera

noticia: la multinacional Telefónica había sido víctima de un ciberataque, ordenando a sus trabajadores que apagaran sus equipos inmediatamente a través de un mensaje en la intranet y de los servicios de megafonía en sus instalaciones. Aquellos detalles de dramatismo (más propios de una película de Hollywood que de una compañía como Telefónica), ilustraban la gravedad de la situación.

Poco a poco comenzaron a conocerse detalles. Era un incidente originado por un ransomware, un tipo de ataque que no era novedoso, pues al menos desde el año 2013 estábamos lidiando con este tipo de amenazas. No obstante, todo apuntaba a que no se trataba de un ataque como los anteriores.

Al cabo de unos minutos, comenzaban a circular por igual informaciones verídicas y falsos rumores sobre otras importantes compañías españolas afectadas. Cundía el pánico. En todas las empresas dedicadas a la ciberseguridad se pedía cautela y máxima implicación para lo que pudiera pasar con los sistemas de los clientes. Era inevitable el símil con el famoso «Five/Nine Hack» que conmocionó al mundo en Mr. Robot, la popular serie estadounidense sobre *hackers*.

Otras víctimas en España y en el resto del mundo

Pasadas unas horas, se comprobó que el ataque había afectado no solo a Telefónica y otras empresas españolas, sino también al servicio sanitario de Reino Unido, Nissan, Fedex y algunas otras. El número de infecciones y de países afectados, hasta 150, se iba incrementando exponencialmente con el paso de los minutos. Una auténtica masacre.

¿Cómo había podido pasar? ¿Qué había sucedido para que organizaciones tan importantes, que dedican tantos recursos económicos a la ciberseguridad (algunas como Telefónica incluso ofrecen sus propios servicios) fueran comprometidas de este modo? ¿Qué tenía de diferente este ataque?

Como hemos visto, tradicionalmente los ataques de ransomware son exitosos cuando los usuarios son engañados mediante ingeniería social, y tras caer con un señuelo, descargan e instalan el programa malicioso que desata la infección. Pero en el caso WannaCry, esta no podía ser la explicación.

¿Se trataría de un exploit Zero Day? Si organizaciones punteras en todo el mundo estaban sucumbiendo al ataque de forma estrepitosa, había razones para pensar que los atacantes explotaban una vulnerabilidad no conocida, ante la que nadie podía defenderse.

Primeros análisis de la amenaza

Como suele suceder siempre que se propaga un nuevo malware de forma masiva, la comunidad investigadora se apresura a conseguir la muestra (el fichero malicioso que origina la infección) para analizarla. Recurren a diferentes técnicas de análisis entre las que se encuentra la ingeniería inversa. El objetivo es destripar el malware para obtener toda la información posible sobre su funcionamiento con el fin de combatirlo con solvencia.

Tras los primeros análisis, enseguida se encontró la respuesta y la explicación para el devastador efecto dominó de WannaCry. El vector de propagación de este malware se basaba en la explotación de una vulnerabilidad crítica de los sistemas Microsoft, recogida en el Microsoft Security Bulletin con la numeración MS17-10.

Este boletín, que incluía el parche para la vulnerabilidad, fue publicado por Microsoft en marzo de 2017, dos meses antes de que se produjera el devastador ataque. Es decir, no se trataba de una vulnerabilidad Zero Day, pero aun así la magnitud del impacto ocasionado fue de dimensiones estratosféricas. Imaginemos lo que podría haber pasado si de verdad se tratara de un Zero Day, porque en su momento sí que lo fue, como toda vulnerabilidad que es descubierta antes de ser reportada al fabricante.

La historia de esta vulnerabilidad es curiosa, porque los exploits que permitían aprovecharla pertenecieron en su día al arsenal privado de exploits Zero Day de la todopoderosa NSA estadounidense. Los investigadores que las descubrieron las bautizaron como «EternalBlue» y «Doublepulsar». Pero ¿cómo sabemos todo esto?

La historia de EternalBlue, Doublepulsar, Shadow Brokers y la NSA

Allá por 2016 un colectivo hacktivista apodado «Shadow Brokers» anunció públicamente que sus miembros habían sido los primeros y únicos en conseguir *hackear* a la NSA, la agencia de espionaje estadounidense. Aseguraban que habían comprometido la seguridad de «Equation Group», un grupo de *hackers* de élite vinculando a la agencia e identificado en 2015 por investigadores del popular fabricante Kaspersky. Fueron ellos quienes acuñaron este nombre para el selecto equipo de *hackers*, al que responsabilizaron de más de 500 infecciones en al menos 42 países. No

hablamos de infecciones con malware corriente de andar por casa, sino de ataques dirigidos y sofisticados, que se habían llevado a cabo con extrema planificación. Ataques que, debido a su complejidad y refinamiento, denotaban unas habilidades técnicas extraordinarias de sus ejecutores. Es por esto que tratar de *hackear* a Equation Group no se presumía tarea fácil.

A través de sus comunicados, los miembros de Shadow Brokers afirmaron que habían accedido a las bases de datos de la NSA, extrayendo no solo gran cantidad de información sensible, sino parte de su arsenal de herramientas, entre ellas, muchísimos exploits Zero Day. Evidentemente, si alguien hace una afirmación de tal calibre debe proporcionar una prueba que lo acredite.

Como primera muestra, el colectivo publicó algunos ficheros y documentos extraídos de los servidores de la NSA, entre los que se encontraban populares herramientas como Stuxnet, el malware que se utilizó para atacar las centrales nucleares de Irán y del que hablaremos en el próximo capítulo.

El siguiente paso fue anunciar una subasta para ofrecer al mejor postor el resto de herramientas y exploits que tenían en su poder. Llegaron a pedir un millón de bitcoins, aproximadamente 568 millones de dólares en aquel momento. Con el paso de los meses, supimos que a través de una plataforma llamada ZeroNet estaban intentando vender los exploits uno a uno, con precios de entre uno y cien bitcoins, tras no prosperar la subasta por la colección completa. Continuaron buscando maneras de rentabilizar su «hazaña», ofreciendo diferentes paquetes de exploits. En abril de 2017, liberaron de manera gratuita un pequeño conjunto de exploits para demostrar una vez más la veracidad de sus afirmaciones y «para ayudar a la gente», según rezaba su comunicado. Entre estos exploits, se encontraban los ya famosos EternalBlue y Doublepulsar que permitían aprovechar vulnerabilidades en diferentes versiones de Microsoft Windows. Fueron los utilizados en WannaCry.

Revelar al mundo el código de los exploits posibilitó que cualquiera pudiera utilizarlos para comprometer la seguridad de equipos vulnerables que aún no estaban actualizados. Recordemos que Microsoft publicó un parche para proteger nuestros equipos en marzo de 2017. Un mes después, los miembros de Shadow Brokers obsequiaron al mundo con estos y otros exploits. Otro mes más tarde se lanzó WannaCry, el ciberataque más grande de la historia.

A raíz del impacto generado por este malware, el controvertido colectivo Shadow Brokers volvió a aparecer en escena, informando de que no tenía

nada que ver con el ataque. De paso, aprovecharon la ocasión para ofrecer un modelo de suscripción mensual a su arsenal de exploits, una vez comprobada la efectividad de los mismos. Surrealista.

El malware WannaCry causó estragos en multitud de organizaciones punteras en todo el planeta, explotando vulnerabilidades conocidas para las que en realidad existía remedio. Desde que la Agencia desarrolló o adquirió los exploits hasta marzo de 2017, cuando se dispuso del remedio, los agentes de la NSA tenían la capacidad de comprometer alegremente cualquier equipo con sistema Windows que fuese accesible desde internet. Se dice pronto y fácil. Pudieron hacerlo de manera silenciosa sin que nadie se percatase de ello.

WannaCry fue diferente en cuanto a la visibilidad del ataque, pues se trataba de un ransomware que buscaba que el usuario fuera consciente del ataque. Algunos especularon con la posibilidad de que WannaCry hubiera sido creado por quienes querían «quemar» estos poderosos exploits y que nadie pudiese volver a utilizarlos. El razonamiento es simple. Tras el revuelo por un ataque de esta dimensión, todos aquellos que no habían instalado aún el parche de Microsoft, se asegurarían de hacerlo a la mayor brevedad posible. Al menos en teoría, ya que un mes después se produjo un nuevo incidente de repercusión mediática mundial a causa de un malware bautizado como «Non-Petya», que aprovechaba los mismos agujeros de WannaCry.

Grandes organizaciones con equipos sin actualizar

Algo que llamó la atención de muchos fue que grandes organizaciones de dimensión multinacional sucumbieran a un ataque de estas características por no tener sus equipos actualizados. Muchos podrían pensar que esto sería más propio de una pequeña empresa con pocos recursos dedicados a las TIC y donde no existiera un perfil dedicado a la ciberseguridad. Sin embargo, en grandes empresas y multinacionales, el proceso de parcheo y actualización de los equipos corporativos no es una tarea sencilla. Requiere de mucha coordinación y planificación. El número de equipos no supone obstáculo alguno, ya que se pueden actualizar de forma remota y automática, sean 20 o 2000.

Las organizaciones utilizan equipos «plataformados» con una misma configuración para un elevado número de usuarios. El problema aparece cuando, dependiendo de la actividad de la organización, existen una o más de estas configuraciones para los distintos tipos de equipos. Por tanto, es

necesario comprobar que la instalación de un parche no genera conflictos para cada una de las diferentes configuraciones. Podría ser que al instalarlo sin realizar estas comprobaciones, dejase de funcionar correctamente alguna aplicación crítica. Las consecuencias de un error de este tipo podrían ser devastadoras y desembocar incluso en una autodenegación de algún servicio. Desde la publicación de un parche hasta que todos los equipos están actualizados, hay una ventana de tiempo que se debe intentar reducir al máximo, y durante la cual algunos equipos pueden ser vulnerables. En este proceso que forma parte de lo que se conoce como «gobierno de la seguridad TI» se analizan todos los activos tecnológicos de la organización para identificar los más sensibles en función de diferentes parámetros, y actualizar primero los que resultan más críticos para el negocio y la operatividad de la compañía.

En un mundo ideal, todos los equipos deberían tener instalado un parche de seguridad crítico nada más ser publicado por el fabricante, pero esto no es posible en algunos casos. Entra dentro de lo previsto que una organización de cierta dimensión tenga algunos equipos sin actualizar, como les sucedió a las empresas afectadas por WannaCry. Esto no significa que estén gestionando mal su seguridad, siempre y cuando todo esté contemplado en su política de gestión de riesgos y cuenten con un plan adecuado de respuesta a incidentes. Telefónica fue un ejemplo en la gestión de la crisis WannaCry, pues pese al revuelo mediático inicial, lograron contener el incidente sin perder información sensible, sin que ningún cliente se viese afectado y sin que ninguno de los muchos servicios y líneas que proporcionan a empresas y usuarios en todo el mundo se cayese. Lo lograron porque disponían de un plan de respuesta a incidentes. Ese protocolo que se pone en marcha cuando las cosas se ponen feas. Es inevitable que en algún momento nuestra seguridad pueda ser comprometida, pero lo que marca la diferencia es estar preparado para cuando ocurra.

Una vez explicada con detenimiento la intrahistoria de la vulnerabilidad que originó el caos de WannaCry, volvamos al incidente.

El kill switch que permitió neutralizar el ataque

Durante aquel día del ciberataque masivo, las televisiones, rotativos y radios informaban de la última hora, actualizando las cifras relativas al número de infecciones y países afectados. Una de las noticias más destacadas fue la de un investigador inglés llamado Marcus Hutchins, que había logrado

desactivar el ransomware evitando que continuara propagándose. Este joven *hacker*, hasta entonces desconocido para el mundo, fue aquel día coronado como el salvador. Pero ¿cómo lo hizo?

Al igual que otros muchos investigadores, aplicó ingeniería inversa para inferir el comportamiento del malware. En el proceso, descubrió de manera accidental que los programadores del gusano habían introducido en el código fuente lo que se conoce como un kill switch, una especie de botón rojo a modo de freno de emergencia, que les permitiese paralizar su actividad, impidiendo que el ransomware iniciase el cifrado de todos los archivos, aunque hubiese infectado el equipo. El kill switch estaba diseñado para activarse en remoto, tal vez cuando hubiesen logrado su objetivo o recaudado una cantidad económica suficiente por el rescate. El caso es que para implementarlo, habían introducido una condición en el flujo de ejecución del programa, que consistía en comprobar la existencia en internet de un dominio determinado. Si ese dominio no estaba registrado, el programa proseguiría su curso, cifrando toda la información del equipo para exigir un rescate económico a cambio. En el momento en que ese dominio estuviese registrado en internet, el malware se detendría inmediatamente.

Como decíamos, Marcus Hutchins dio con este antídoto de manera accidental, pues en primera instancia no sabía que con el registro del dominio estaba activando un kill switch. Su propósito inicial era hacer lo que se conoce como un sinkhole para investigar con mayor profundidad el incidente. Se trata de una técnica utilizada para desarticular botnets y otras campañas de malware. Consiste en registrar los dominios que se encuentran en el código fuente del malware si no están registrados, pues son dominios a los que se conectan las máquinas infectadas. Estos dominios se apuntan a la IP de un servidor controlado por el investigador que realiza el sinkhole. El objetivo es que los equipos infectados se conecten a dicho servidor en lugar de al de los cibercriminales, para así identificar equipos infectados, evitar que sigan siendo controlados e intentar averiguar cómo funciona la campaña o la botnet.

Registrando aquel dominio, Hutchins activó el botón de apagado y consiguió neutralizar un ciberataque que traía de cabeza a los responsables de seguridad de medio mundo. Desde ese momento todos los equipos que eran infectados no sufrían ningún tipo de daño o consecuencia. El *hacker* británico había conseguido detener el efecto dominó de WannaCry. Desde entonces pasó a formar parte de los anales de la historia como el «héroe de WannaCry». De ser un completo desconocido, pasó a ser un reconocido *hacker* con más de 100 000 seguidores en su cuenta de Twitter.

La rocambolesca historia de Marcus Hutchins

La historia de este brillante investigador de veintiún años es cuanto menos curiosa, como todo lo que rodea a WannaCry. Resulta que, tras ser elevado a los cielos por la hazaña de WannaCry en mayo de 2017, le tocó descender a los infiernos en agosto del mismo año. El FBI le detuvo en Las Vegas cuando estaba a punto de subir al avión de vuelta tras participar en una de las conferencias de *hackers* más famosas a nivel mundial: DEFCON. Se le acusaba de haber participado años atrás en la creación de un malware bancario llamado «Kronos», un troyano que robaba las credenciales de acceso a la banca en línea de los usuarios y que se prodigó allá por 2014. El FBI atribuía al héroe de WannaCry la creación del malware por un tuit que escribió en 2014, pidiendo una muestra de Kronos, así como por supuestos mensajes en foros underground en los que anunciaba su venta con *nicks* que se relacionaban con él.

Marcus Hutchins se declaró inocente de todos los cargos. La noticia causó gran revuelo y la comunidad se volcó con el investigador. Tras unos días en prisión, finalmente fue puesto en libertad condicional. En el momento de escribir este libro, el *hacker* aún reside en Los Ángeles, pues tiene prohibido abandonar el país y continúa a la espera de que se celebre el juicio por su caso.

Procedencia del ataque

Por otra parte, en los días posteriores a WannaCry, como siempre que se produce un incidente de estas características, comenzaron a circular informaciones sobre la presunta procedencia del ataque, fruto de las primeras investigaciones. Para bien o para mal, en este mundo es muy difícil atribuir en última instancia la autoría de un ataque a un individuo, grupo, organización o país, pues al final se trata de malware que se desarrolla y se distribuye de manera masiva por todo el planeta utilizando diferentes canales. Aunque no es algo sencillo, tras investigar en detalle las muestras de malware, el tipo de código, el *modus operandi*, la infraestructura que hay detrás de la campaña, etc., se suele apuntar en un sentido u otro.

Cuando se analiza el código fuente obtenido con ingeniería inversa, se presta atención, entre otros aspectos, al idioma que utilizan los programadores en los comentarios de ayuda para explicar diferentes partes del código. Muchas veces los comentarios se introducen a propósito en ruso, chino o

árabe para confundir a los investigadores y desviar su atención hacia grupos o colectivos de otros países.

No obstante, en algunos casos, son muchas las pistas que llevan a un único sospechoso y aunque este lo niegue públicamente, al final se asume que está detrás del ataque. En el caso del gusano informático Stuxnet, con el paso del tiempo y las diferentes pruebas, se demostró que se trataba de un ataque dirigido por Estados Unidos en colaboración con Israel. Lo comentaremos en el próximo capítulo.

En el caso de WannaCry, en los días posteriores al incidente, investigadores de Kaspersky especulaban con Corea del Norte como origen del ataque, por encontrar similitudes en el código con otras ciberarmas atribuidas en su día a «Lazarus Group», un grupo de *hackers* vinculados al Gobierno norcoreano. Se les responsabiliza, entre otros, del ataque a la multinacional Sony Pictures a finales de 2014. También hablaremos de ellos en el próximo capítulo.

Con el paso de los meses, fabricantes y gobiernos continuaron investigando en detalle el caso WannaCry. En el mes de octubre, un responsable del Gobierno británico afirmaba públicamente que «estaban lo más seguros posible» de que Corea del Norte estaba detrás del popular ciberataque. No fue hasta diciembre de 2017 cuando Estados Unidos acusó formalmente a Corea del Norte como responsable de WannaCry, y aportaron evidencias halladas por el Gobierno estadounidense, por otros gobiernos, fabricantes y empresas privadas.

Finalmente, en diciembre de 2017, Konstantin Kozlovsky, un ciberdelincuente ruso detenido por la distribución del malware «Lurk» en 2016, confesó en una entrevista su participación en la creación de WannaCry, algo que no ha sido confirmado ni desmentido hasta la fecha.

WannaCry, un malware con fallos de envergadura

Pese al impacto que generó, WannaCry era un programa mal diseñado, que contenía algunos bugs y evidenciaba carencias en lo que se refiere a la estética y elegancia del código. Uno de los afortunados errores fue que el kill switch no estuviera bien protegido y pudiera ser habilitado por alguien externo. Otro error de envergadura en las primeras versiones del ransomware fue que los ciberdelincuentes no habrían podido identificar a las víctimas que pagaran el rescate, puesto que no almacenaban el identificador del «cliente» que había abonado el pago. Aunque quisieran, jamás habrían podido

devolverles su información. Es curioso que aun con estos errores y carencias, WannaCry consiguiera poner en jaque a medio mundo.

Respecto a la recaudación económica, WannaCry no fue un ataque especialmente lucrativo para quienes estuvieran detrás de él. Si bien en los primeros días del incidente consiguió infectar a más de cien mil equipos en ciento cincuenta países y convertirse en el ataque más mediático e importante de la historia hasta la fecha, apenas tuvo repercusión económica. Se generaron alrededor de ciento sesenta transacciones en los primeros tres días que ascendían a poco más de 30 000 euros. Como era de esperar, los ciberdelincuentes no movieron el dinero del monedero de bitcoin donde almacenaban la recaudación para evitar generar más ruido. Pasados unos meses, en agosto de 2017, vaciaron el monedero con un acumulado de cerca de 115 000 euros en bitcoins, es decir, una cantidad despreciable para la trascendencia e impacto que tuvo WannaCry.

A lo largo de este análisis hemos introducido conceptos y nociones mientras repasábamos todas las peculiaridades que se produjeron en torno al popular incidente. WannaCry no es ni de lejos la amenaza más sofisticada o profesional a la que hemos tenido que hacer frente. Para los que estamos familiarizados con este mundo, ni siquiera era algo imprevisto, sino más bien todo lo contrario. Asumimos que este tipo de cosas pueden pasar y que lo realmente aterrador es que puedan estar sucediendo de manera silenciosa sin que nadie se percate de ello. Por este motivo, si eres responsable de gestionar la seguridad de una organización, debes seguir a rajatabla las recomendaciones que establecimos en el plan de respuesta a incidentes. Necesitamos estar continuamente preparando nuestras capacidades, nuestros sistemas y nuestras organizaciones para ser resilientes ante este tipo de ataques y todos los que puedan venir. Asumamos que en algún momento seremos atacados y comprometidos.

A pesar de todos los matices, el impacto de WannaCry marcó un antes y después en la manera de pensar de muchos. Algunos de los que tenían menos conciencia acerca de la importancia de la ciberseguridad empezaron a cambiar su forma de pensar respecto al ciberespacio y las nuevas tecnologías. En este sentido, no hay mal que por bien no venga.

10

Ataques dirigidos: Stuxnet y el ataque a Sony Pictures

En los capítulos anteriores hemos tratado todo lo referente a las principales amenazas a las que continuamente están expuestos usuarios y organizaciones en internet. Las más comunes son las campañas masivas articuladas por los ciberdelincuentes para maximizar la rentabilidad de sus ataques. Pero no son los únicos golpes a los que estamos expuestos, ni mucho menos los más peligrosos.

A continuación, abordaremos en detalle los ataques que a día de hoy deben representar la principal preocupación para usuarios y organizaciones en todo el mundo: los ataques dirigidos. En contraposición con los ataques masivos, en los que se intenta alcanzar el máximo número posible de usuarios de manera indiscriminada, las ofensivas dirigidas se conciben para un objetivo determinado y concreto, típicamente una organización, aunque también podría tratarse de un único usuario.

Son amenazas con un nivel de sofisticación considerable, que se planifican con muchísima antelación, en las que se estudia previamente de manera minuciosa el ecosistema y las circunstancias que rodean al objetivo. La meta es diseñar un ataque infalible que se adapte como un guante a la víctima, como si de un traje a medida se tratara, y lanzado una sola vez para evitar su detección. El fin no es conseguir acceso de manera efímera, sino permanecer en el corazón del objetivo robando información de manera silenciosa durante el mayor tiempo posible: por lo general meses o incluso años.

Esto, que dicho así puede parecer utópico, es real. Los ataques dirigidos constituyen actualmente el mayor peligro al que podemos enfrentarnos cuando hablamos de amenazas en la red. Las empresas que sí invierten en

ciberseguridad centran todos sus recursos y esfuerzos en intentar prevenir e identificar estos ataques, pues son conscientes de su peligrosidad y de la dificultad de su detección. Aunque se basan, como cualquier otro ataque, en la explotación de vulnerabilidades técnicas y humanas, son ataques únicos, complejos y sofisticados, confeccionados exclusivamente para cada objetivo, imposibles de clasificar o relacionar. Resulta complicado defenderse de algo que no se conoce o ni tan siquiera sabemos si existe. Lo mismo ocurre con los exploit Zero Day.

Advanced Persistent Threats

En el mundo de la ciberseguridad existe un acrónimo para designar estos ataques dirigidos: APT o Advanced Persistent Threat. Se incorporó a la jerga de vocablos técnicos del sector hacia 2013. En un principio, daba la sensación de ser uno más de tantos términos técnicos que se utilizan con ligereza para adornar la retórica y dar sensación de conocimiento, con el fin último de convencer en la venta del producto, servicio, imagen… o humo, pero venta al fin y al cabo. Cada año esta lista de palabros tecnológicos se hace más larga: Cloud Computing, Big Data, Machine Learning, Inteligencia artificial… términos que pertenecen al sector TIC en general. Otros como Resilience o APT forman parte del sector de la ciberseguridad en particular.

Sin embargo, el acrónimo APT —en castellano «Amenaza Persistente Avanzada»— ha demostrado con el paso del tiempo su utilidad. «Persistente», porque busca obtener acceso permanente a las entrañas del objetivo para el robo silencioso y continuado de información sensible; «avanzada», porque efectivamente hablamos de ataques con alto nivel de complejidad y sofisticación.

No podría tampoco ser de otro modo, pues en los tiempos que corren no es sencillo quebrar la seguridad de los firewalls y dispositivos de detección de intrusos que ofrecen los principales fabricantes del mercado. Cualquiera de estos dispositivos analiza en vivo el tráfico de red e incorpora inteligencia actualizada por los fabricantes sobre amenazas en tiempo real. Suponen una importante ayuda para identificar gran parte de los incidentes de seguridad que amenazan a una organización. No es posible burlar a estos dispositivos con un ataque convencional, con más razón si se pretende hacer de manera prolongada en el tiempo. De ahí que se requiera un nivel de sofisticación extraordinario en una APT. Un ejemplo de esto lo encontramos a la hora de filtrar al exterior la información sensible recopilada de la red de la víctima.

Seguro que se te ocurren muchas maneras de sacar esa información: enviarla en adjuntos de correos electrónicos, subirla a un servidor FTP, volcarla en la nube… Pero todas dejan un rastro evidente de la transmisión. Para no ser detectados por estos dispositivos se suelen utilizar los llamados «canales encubiertos», técnicas avanzadas para camuflar la transmisión de la información entre paquetes de tráfico convencional, como, por ejemplo, el del acceso a cualquier web de noticias. Así no sería identificado como tráfico sospechoso por parte de los firewalls y sistemas de detección de intrusos, pues cualquier empleado de una organización podría estar generando este tráfico.

El precepto fundamental que hay detrás de una APT es devastador: si quien tenga la motivación para un ataque de este tipo cuenta con recursos y tiempo suficientes, y se propone verdaderamente comprometer nuestra seguridad, en algún momento lo va a lograr. A estas alturas ya tenemos una visión más clara de cómo se materializan los ataques e incidentes y de cómo se gestiona la seguridad. Hemos visto que son muchos los flancos a cubrir y que no es sencillo mantener una organización protegida en todo momento contra todas las vulnerabilidades conocidas.

En cuanto a los posibles actores y las motivaciones detrás de una APT, se incluyen las destinadas al lucro económico, pero por lo general la principal motivación es el robo de información sensible, y sus demandantes son quienes tienen los recursos y la capacidad para planificar ataques de este tipo: organizaciones cibercriminales, gobiernos, agencias de inteligencia y empresas interesadas en el espionaje industrial.

¿Cómo se planifica una APT?

Como ya hemos señalado, la puesta en marcha de un ataque dirigido o APT lleva consigo una planificación minuciosa. En la fase inicial, se estudia toda la información disponible que existe acerca del objetivo. Información de cualquier tipo: actividad de la organización, modelo de negocio, estructura, sedes físicas, infraestructura tecnológica, departamentos…

Se intenta obtener el máximo conocimiento posible a nivel técnico de todos los sistemas que existen en la organización: dominios, direcciones IP, servidores, servicios abiertos al exterior, soluciones de seguridad, antivirus, tecnologías utilizadas… Por otra parte, también se profundiza en el conocimiento del equipo humano que conforma la compañía: estructura jerárquica, departamentos, roles, perfiles de los trabajadores en las redes sociales, *hobbies*, intereses, afinidades, enemistades…

Para lograr este cometido, se utiliza lo que se conocen como técnicas de OSINT (Open Source Intelligence), de las que hablaremos en el capítulo 12.

Cualquier dato que se pueda recabar en esta fase es valioso para planificar el ataque. Una APT se compone de varias fases y lleva consigo más de una técnica de ataque, pero el vector de entrada inicial es casi siempre el mismo: los usuarios, el eslabón más débil de la cadena. Generalmente se utiliza la ingeniería social para lograr comprometer a uno o varios de los trabajadores de la organización objetivo mediante un *phishing* dirigido, creado a medida, específicamente para ellos. Se elabora un señuelo sofisticado que maximice las posibilidades de que la víctima caiga en la trampa y habilite la primera puerta de entrada a los atacantes.

Para explicar los ataques dirigidos y cómo se construye una APT, me gusta utilizar el ejemplo de una de mis películas favoritas: Ocean's Eleven. En esta película, un grupo de ladrones profesionales de guante blanco que visten de traje y corbata planean el asalto a uno de los objetivos más seguros de la ciudad de Las Vegas: el casino del Hotel Bellagio. Reúnen para ello a un equipo multidisciplinar, cada uno experto en un área específica. Pasan meses planificando cada detalle del ataque al casino. Analizan minuciosamente el entorno, la infraestructura, el personal y la operativa del casino. Un plan que requiere de una sofisticación considerable y que debe ser meticulosamente diseñado, como cualquier ataque dirigido, contemplando todas las posibilidades o dificultades que puedan surgir en cada paso. Durante su ofensiva, infiltran a un miembro de la banda como empleado del casino o roban una bomba para apagar la luz de la ciudad durante diez segundos y *resetear* así una alarma (sí, es ficción). Ejecutan un sinfín de actuaciones en las cuales la ingeniería social está siempre presente. Una de las partes más delicadas del ataque es extraer el dinero robado por la única salida posible sin ser detectados. Lo logran porque conocen de antemano el protocolo de actuación ante emergencias del Bellagio. En primer lugar, llaman al dueño para comunicarle que le están robando todo su dinero. Posteriormente interceptan la llamada del casino a los SWAT y son los propios atacantes disfrazados de agentes de operaciones especiales quienes acuden al rescate y aprovechan la circunstancia para sacar tranquilamente el dinero por la puerta principal del casino, sin que nadie se percate de ello. Es un ejemplo ideal de canal encubierto.

Otra característica de un ataque dirigido es que, pese a que transcurre fundamentalmente en el ciberespacio, en muchos casos se complementa con actuaciones en el mundo físico. Son los casos en los que es necesario acceder

físicamente a la sede o infraestructura de la organización objetivo, quizá para comprometer un servidor o dispositivo aislado de internet en una localización concreta, o bien en la fase de recolección de información, para acercarse al personal de la compañía y localizar algún empleado descontento que pueda convertirse en un caballo de Troya, también para llevar a cabo ataques de ingeniería social combinando elementos del mundo físico. Los límites están en las condiciones de cada escenario, los recursos y la creatividad de los atacantes.

Stuxnet, la primera ciberarma conocida

Uno de los ejemplos de APT más conocidos es Stuxnet, un ataque dirigido que tuvo lugar en 2009, y que hasta hoy se sigue considerando uno de los ataques más sofisticados de la historia. Fue el primer incidente real que motivó la creación del acrónimo APT.

Stuxnet fue una operación llevada a cabo en conjunto por Estados Unidos e Israel y que tenía como finalidad retrasar el programa de creación de armas nucleares de Irán. Para conseguirlo, se propusieron atacar la central nuclear iraní de Natanz. ¿De qué manera exactamente? Ocasionando daños controlados en los rotores y las válvulas de las centrifugadoras para ralentizar el proceso de enriquecimiento de uranio. El objetivo era tan ambicioso que por aquel entonces no se había visto ni en la ficción.

Podemos imaginar diferentes formas de comprometer ordenadores, *smartphones* o cualquier otro dispositivo conectado a internet. Pero cuando hablamos de sistemas de control industrial que forman parte de una central nuclear aislada de internet, la cruzada se antoja complicada. Más aún en el año 2009.

Los creadores de Stuxnet centraron primero sus miras en los controladores Siemens que se encargaban de regular válvulas y sensores de presión de las centrifugadoras. Fue la primera versión del ataque, menos sofisticada que la definitiva, y tenía forma de archivo de configuración para el *software* de Siemens. Requería que alguien abriese manualmente el archivo de configuración malicioso en uno de los portátiles que se utilizaban para configurar los sistemas y carecía de algún método de autopropagación. Cuando el archivo se ejecutaba, tomaba el control del sistema, pero su efecto era muy moderado. Aislaba etapas de las centrifugadoras, con lo que se incrementaba la presión del sistema. Cuando las válvulas de escape debían dejar salir el exceso de presión, no lo hacían. Aunque las válvulas disponían

de unos sensores de presión, Stuxnet los descalibró. La presión del sistema seguía subiendo hasta que el propio malware interrumpía el ataque.

De no parar el ataque, Stuxnet podría haber destrozado por completo la central nuclear de Natanz, pero este no era su propósito. Si lo hubiera hecho, los ingenieros iraníes habrían investigado exhaustivamente el incidente hasta dar con la raíz del problema y solventarlo. No se habría conseguido un retraso considerable en el programa nuclear iraní, que era el objetivo principal. En su lugar, era mucho más inteligente provocar fallos comedidos en las centrifugadoras que generasen estrés en los rotores y obligaran a reemplazos frecuentes. Los ingenieros iraníes invertían su tiempo en intentar resolver las incidencias buscando fallos en el diseño o la construcción del sistema en lugar de optimizar el rendimiento de la central. Difícilmente se les ocurriría pensar que un malware pudiera provocar fallos puntuales de esta manera. Resultaba impensable.

Si bien Stuxnet ya conseguía comprometer la seguridad de la central nuclear, dependía de que alguien en el interior de la central ejecutase el malware en el equipo en cuestión, y en un momento dado parece ser que se perdió el acceso. Es la segunda y definitiva variante de este programa malicioso la que hace honor a su fama y repercusión, y la sitúa como la primera ciberarma de la historia. Se especula que los creadores de esta versión definitiva podrían ser los ingenieros de la NSA.

El verdadero aspecto diferenciador de esta novedosa versión estaba sin duda en su método de infección y propagación. Teniendo como objetivo los controladores industriales Siemens S7-315 que se encontraban en el interior de la central, se planificó llegar a ellos a través de contratistas externos que trabajaban en la central, e infectar alguno de sus equipos para que el gusano informático se propagase hasta llegar al equipo que controlaba los dispositivos Siemens. Se utilizaron nada más y nada menos que cuatro vulnerabilidades Zero Day para lograrlo. Al no ser conocidas, permitían comprometer fácilmente los equipos atacados. El malware infectaba cualquier dispositivo que se conectara a las unidades USB de un equipo y lo transmitía de un ordenador a otro. Además, utilizaba una vulnerabilidad en sistemas Windows que le permitía infectar todos los equipos de la red interna a la que se conectara el equipo infectado. Solo era cuestión de tiempo que llegase a comprometer el ordenador que controlaba los Siemens S7-315.

Y así fue. Una vez controlados estos sistemas industriales, se modificó la velocidad de los rotores. Su velocidad se redujo de 63 000 rpm hasta casi pararlos a 120 rpm, para volver a llevarlos a la velocidad normal. En este

proceso, los rotores pasaban por varias velocidades críticas que los hacían vibrar, ocasionándoles daños que reducían su vida útil. Asimismo, el malware se ocupaba de que no se ejecutase correctamente el código que actualizaba las lecturas de velocidad de los rotores, por lo que a ojos de cualquiera que monitorizase el sistema, todo parecería normal. Es cierto que un cambio de velocidad tan grande en los rotores podría haber sido percibido por cualquiera que estuviese en la central, pero los ingenieros iraníes utilizaban auriculares protectores, con lo que no se percataron de estas alteraciones.

Así logró Stuxnet su propósito de generar pérdidas millonarias y retrasar el desarrollo del programa nuclear de Irán. Un malware que llegó a infectar más de 100 000 equipos en todo el mundo, ya que, aunque se diseñó para infectar los equipos de contratistas externos que accedían a la central nuclear de Natanz, el código malicioso se propagaba no solo por la red interna del equipo infectado, sino por los dispositivos USB que se iban conectando, y que a su vez se conectaban en otros equipos. De este modo el malware no se limitó al entorno de la central de Natanz, sino que se expandió por equipos en todo el mundo hasta que llegó a manos de los fabricantes de seguridad. Ellos fueron los que lo identificaron y sacaron a la luz un año después de su aparición, en 2010.

Esta información nunca ha sido confirmada oficialmente por el Gobierno estadounidense. No obstante, tras años de exhaustiva investigación acerca de cada detalle que rodeaba la trama de Stuxnet, se han ido obteniendo estas conclusiones. Muchas de ellas se han elaborado a partir de diversas evidencias que han permitido contrastar y verificar las diferentes hipótesis hasta llegar a confirmar su veracidad. Todas estas conclusiones acerca de Stuxnet están accesibles en los informes técnicos elaborados por algunos fabricantes del sector. En ellos se incluye información detallada sobre el funcionamiento de la central nuclear de Natanz, las centrifugadoras, rotores, válvulas, los sistemas de control industrial que los supervisan… así como todas las evidencias y aspectos técnicos acerca de las vulnerabilidades explotadas, el malware o el método de propagación. También se ha publicado un documental titulado Zero Days, que aborda todos los pormenores de Stuxnet y el futuro de las ciberguerras.

Stuxnet abrió la veda de este tipo de complejos ataques dirigidos. En los años siguientes, se identificaron otras APT similares en sofisticación y orientadas al ciberespionaje, como «Duqu», «Red October» o «Flame». Según el fabricante Kaspersky, Flame guardaba relación con Stuxnet debido a similitudes en alguno de sus módulos.

El ciberataque a Sony Pictures Entertainment

El segundo ejemplo de ataque dirigido corresponde a un incidente que tuvo lugar en diciembre de 2014 y que, sin llegar a los niveles de WannaCry, gozó de una trascendencia y repercusión mediática considerables. Un incidente que acabó derivando en un conflicto diplomático entre dos naciones: el ciberataque a la multinacional Sony Pictures Entertainment.

Todo comenzó la mañana del 24 de noviembre de 2014. Aquel lunes por la mañana, como si de una película de ficción se tratara, los empleados de la conocida multinacional vieron cómo, misteriosamente, sus equipos dejaban de operar con normalidad y mostraban como imagen de fondo un esqueleto con el título «Hacked by #GOP» y un mensaje de advertencia. En él, un grupo que se hacía llamar «Guardians of Peace» recordaba a los responsables de Sony que ya les habían advertido previamente. Según parece, algunos directivos de Sony habían recibido un *mail* el viernes anterior de un grupo llamado «God's Apstls» en el que pedían una compensación económica a cambio de no «bombardear» a la multinacional. Fue un mensaje ignorado como *spam*. Junto con la imagen del esqueleto, informaban de que continuarían sus ataques hasta que sus peticiones fueran satisfechas. Sostenían que habían obtenido todos los datos internos de la organización, entre los que supuestamente había información confidencial. Les daban hasta las once de la noche para tomar una decisión al respecto. Si no accedían a sus demandas, filtrarían al mundo la información de la compañía.

Desde la multinacional se comenzó a investigar el incidente y se ordenó a los empleados que apagaran sus equipos. Los sistemas de la organización no respondían. Una multinacional de la talla de Sony estuvo completamente paralizada durante varios días. Aquella primera noche en la que vencía el plazo no sucedió nada, pero pasados unos días, los miembros de «GOP» comenzaron a filtrar al mundo información sensible y confidencial de la compañía. En primer lugar, filtraron copias internas de cinco películas que aún no habían sido estrenadas. Una semana más tarde, comenzaron a liberar documentos internos de la compañía que incluían correos electrónicos y detalles del salario de varios directivos, incluido el CEO. También filtraron el domicilio, los números de la seguridad social y otros datos de 47 000 empleados de la multinacional. Pero esto era solo el principio.

En un correo enviado a diferentes medios de comunicación, un miembro del colectivo, que firmaba como «Boss of GOP», reivindicaba el ataque y la filtración de las películas. El grupo afirmaba que disponía de unos 100

terabytes de datos pertenecientes a Sony, y que los irían filtrando con el paso del tiempo.

Sony activó sus protocolos de respuesta ante incidentes, al tiempo que acudía al FBI y también al fabricante de seguridad FireEye, intentando proteger a los empleados, cuya información personal había sido expuesta, y reparar los daños ocasionados por el incidente en la infraestructura tecnológica de la organización, además de determinar la procedencia del ataque.

Las primeras especulaciones apuntaban a Corea del Norte como responsable del incidente por un motivo principal. La fecha del ataque coincidía en el tiempo con el estreno inminente de la película de Sony The Interview. Era una comedia acerca de dos periodistas que planeaban asesinar al líder de Corea del Norte, Kim Jong-un. Meses atrás, el régimen asiático había considerado públicamente el estreno del film como un acto de guerra y de terrorismo gratuito.

Unos días después de las filtraciones esta teoría cobró aún más fuerza, pues los miembros de Guardians of Peace volvieron a la carga. Lanzaron un comunicado en el que advertían que sembrarían el terror en los cines que proyectaran la película. Amenazaban a Sony con vivir «su 11 de septiembre particular» y recomendaban a todo el mundo mantener las distancias con los cines donde se estrenara The Interview: «Si tu casa está cerca, será mejor que te vayas».

Ante las amenazas, los protagonistas de la película cancelaron todas sus apariciones en medios de comunicación destinadas a promocionar el film. Las empresas que gestionaban las cinco cadenas de salas de cine más importantes de Estados Unidos decidieron no correr riesgos y retiraron la película de su cartelera navideña. Ese mismo día, Sony cedió ante las amenazas terroristas y comunicaron que cancelarían el estreno planificado para el 25 de diciembre, entendiendo y respetando la postura de los cines. Al mismo tiempo, anunciaron que no habría ningún otro plan de lanzamiento de la película.

El ciberataque a Sony llegó a convertirse en un problema de Estado. El presidente de Estados Unidos, Barack Obama, hizo referencia al incidente en una rueda de prensa el 19 de diciembre. Se lamentaba de la decisión de Sony de cancelar el estreno de la película, y se tomó el ataque a Sony Pictures como un ataque a la nación, por lo que lanzaron una advertencia: «Responderemos proporcionalmente y lo haremos en tiempo y de la manera que nosotros elijamos». Tres días después, Corea del Norte sufrió un apagón de internet. El país entero se quedó sin acceso a la red de redes durante diez

horas. Una denegación de servicio a toda una nación. Una portavoz del Gobierno de Estados Unidos evitó afirmar o desmentir la relación del apagón con la respuesta estadounidense.

En este proceso, el FBI declaró formalmente que, según sus hallazgos, el ciberataque a Sony guardaba relación con el Gobierno norcoreano. Basaban su alegato en el uso de técnicas y herramientas de *hacking* similares a las utilizadas en otros ataques provenientes de Corea del Norte. Esta teoría no es compartida por otros fabricantes y analistas que investigaron el incidente. Expertos de la firma Norse sostenían que el ataque había sido acometido por insiders, empleados de la propia organización. Señalaban en concreto a seis empleados que fueron despedidos de la multinacional tras una reestructuración en mayo de 2014. Algunos habían hecho declaraciones públicas en las que expresaban su descontento y hostilidad hacia la firma a causa de su despido y se encontraban en posición de encontrar la manera para acceder a zonas seguras de los servidores de Sony. Tras una reunión privada de tres horas, los miembros del FBI rechazaron esta posibilidad.

En febrero de 2016, transcurrido poco más de un año, diversos fabricantes, entre los que se encontraban Noveta, Kaspersky, Symantec, AlientVault o Trend Micro, publicaron un informe con los resultados de una investigación conjunta de este y otros incidentes, bajo el título «Operation Blockbuster». En él concluían que el ciberataque a Sony no había sido cometido por insiders o hacktivistas. En su lugar, relacionaban el ataque con otros perpetrados por el grupo de *hackers* «Lazarus Group», el que según las evidencias recolectadas por los investigadores, guardaba estrecha cercanía con el Gobierno de Corea del Norte. Al grupo se le atribuían otros ataques a diferentes estamentos y organismos de Corea del Sur. En 2015, habrían participado en ataques a bancos de Ecuador y Vietnam, y en 2016, se les acusó de haber sustraído 81 millones de dólares al Banco Central de Bangladesh. Este informe reforzaba la teoría inicial del FBI respecto a la responsabilidad del Gobierno de Corea del Norte en el ataque a Sony.

Como podemos ver, se trata de un incidente bastante complejo que generó un impacto considerable a nivel internacional por la magnitud de los hechos acontecidos, incluyendo amenazas terroristas. A una multinacional de la talla de Sony le fueron robadas cinco películas sin estrenar y una cantidad ingente de información confidencial que se fue publicando durante semanas. La compañía invirtió cerca de 15 millones de dólares en el primer trimestre de 2015 para sufragar los daños ocasionados por el incidente. Como curiosidad, Sony decidió estrenar finalmente la polémica película The Interview en

trescientas salas de cine independiente el día 25 de diciembre, como estaba previsto inicialmente.

Cómo estar preparado para detectar o responder ante una APT

Hemos repasado dos de los ejemplos más ilustrativos del actual panorama digital. Un campo de batalla donde no existen límites y donde es plausible casi cualquier acontecimiento que podamos imaginar. Además de estos ataques dirigidos, existen muchos otros ejemplos de amenazas persistentes avanzadas, orientadas a diferentes sectores específicos, como el financiero, la industria petrolífera o el sector químico. Cualquier organización del mundo está hoy expuesta como diana de un ataque dirigido de estas dimensiones. Si bien es cierto que exigen muchísima planificación y recursos, existen actores dispuestos a invertir lo necesario para ejecutar estas agresiones.

Es perfectamente posible que una organización de menor entidad se convierta en blanco de los atacantes. Por eso es fundamental tener nociones del concepto APT y de la manera en que estas amenazas son diseñadas, con vistas a tomar las medidas oportunas para detectarlas y hacerles frente.

Como responsable de una organización, algunas consideraciones al respecto:

- Es necesario tener en cuenta que lo más difícil en estos casos es precisamente la detección, dado el nivel de sofisticación que incorporan estos ataques.
- Es esencial dedicar recursos a la monitorización de todos los niveles de infraestructura y sistemas de la organización, utilizando diferentes soluciones de fabricantes.
- Existen soluciones específicas dedicadas a la prevención del robo o la pérdida de información, conocidas como soluciones DLP (Data Loss Prevention), que pueden ser implementadas para prevenir en parte este tipo de amenazas.
- Dada la complejidad del tema, se necesita de profesionales especializados en la materia que puedan ayudar a detectar e identificar este tipo de amenazas.
- Lo normal en el caso de pequeñas y medianas empresas es que este servicio se contrate a profesionales o empresas externas que se constituyan como el centro de respuesta a incidentes de la organización.
- Además de todo esto, es indispensable impartir formación y concienciación a los diferentes trabajadores en materia de

> ciberseguridad, con el fin de conocer de primera mano no solo las amenazas genéricas de las que puedan haber oído hablar, sino de los ataques más perfeccionados que acechan a las empresas.

En muchas de las sesiones de concienciación que suelo impartir al personal no técnico de las organizaciones, trato de incidir con detenimiento en el concepto de ataque dirigido, realizando algunas demostraciones prácticas de cómo podría planificarse un ataque de este tipo de manera muy simplificada. Utilizo para ello tanto la información que existe de la organización como la de los propios empleados, procurando hacerles ver que cualquier detalle puede ayudar a los ciberdelincuentes a lograr su cometido. Es esencial pensar siempre en cómo los atacantes con intenciones maliciosas podrían utilizar la información personal y corporativa que exponemos. Aunque una APT es algo muy sofisticado que requiere de muchas variables y factores para prosperar, cuanto más difícil se lo pongamos a los enemigos potenciales, menos posibilidades de éxito tendrán.

11

Lo que la red sabe de nosotros: el Gran Hermano

En plena era del Big Data, uno de los temas que preocupa cada vez más al conjunto social es el valor que tienen nuestros datos y el uso o abuso que hacen de ellos los gigantes tecnológicos. La gran mayoría de usuarios es consciente de que proveedores como Facebook, Google, Twitter o Instagram nos proporcionan una serie de servicios con funcionalidades increíbles de manera gratuita y asumen como algo normal facilitar a cambio sus datos e información personal.

No en vano, una de las frases más recurrentes a la hora de abordar el tema es: «Cuando algo es gratis, el producto eres tú». Es evidente que las compañías tecnológicas que nos ofrecen esta amalgama de servicios no viven del aire. Su modelo de negocio se sostiene rentabilizando la información que millones de usuarios vierten en sus sistemas, por ejemplo, vendiéndola a anunciantes con fines comerciales.

Esto es un hecho que la gran mayoría de usuarios acepta sin mayor problema, sabedores de que está en ellos establecer o no los límites a la hora de compartir información. A pesar de ello, veremos que no siempre es así.

Muchos se percatan del riesgo que supone para su privacidad exponer demasiados aspectos de su vida personal: fotografías de sus hijos, domicilios, profesión, actividades de ocio, lugares que visitan, destinos vacacionales… Pero lo hacen de manera voluntaria, sin reparar más allá de las consecuencias evidentes que se deducen de tales acciones, como el hecho de que sus amigos en redes, o amigos de amigos, puedan acceder a esta información. Se puede obtener muchísimo conocimiento adicional de los usuarios por su actividad en la red. Analizando los contenidos que los usuarios vierten en redes sociales como Facebook, Twitter o LinkedIn es posible generar muchísima Inteligencia, siempre dependiendo de las publicaciones y del comportamiento

de cada usuario en particular. Algunos de los datos que se pueden obtener, además de los propios que los usuarios comparten de manera voluntaria (tales como lugar de nacimiento, residencia, edad, profesión…), son: *hobbies*, intereses, ideología política, nivel socioeconómico, nivel cultural, creencia religiosa… En algunos casos, es posible inferir el perfil psicológico de un usuario tan solo a través de sus publicaciones o sus likes. Cualquier actividad, por pequeña que sea, deja un rastro susceptible de ser analizado o interpretado.

Todos estos aspectos no solo afectan a la privacidad de los usuarios, sino que suponen un riesgo indudable para su seguridad. Como hemos visto en los ataques dirigidos, cuanta más información obtenga un atacante de un objetivo concreto, más vectores de ataque encontrará. Todo el conocimiento generado es clave para planificar esquemas de ingeniería social e intentar comprometer a los usuarios. Comentaremos algunos ejemplos a la hora de hablar de ciberinteligencia.

El caso de Facebook y Cambridge Analytica

La intromisión de los proveedores tecnológicos en la privacidad de los usuarios es uno de los temas que más debate suscita en la actualidad, y son muchos los incidentes que han generado controversia. El más reciente y notorio es el que situó a Facebook en el disparadero a mediados del año 2018, a raíz del escándalo de Cambridge Analytica, una fuga de datos que afectó a alrededor de 87 millones de usuarios de Facebook y acabó con Mark Zuckerberg compareciendo ante el Senado y el Congreso de Estados Unidos para pedir perdón, así como para dar explicaciones sobre lo acontecido.

Cambridge Analytica era una consultora británica famosa por haber trabajado para la campaña presidencial de Donald Trump. Sus problemas comenzaron cuando un exdirectivo declaró que la compañía había comprado datos de millones de usuarios de Facebook sin su consentimiento. Se obtuvieron a través de una aplicación de perfiles psicológicos desarrollada en 2014 por un investigador de la Universidad de Cambridge. El aplicativo, solicitando los permisos correspondientes, accedía a los datos de los usuarios que instalaban la herramienta. El problema es que también recababa los datos de todos sus contactos sin su consentimiento. Todos estos datos fueron entregados a Cambridge Analytica. El exdirectivo de la compañía afirmó que la información se utilizó para perfilar votantes y dirigirles propaganda personalizada, así como noticias falsas. Esto supuestamente influyó en las

elecciones estadounidenses y en otros procesos electorales, como el referéndum del brexit a través de empresas vinculadas.

Estas revelaciones generaron un revuelo mediático que puso en graves aprietos no solo a Cambridge Analytica, sino también a la todopoderosa red social. Las primeras noticias hablaban de una fuga de datos que implicaba a 50 millones de usuarios. En el análisis realizado *a posteriori* por Facebook, esta cifra ascendió a 87 millones. Además de pedir perdón en sucesivas ocasiones ante los medios y los estamentos políticos, Facebook se vio obligada a revisar las condiciones de privacidad y la gestión de la información personal de los usuarios.

Por su parte, la consultora británica, pese a defender su inocencia afirmando que sus empleados actuaron de manera ética y legal, tuvo que cesar su actividad. La presión del entorno y la cobertura mediática influyeron de tal manera que tanto sus clientes como sus proveedores se distanciaron de la compañía. El negocio ya no era viable.

El incidente colocó de nuevo el foco sobre el abuso de los principales gigantes de internet de los datos de los usuarios. No solo Facebook maneja información sensible de sus usuarios. Merece la pena comentar algunos ejemplos más.

Google y los datos que almacena de los usuarios: el ojo que todo lo ve

Empresas como Apple o Google también manejan gran cantidad de datos que recaban desde los servicios interconectados que ofrecen a sus usuarios. Muchos de ellos desconocen que estos datos están siendo recolectados. Aunque se incluya esta información en las políticas o licencia de uso, prácticamente nadie las lee. Además, en la mayor parte de los casos, los datos se recogen por defecto. ¿Qué quiere decir esto?

Google almacena de manera predeterminada la información de todo nuestro historial de navegación desde el ordenador o el móvil si estamos conectados con nuestra sesión iniciada. Esta no se cierra a no ser que lo hagamos expresamente. De este modo, cuando realizamos cualquier búsqueda en internet o accedemos a cualquier página, Google registra esta información. También se archivan todas las búsquedas de vídeos en Youtube, así como nuestras ubicaciones cuando utilizamos Google Maps. Google tiene una función que registra todos y cada uno de nuestros movimientos si tenemos habilitado el historial de ubicaciones de Google Maps. Como siempre, suele

estar habilitado por defecto en nuestros dispositivos, por lo que, si no cambiamos la configuración, Google seguirá todos nuestros pasos. Es capaz de saber dónde hemos estado cada día, el medio de transporte que hemos utilizado, las paradas en establecimientos y nuestras rutinas diarias. Con esta información puede aportarnos funcionalidades útiles, como avisarnos de que debemos salir hacia el aeropuerto si no queremos perder nuestro vuelo. Google une la información de nuestra ubicación con la congestión del tráfico en esa zona y con la de nuestro calendario. Cuando hemos comprado un billete de avión, tras recibir el correo de la compañía aérea, Google ya ha incluido automáticamente una cita en nuestro calendario para el día de la salida con el número de vuelo y los datos pertinentes. Todo ello sin que nosotros hayamos hecho nada.

Pero hay más. Google posee la información de todos nuestros contactos telefónicos si están almacenados en Google Contacts, o la información que subimos a la nube, así como la que eliminamos si somos usuarios de este servicio. En el pasado, el gigante tecnológico leía también los correos electrónicos de los usuarios de Google Mail para ofrecerles publicidad personalizada. Lo hacía con todos los que utilizaran la versión gratuita de Gmail para su correo personal, pero no para las empresas que adoptasen este servicio de pago como solución de correo corporativa. No obstante, en 2017 el vicepresidente de Google anunció que se dejarían de leer los correos electrónicos de los usuarios.

Es tanta la información que Google tiene de nosotros y de nuestra actividad, que la teoría de un Gran Hermano que nos vigila a todos cobra fuerza. No obstante, si un usuario quiere, puede deshabilitar muchas de estas funcionalidades y evitar que Google almacene datos sobre sus búsquedas, preferencias, historial de navegación, gustos, rutinas, ubicaciones, viajes, citas profesionales o médicas y contactos. Ha de hacerlo expresamente para cada uno de estos servicios, rebuscando entre las opciones de configuración de privacidad. La contrapartida es que, dependiendo de algunos casos, perderá algunas funcionalidades y servicios. Es cuestión de valorar el punto de equilibrio entre las funcionalidades que nos ofrecen y la exposición de nuestra privacidad.

- Google pone a disposición de los usuarios un servicio llamado «Google TakeOut», donde cualquiera puede descargarse una copia de todos y cada uno de los datos propios almacenados.
- Si quieres conocer y controlar los datos que Google tiene de ti, accede a su web y solicita una copia de tus datos.

- Google te enviará a tu correo un enlace para descargarte una copia organizada en la que podrás consultar todo lo que el buscador sabe de ti.

No solo Google almacena datos de sus usuarios. Prácticamente todos los proveedores lo hacen por defecto. Cuando un usuario configura un iPhone por primera vez, Apple le mostrará un asistente mediante el que, entre otras cosas, activará iCloud, el servicio de nube para los usuarios de la manzana. Por defecto, a no ser que el usuario lo indique de manera expresa, iCloud configurará copias de seguridad que incluirán fotos, correos, contactos, contraseñas de servicios o redes *wifi*, historial de navegación de Safari o las conversaciones de WhatsApp de los usuarios. Muchos de estos datos son compartidos por los diferentes dispositivos que el usuario tiene configurados en la misma cuenta de iCloud. De este modo, si el usuario introduce la contraseña de una red *wifi* en su iPhone al conectarse por primera vez, no tendrá que hacerlo cuando utilice su iPad o Macbook Pro, puesto que la contraseña se habrá almacenado en iCloud.

Como vemos, algunas de las funcionalidades aportan valor a los usuarios, mientras que otras suponen una intrusión en su privacidad más que otra cosa. Como siempre, es el usuario quien debe decidir qué funcionalidades mantener y cuáles deshabilitar para evitar que los gigantes tecnológicos se inmiscuyan en su privacidad.

Las smart TV que escuchan a sus usuarios

Existen infinidad de ejemplos, además de los más típicos de Apple o Google. La llegada al mercado de las smart TV trajo consigo nuevas alternativas para que los proveedores pudiesen registrar información de los usuarios. Samsung, en un intento de transparencia, informó en sus políticas de uso de que sus televisores podrían escuchar a los usuarios incluso cuando estos no estuviesen viendo la televisión, con el fin de mejorar su funcionalidad de reconocimiento de voz. Esto generó bastante polémica entre los usuarios, pero al menos Samsung informaba de ello. LG, su principal competidor en el mercado de las smart TV, registraba en su día información privada de los usuarios sin notificarlo y, por supuesto, sin requerir su consentimiento. Enviaba a sus servidores la información de los canales y programas de televisión que los usuarios veían, así como de los contenidos que visualizaban a través de *pendrives* USB que pinchaban en el televisor.

Cómo proteger nuestra privacidad

Existen infinidad de técnicas, posibilidades y canales por los que los proveedores de servicio recolectan datos de los usuarios atentando contra su privacidad. La manera de evitarlo dependerá en cada caso del proveedor y de las alternativas que ponga a disposición de los usuarios. Dicho esto, es posible establecer algunas recomendaciones generales que ayuden a aumentar nuestro nivel de privacidad:

- Cuando utilizamos cualquier servicio en internet, es recomendable dedicar un rato a leer las políticas de uso y las cláusulas, buscando información complementaria en la red sobre las condiciones de privacidad.
- Del mismo modo, es indispensable revisar concienzudamente todas las opciones de configuración de privacidad y seguridad para cada servicio.
- En general, habrá que hacerlo no solo al principio, sino de manera frecuente. Los proveedores modifican a menudo sus opciones de configuración y sus políticas precisamente para volver a recopilar datos de usuarios. Lo hacen sabiendo que estos dan su consentimiento sin leer los cambios ni explorar las opciones modificadas.
- En las opciones de configuración, debemos deshabilitar expresamente todo lo que no queremos que se almacene.
- A la hora de configurar dispositivos o servicios, no deberíamos habilitar aquellos que no nos aporten valor y que nunca vamos a utilizar. No conviene exponer información ni datos si encima no obtenemos nada a cambio.
- Si no queremos que proveedores como Google almacenen la información de nuestra actividad, además de deshabilitar las opciones correspondientes, podemos navegar sin iniciar sesión con nuestra cuenta.

En cierto modo, se trata de aplicar la filosofía *hacker* a la hora de utilizar cualquier nuevo producto o servicio: sin conformarnos con utilizar las funcionalidades que se nos presentan, explorando e investigando en detalle todas las opciones de configuración y la manera en que afectan a nuestra privacidad y seguridad. Obviamente, dentro de las posibilidades que cada proveedor nos ofrece.

La responsabilidad de proteger los datos de los usuarios

En este capítulo hemos abordado cómo los proveedores tecnológicos recopilan los datos de sus usuarios a partir de los servicios que prestan. Esto es bien diferente de los casos en los que los datos se filtran por una mala praxis de los proveedores, a causa de vulnerabilidades o problemas de seguridad, como en algunos de los ejemplos comentados en otros capítulos. Este tipo de errores por parte de los proveedores puede suponer un serio riesgo para la privacidad de los usuarios, sobre todo si manejan datos sensibles, como los relacionados con la salud.

Es el caso de las vulnerabilidades que descubrí a mediados de 2018 en una solución para gimnasios desarrollada por una empresa española. Era una aplicación móvil que daba soporte a 1600 gimnasios en 16 países, muchos de ellos en España. Entre otras cosas, demostré que era posible acceder a las rutinas de entrenamiento de todos los usuarios de cada gimnasio a los que daban soporte. Y no solo eso. Lo realmente grave era el acceso a los informes en PDF que se generaban para cada usuario, tras realizar un control de peso en el gimnasio. Junto al nombre, los apellidos y la foto de todos los clientes, se podía ver su índice de masa corporal, porcentaje de grasa, nivel de líquidos corporales, edad metabólica, tejido adiposo o porcentaje de masa muscular. Por no tener en cuenta la seguridad al desarrollar la aplicación, podía acceder sin problemas a los datos de salud de cerca de 10 millones de personas en todo el mundo. Evidentemente, reporté las vulnerabilidades a la empresa correspondiente. Aunque en un principio no recibí respuesta por su parte, tras publicarlo en una conferencia y cuando los medios de comunicación nacionales se hicieron eco de la noticia, algunos de sus clientes pusieron el grito en el cielo. Fue entonces cuando me contactaron para que les informara del alcance de las vulnerabilidades, dedicando esfuerzos para remediar el problema.

El tema de los datos es muy delicado. Si como responsable de una empresa manejas datos personales de usuarios, debes asegurarte de que se implementan los mecanismos correctos para garantizar su integridad y seguridad, e informar de cualquier problema o incidente que se genere. Como comentamos en el capítulo 3, a raíz de la entrada en vigor del nuevo reglamento europeo en mayo de 2018, la cuestión adquiere más relevancia que nunca. Las sanciones a las que se puede enfrentar una organización son

considerables y podrían acabar incluso en la quiebra y la total desaparición de la empresa responsable.

12

OSINT, ciberinteligencia y WhatsApp como fuentes de conocimiento

A la hora de hablar de ataques dirigidos y de su planificación por los ciberdelincuentes, introdujimos el concepto Open Source Intelligence (OSINT). Este acrónimo, que en origen se utilizaba tan solo en el ámbito militar, está hoy día muy ligado al mundo de la ciberseguridad. Se refiere a la inteligencia basada en fuentes abiertas o de acceso público. ¿Cuáles son estas fuentes? Pues básicamente cualquier entidad de información accesible de manera pública o abierta:

- Medios de comunicación tradicionales: prensa, televisión, radio, revistas.
- Medios de comunicación en línea, sitios web, blogs, wikis, foros.
- Información pública de fuentes gubernamentales.
- Redes sociales.
- Conferencias, simposios, papers académicos…

Estas fuentes, unidas a cualquier otra que se nos pueda ocurrir (siempre que sea accesible y pública), constituyen la base sobre la cual se aplican las técnicas OSINT.

Tradicionalmente, OSINT era conocido y utilizado junto a otros, como HUMINT, TECHINT, SIGINT o MASINT, en el contexto militar y de la defensa. Se empleaba para recolectar información de posibles objetivos y generar Inteligencia acerca de potenciales enemigos hostiles, con el fin de velar por la seguridad nacional. El concepto aparece de manera recurrente en boca de los protagonistas de series como Homeland, con tramas de espionaje entre gobiernos y agencias de Inteligencia, como la CIA o el Mossad.

A día de hoy, OSINT se utiliza casi con más recurrencia en el ámbito de la ciberseguridad. En primer lugar, porque los ataques en el ciberespacio funcionan de manera similar a los que se acometen en el mundo físico, sobre todo en lo que a planificación se refiere. Es indispensable la generación de Inteligencia sobre objetivos en el aspecto ofensivo, así como sobre amenazas en el aspecto defensivo si se quiere tener éxito en la cruzada.

En segundo lugar, con la evolución de la red y la proliferación de dispositivos tecnológicos y servicios, el número de fuentes abiertas ha crecido hasta tal dimensión que prácticamente utilizando únicamente la información disponible en internet y explotándola adecuadamente, es posible correlacionar datos para obtener Inteligencia de personas u organizaciones. Se ha de analizar, clasificar, normalizar y procesar una cantidad de información descomunal.

Si, por ejemplo, queremos extraer información de los empleados de una organización, sabemos que es posible obtenerla consultando diferentes fuentes: el sitio web de la organización, una memoria corporativa, si existe, los perfiles de los trabajadores en LinkedIn, las direcciones de contacto en ofertas de empleo u otros comunicados…

Consultar todas ellas es una tarea ardua que requiere de cierta dedicación. Hay que asumir que en algunos casos será necesario realizar búsquedas manuales para localizar el punto exacto en el que se encuentra la información que necesitamos, pero el grueso del análisis se abordará con herramientas automatizadas que nos permitan un adecuado tratamiento de la información. Lo realmente importante es conocer bien las fuentes sobre las que se trabaja y los fundamentos de las herramientas empleadas.

Existen muchas herramientas OSINT dedicadas a extraer información de fuentes diferentes que han sido desarrolladas por investigadores de la comunidad *hacker* y que son aprovechadas por los ciberdelincuentes para recolectar información y planificar los ataques.

El ejemplo de los metadatos en ficheros de ofimática

Para ilustrar esta última disertación, podemos retomar el ejemplo en el que pretendemos obtener información de los empleados de una organización. Además de las fuentes habituales, existen muchos ficheros ofimáticos en formatos PDF, Excel o Word que, además del contenido, almacenan metadatos. Los metadatos son atributos, entidades de información asociadas a los ficheros que aportan información sobre los propios datos contenidos. Son

ejemplos de metadatos el nombre del fichero, el tamaño, la fecha de creación, la fecha de modificación, la versión, el autor, el programa con el que ha sido generado… Todos van incrustados por defecto en los propios documentos, a no ser que se eliminen explícitamente.

Muchas organizaciones cuelgan documentos ofimáticos de diverso tipo en sus sitios web, a menudo ficheros PDF. Generalmente, cuanto mayor es la dimensión de la organización, más ficheros podremos encontrar. Si descargamos estos PDF y analizamos los metadatos que contienen, es posible obtener información acerca de empleados de la organización, que pueden ser visibles sin que nadie se haya percatado de ello. Entre otras cosas, podremos encontrar nombres y apellidos de trabajadores, sus nombres de usuario, direcciones de correo, nombres de impresoras, rutas internas de unidades compartidas, así como versiones concretas del *software* instalado en sus equipos.

Como puedes imaginar, hablamos de información valiosa que permitiría a los atacantes generar inteligencia sobre el objetivo mientras preparan la artillería para la ofensiva. Descubrirían usuarios a los que investigar para tejer una elaborada telaraña de ingeniería social o podrían identificar y explotar vulnerabilidades del *software* que corre en sus equipos.

La búsqueda de metadatos en los documentos públicos de una organización es una práctica muy manida en el mundo del *hacking*. Se conoce desde hace ya muchos años y representa tan solo una más de las diversas técnicas OSINT en la investigación de un objetivo. Sin embargo, resulta curioso ver los rostros de asombro de los asistentes en las sesiones de concienciación cuando les enseño la información que se puede recabar en tiempo real a través de los metadatos. Su sorpresa aumenta cuando utilizamos su propia organización como ejemplo.

El concepto de ciberinteligencia

El término ciberinteligencia hace referencia a la inteligencia generada a partir de la información que existe en el ciberespacio. Este concepto es un tanto ambiguo o abierto. Por un lado, se utiliza el término para hacer referencia a la inteligencia recabada en el análisis de amenazas, campañas de malware, actores involucrados… Es información que los fabricantes incorporan luego en sus dispositivos de seguridad para detectar o neutralizar ataques en tiempo real. Por otro lado, ciberinteligencia se utiliza indistintamente para hablar también de Inteligencia basada en fuentes abiertas u OSINT.

Por supuesto, las redes sociales constituyen una pieza fundamental a la hora de aplicar OSINT y recolectar inteligencia sobre objetivos. Muchos usuarios vierten compulsivamente contenidos en redes como Facebook, Twitter, LinkedIn o Instagram.

La potencia que tiene el uso de estas técnicas se ejemplifica al cruzar datos de diferentes fuentes, casando un perfil con otro. Si una persona tiene un perfil en Facebook y somos capaces de encontrar un perfil suyo en una red social como Badoo, aunque utilice otro nombre o un pseudónimo (ya que típicamente en esta red los usuarios utilizan *nicks* y no publican información personal), podríamos saber que el usuario tiene necesidades afectivas o que es proclive a entablar relaciones de amistad, emocionales o sexuales con otras personas. Es un ejemplo muy sencillo, pero podría facilitar las cosas a los atacantes en sus planes de ingeniería social.

Uso de otras fuentes como WhatsApp

Como ejemplo de que siempre es posible buscar nuevas fuentes que utilizar para la obtención y generación de Inteligencia, es interesante comentar un trabajo de investigación que publiqué hace unos años en diversos congresos de ciberseguridad, relacionado con la utilización de WhatsApp como fuente OSINT. Todo comenzó con el descubrimiento de una vulnerabilidad que tuvo bastante repercusión. Hacia finales de 2013, me dispuse a investigar el protocolo de comunicación de WhatsApp, dado que en un principio fue noticia por sus problemas de seguridad, aunque al mismo tiempo se había erigido como dueña absoluta en lo que a sistemas de mensajería instantánea se refiere.

Por aquel entonces, WhatsApp ofrecía ya unas garantías adecuadas de seguridad, puesto que el protocolo había sido corregido en varias ocasiones, y en aquel momento la información transmitida se cifraba correctamente. Pero analizándolo mejor descubrí que, antes de iniciar la comunicación cifrada con los servidores de WhatsApp, nuestros dispositivos enviaban un paquete en texto plano sin cifrar, con información relevante sobre el sistema operativo, la versión de la aplicación y nuestro número de teléfono con el prefijo del país, puesto que en WhatsApp el número de teléfono es el atributo utilizado para identificar de forma inequívoca a nuestro usuario.

Una vez descubierto, era fácil inferir que cualquiera que monitorizara el tráfico en una red (como las *wifis* abiertas de hoteles, aeropuertos, cafeterías o centros comerciales) podría capturar este paquete en texto plano y obtener así

los números de teléfono de los usuarios que estuviesen conectados en redes abiertas. Así que desarrollé una herramienta llamada WhatsApp Discover, orientada a la extracción automatizada de toda esta información, incluyendo los números de teléfono de los usuarios que estaban utilizando WhatsApp, la información de sus dispositivos y la versión del aplicativo.

En mis conferencias la utilizaba para capturar en tiempo real los números de teléfono de los asistentes que se conectaban a la *wifi* del evento. Quedaban perplejos al ver en pantalla la información de sus dispositivos. La herramienta se incluyó en distribuciones de Linux como Wifislax, utilizada por la comunidad de profesionales de la ciberseguridad.

WhatsApp Discover estuvo funcionando durante dos años, aproximadamente hasta marzo de 2016, cuando WhatsApp introdujo el cifrado punto a punto para todos los sistemas operativos a los que da soporte y modificó el protocolo por completo. Durante aquellos dos años, sus desarrolladores intentaron ocultar la información del número de teléfono. Lo que hacían en realidad era mover la información de sitio dentro del paquete o camuflarla. Yo liberé varias versiones actualizadas de la herramienta cada vez que esto pasaba. Era como el juego del ratón y el gato.

Por medio del uso de WhatsApp Discover en un montón de redes *wifi* públicas por todo el mundo durante mis viajes de trabajo, recopilé muchísimos números de teléfono de usuarios anónimos, tanto en España como en el extranjero. Al analizar con detalle el tráfico que dichos usuarios generaban en la red, junto con la información pública de su perfil de WhatsApp (foto de perfil, hora en línea y estado), me di cuenta de que podía inferir mucha información de sus vidas sin conocerlos de nada.

Fue entonces cuando pensé en la posibilidad de explotar WhatsApp como fuente OSINT y comencé a investigar si era posible generar Inteligencia a partir de la información que los usuarios publicaban en esta popular aplicación. Desarrollé otra herramienta, llamada WhatsApp Intelligence, la cual, a partir de una lista de usuarios, se conectaba diariamente a los servidores de WhatsApp y descargaba la foto de perfil, el estado y la hora en línea de cada contacto, y los almacenaba en una estructura de directorios y en una base de datos para su posterior explotación. En definitiva, automatizaba la recogida de información que un usuario ojea habitualmente en su lista de contactos y la ordenaba para su análisis. También recopilaba información de usuarios anónimos.

El resultado de la investigación fue bastante interesante, a la par que sobrecogedor. Es increíble la cantidad de información que se puede obtener

de las personas a través de la tecnología. Individuos que comunican sus sentimientos, emociones o estados de ánimo. Los datos que aportan los estados del perfil o las fotografías nos revelan *hobbies*, intereses, mascotas, ubicaciones o el rostro de los hijos menores de edad.

De entre todos los perfiles recopilados, uno que me llamó mucho la atención fue el de una mujer, que utilizaba en su perfil diferentes fotos donde aparecía con sus hijos pequeños. Analizándolo conjuntamente con la información de su estado, podíamos conocer los nombres de estos chicos, pues los mencionaba en uno de ellos: «Mis joyas: A, B y C». En otro estado anterior, promocionaba el nombre de su propio negocio. Buscando el nombre de la empresa en la red, se llegaba también a un perfil de Badoo que correspondía al de la pareja de la mujer. Indicaba que estaba abierto a hacer nuevos amigos, y ambos aparecían juntos en varias fotografías. También aparecían juntos en las fotos del WhatsApp de ella. Si hubiésemos prolongado el seguimiento a lo largo del tiempo, seguro que habríamos obtenido mucha más información.

En muchos casos, fue posible cerrar el ciclo y lograr identificar con nombre y apellidos a los usuarios anónimos de WhatsApp, localizados aleatoriamente en redes *wifi*. ¿Cómo? Llegando a sus perfiles de redes sociales a través de la foto de perfil, pues era la misma que utilizaban en WhatsApp.

Decir que alguien podría planificar el ataque a una organización basándose tan solo en la información que publican sus empleados en WhatsApp podría parecer exagerado. Pero sin duda, se trata de una fuente de información extra que colabora en la creación de la Inteligencia necesaria para planificar estos ataques.

Otra vertiente de análisis es la adicción o la dependencia que tenemos los usuarios de WhatsApp. Algunos están permanentemente conectados. Si quisiésemos hacer un seguimiento a un usuario que sigue un patrón regular de conexiones a WhatsApp, podríamos inferir, entre otras cosas, a qué hora se levanta y se acuesta, cuáles son los tramos horarios en los que dedica más tiempo a utilizar este sistema de mensajería, cuáles son los tramos en los que no es tan activo por otras obligaciones… Estos aspectos, cruzados con la Inteligencia extraída de la información de su foto de perfil o de su estado, nos revelaría mucho conocimiento de un potencial objetivo. En los próximos años, con el desarrollo constante de nuevas aplicaciones y funcionalidades, los datos y la información serán cada vez más profundos y precisos.

Imaginemos un análisis de este tipo sobre los vigilantes de una organización. Como vimos en el ejemplo de Ocean's Eleven, el intento de acceder físicamente a la sede de una institución con el fin de recabar información o tener acceso físico a un sistema forma parte de las posibilidades en una amenaza persistente avanzada (APT). Si rastreamos los perfiles de WhatsApp de los vigilantes, no es para nada desacertado pensar en la posibilidad de utilizar esta información para planificar el ataque en función de sus turnos. Podríamos determinar quién es el más permisivo, cuál de ellos está triste o sus aficiones e intereses, para poder entablar una conversación casual y caerles bien utilizando la ingeniería social.

Algunas recomendaciones para ponérselo difícil a los ciberdelincuentes

Hemos comprobado que el potencial que tiene el uso de fuentes y técnicas OSINT es inmenso. Desde la perspectiva como usuarios o responsables de una organización, deberíamos tener claro que exponer información pública es inevitable, a la par que necesario. Es indispensable tener presencia en internet, tanto a nivel personal como corporativo. No obstante, ahora que conocemos las aproximaciones utilizadas por los ciberdelincuentes para planificar los ataques, debemos pensar en cómo podemos ponérselo difícil. Se trata de evitar, en la medida de lo posible, la exposición de información que no aporte valor. Algunas consideraciones:

- Como responsables de empresa:
    - A la hora de publicar documentos ofimáticos en sitios web, existen soluciones para limpiar todos los metadatos y evitar exponer información sensible.
    - Este ejercicio debe hacerse para todos los canales por los que la organización difunde contenidos e información y valorar aquella que podría facilitar un ataque contra la compañía.
    - Es interesante realizar o encargar a algún experto un estudio de toda la información que un atacante pudiese recopilar con estas técnicas, para identificar aquella que se debe filtrar o eliminar de la red.
    - Tiene sentido ocultar o eliminar esta información identificada como potencialmente peligrosa siempre y cuando no sea contraproducente para el negocio.
- Como usuarios:

- No existe una receta mágica para determinar qué se debe compartir o no en redes sociales o en sistemas de mensajería.
- Cada usuario puede elegir hasta dónde exponer su privacidad y qué aspectos de su vida compartir.
- Lo recomendable desde el punto de vista de la seguridad es exponer cuanta menos información mejor, pero esto es algo que cada usuario debe decidir.
- Por poner un ejemplo: a la hora de compartir la foto de perfil, el estado o la hora en línea en aplicativos como WhatsApp, pueden habilitarse opciones de privacidad que restrinjan esta información solo a nuestra lista de contactos. Así impedimos que un desconocido monitorice nuestra vida, al menos mediante este medio.
- Lo mismo ocurre a la hora de compartir contenidos en otras redes como Facebook o Instagram.
- Por tanto, cada usuario ha de encontrar el punto de equilibrio entre la información que comparte y la privacidad que expone.
- Lo que sí es esencial es controlar y conocer en detalle toda la información que se comparte, con quién se comparte y hasta dónde se comparte. Sin eso, es imposible evaluar lo que un atacante con fines maliciosos podría inferir acerca de nosotros.

13

Mitos y realidades de la Internet Oscura

Uno de los temas que siempre salen a la palestra a la hora de hablar del ciberespacio y el universo de los *hackers* es el de la famosa Internet Profunda. La idea de un oscuro universo paralelo en las entrañas del underground, donde se pueden encontrar las mayores atrocidades jamás concebidas, resulta cuanto menos interesante.

Probablemente habrás leído u oído hablar de esta Internet Oscura y de algunos de sus tópicos más asentados, como el de la famosa imagen del iceberg. Es un gráfico que aparece siempre en todos los artículos o noticias que tratan el tema. Con él se expresa que la internet que todos conocemos, la Surface Web, con sitios web estándar, redes sociales, medios de comunicación o foros constituye tan solo la punta del iceberg.

Según este gráfico, lo que la mayor parte de los usuarios conoce de la red representa tan solo el 4 por ciento del internet global. La llamada Internet Profunda o Deep Web, esa que no es accesible para la gran mayoría de los mortales, constituye el otro 96 por ciento. También se distingue entre los diferentes «niveles de acceso» a la información que hay en ella, enumerando lo que puede encontrarse en cada uno, así como los peligros que se afrontarían si se avanza de nivel. Por poner un ejemplo, según estos gráficos, el nivel cuatro «es un nivel peligroso si el usuario es detectado», y aseguran que: «puede recibir años de cárcel por el hecho de estar en estos sitios con pornografía infantil». En el nivel seis, «los mejores *hackers* logran acceder, el riesgo de que te descubran es muy alto, y se pueden encontrar suicidios y muertes en vivo». Dependiendo del sitio donde consultemos este gráfico, habrá seis o siete niveles. Algunos hablan incluso de un sitio llamado «Mariana's web», al que atribuyen el 2 por ciento de internet. Según especifican, «el que llegue aquí es realmente un genio. En este sitio se

encuentra un código inmensamente grande, unos 15 543 dígitos, entre números y letras». Algunos portales web especifican que en algunos de los niveles más altos «se pueden encontrar cosas tan terroríficas que serían capaces de arrastrar al usuario al suicidio, por lo que se ha de extremar la precaución y estar bien preparado ante lo que pueda encontrarse».

Todas estas afirmaciones distan mucho de la realidad, por no decir directamente que son patrañas. Cualquiera que se haya interesado un poco por conocer los entresijos de este mundo es capaz de percatarse. Increíblemente, he coincidido en eventos con algún profesional del sector que ostentaba un puesto relevante en una empresa puntera y que aseguraba la existencia de los siete niveles de la Internet Oscura. Esto de los niveles es el mayor de los despropósitos. Sin ninguna consistencia ni veracidad. Respecto a la idea del iceberg, la verdad es que es difícil obtener una estimación real del porcentaje que representa la llamada Internet Profunda en el total de la red. Solo se sabe que existe muchísimo contenido y que en la práctica es difícil de cuantificar.

Antes de proseguir, es importante definir adecuadamente los conceptos que estamos introduciendo para aclarar posibles confusiones. Probablemente, te habrás percatado de que a menudo se utilizan indistintamente los conceptos Deep Web (Internet Profunda) y Dark Web (Internet Oscura), aunque en teoría definen ámbitos diferentes de la red.

La Deep Web frente a la Dark Web

Técnicamente, la Deep Web, o Internet Profunda, hace referencia a todo aquello que no puede ser indexado por los motores de búsqueda tradicionales. Esto no tiene por qué implicar sitios donde se desarrollen actividades ilícitas o turbias. Existe un montón de contenido que, por uno u otro motivo, no puede ser indexado. Por ejemplo, páginas dinámicas cuyo contenido está gestionado por bases de datos y depende de los parámetros que se incluyan en un enlace, sitios bloqueados que requieren de un CAPTCHA para poder acceder, o portales que existen, pero no están enlazados en ningún sitio, también portales que requieren de autenticación para poder visualizar contenido, y contenido en otros formatos diferentes a HTML o redes alternativas de acceso limitado.

Al hablar de redes alternativas de acceso limitado, hacemos referencia a recursos y servicios que no pueden ser alcanzados con una configuración de red estándar. Por eso suscitan el interés de actores maliciosos que podrían cometer actividades delictivas sin ser detectados por los agentes de la ley. Esto incluye sitios con nombres de dominio que no fueron registrados en el

sistema de DNS que conocemos, gestionado por la ICANN (Internet Corporation for Assigned Names and Numbers).

Esta clasificación también incluye redes alojadas en infraestructuras que requieren de un *software* específico para acceder a ellas. Es el caso de la popular red TOR, entre otras. No es la única red anónima de este tipo. Existen otras, como Freenet, Invisible Internet Project (I2P) o Hyperboria, que de hecho están creciendo en los últimos años. Estas redes de acceso limitado son llamadas darknets y son, por tanto, las redes que alojan la llamada Dark Web o Internet Oscura. Es decir, la Dark Web no es la Deep Web, sino que es tan solo una parte de ella.

La red TOR

El llamativo nombre de Dark Web o Internet Oscura no significa que todo lo que acontece en ella sea delictivo o ilegal. TOR, la primera de estas darknets, nació precisamente con fines lícitos, Fue creada con el propósito legítimo de proporcionar *software* libre en defensa de la libertad digital, escapar a la censura y garantizar la libertad de expresión, la privacidad y el anonimato. La Dark Web ayudó a movilizar las protestas de la primavera árabe y tuvo que ver en el éxito de Wikileaks. Algunos periodistas utilizan TOR para conectarse en zonas de conflicto sin temor a ser detectados. Muchos usuarios utilizan TOR simplemente para proteger su privacidad a la hora de navegar por la red y no ser rastreados por empresas, operadores o anunciantes. Lo que sucede es que, como ocurre con cualquier herramienta que se precie, su impacto puede cambiar dependiendo de las intenciones de cada usuario. El anonimato que la red TOR proporciona a los usuarios ha hecho que los cibercriminales vean en ella el coto donde desarrollar sus actividades delictivas sin ser detectados o perseguidos por la justicia.

El acrónimo TOR se traduce como The Onion Router, puesto que esta red sigue un sistema de enrutamiento por capas para garantizar el anonimato. Intentaremos explicarlo de modo sencillo sin entrar en demasiados detalles técnicos:

- Cuando un usuario realiza una petición para acceder a una web, su tráfico pasa por varios puntos intermedios que se conocen como nodos hasta llegar a su destino, el servidor final.
- El primer nodo al que el usuario se conecta se conoce como nodo de entrada. Es el único que conoce la dirección IP del usuario.

- A partir de ahí, el nodo de entrada envía el tráfico a un nodo intermedio.
- Cada uno de estos nodos establece una conexión cifrada con el siguiente nodo de la ruta.
- Solo dichos nodos pueden descifrar el contenido del paquete.
- Ninguno de los nodos conoce la ruta completa ni más detalle que el del nodo al que le va a enviar el paquete.
- El último nodo de la ruta, llamado nodo de salida, envía el paquete al servidor de destino.
- De este modo, el servidor de destino no conoce la dirección IP del usuario que hizo la petición, sino la del nodo de salida que es quien le envía el paquete.

Mediante este encaminamiento por capas, como la cebolla, se consigue enrutar el tráfico a través de diferentes nodos para que este no pueda ser rastreado ni monitorizado. La ruta de nodos se reconfigura nuevamente cada cierto tiempo.

Para acceder a esta red se necesita un *software* específico. Hace unos años era un poco más complejo para un usuario medio, pero a día de hoy existen algunos navegadores, como Tor Browser. Está basado en el navegador Firefox y proporciona conexión a esta red de manera sencilla. Simplemente hay que instalarlo y empezar a navegar. Desde él, se puede acceder a sitios web convencionales de internet con dominios estándar, utilizando TOR para navegar con privacidad y anonimato. Y también a sitios específicos alojados en la red TOR que siguen una nomenclatura diferente, basada en dominios «.onion».

Hemos descrito brevemente el funcionamiento de la red para entender cómo consigue TOR anonimizar las comunicaciones de sus usuarios, puesto que es la red más popular y extendida de las que conforman la Dark Web. Otras como Freenet, I2P o Hyperboria cuentan con topologías y funcionamientos diferentes, pero se basan en la misma idea: ser redes anónimas que escapan de la arquitectura de la red convencional para evitar ser monitorizadas.

Silk Road, el mayor mercado negro de narcotráfico que operaba en la Deep Web

El interés de la sociedad por la Deep Web alcanzó su cota máxima en 2013, cuando el FBI desarticuló el mayor mercado ilegal de narcotráfico concebido

hasta la fecha. Hablamos de Silk Road, un mercado negro alojado en la red TOR concebido para la compraventa de drogas y estupefacientes, aunque en él también se anunciaban armas, servicios de *hacking* o falsificaciones, entre otras actividades ilegales.

Su fundador utilizaba el seudónimo Dread Pirate Roberts (un personaje de ficción) para operar Silk Road, amparado en el anonimato que TOR le otorgaba. Creó este mercado negro en 2010 y el sitio estuvo operando en línea durante varios años.

Los usuarios podían acceder a Silk Road a través de TOR mediante una dirección .onion que iba cambiando regularmente. Una vez dentro, el sitio web era simple y fácil de utilizar, similar al de un portal como eBay. El comprador elegía el producto y el vendedor se lo enviaba directamente, sin ninguna intervención de Dread Pirate Roberts. Para dificultar la trazabilidad del dinero, se implementó el uso de bitcoins en las transacciones económicas.

Fue a mediados de 2013 cuando un investigador de la DEA pudo relacionar el alias Dread Pirate Roberts a una persona física, con nombre y apellidos: Ross Ulbricht. Lo hizo por un desliz que este cometió al publicar su dirección personal de correo en un foro que guardaba cierta relación con Silk Road. Las autoridades estadounidenses llevaban tiempo siguiendo este mercado negro, y pese a que era muy complicado estudiar el rastro de los servidores en la Deep Web, investigaron el hilo de las publicaciones que promocionaban Silk Road en la superficie de la red estándar. Gracias a varias pistas, determinaron que Ulbricht era el creador del mercado negro en línea más grande de la historia. Lograron detenerle el 1 de octubre de 2013 en la biblioteca de San Francisco, cuando se hallaba conectado desde su portátil al sitio web de Silk Road. Fue una operación planificada del FBI para capturarlo e incautar su equipo sin darle tiempo a reaccionar. Querían evitar a toda costa que Ulbricht pudiese activar sobre la marcha un mecanismo para borrar toda la información de su equipo, lo cual impediría relacionarle con Silk Road.

Su detención fue muy sonada por la manera en que se produjo y por sacar a la luz las actividades que tienen lugar en los bajos fondos de la red. Desde entonces, la Deep Web y la Dark Web se popularizaron mucho entre quienes no habían oído hablar de ellas.

¿Qué es lo que se puede encontrar en la Deep Web?

Aunque existen motivaciones legítimas para usar la red TOR o el resto de redes anónimas de la Dark Web, es cierto que en ellas se prodiga todo tipo de

contenido ilegal y actividades delictivas. Algunas de las cosas que se pueden encontrar son las siguientes:

- Venta de drogas y de armas.
- Servidores de comando y control de botnets.
- Servidores e infraestructura de troyanos, ransomware y otro tipo de malware.
- Venta de exploits y malware.
- Servicios de «lavado» de bitcoins y también de monedas convencionales.
- Venta de identidades falsas y de cuentas robadas.
- Venta de pasaportes o documentos de identidad falsificados de diferentes países.
- Leaks de información sensible que proviene de gobiernos, agentes de la ley o personajes famosos.
- Foros dedicados a la pedofilia donde se intercambia material.
- Servicios de contratación de sicarios.

No obstante, dada la naturaleza de la Deep Web, encontrar estos contenidos no es algo trivial ni accesible a cualquiera. Muchos de los sitios donde se distribuye material ilegal o se desarrollan actividades delictivas están muy restringidos. Para poder encontrarlos e incluso acceder a ellos se necesitan credenciales o autorización que circulan en grupos de confianza. En algunos casos es complicado determinar la veracidad del contenido o actividad ilegal que se anuncia en cada sitio. De partida, tratar con las personas que se dedican a este tipo de asuntos representa ya un peligro en sí mismo.

Muchos de los portales que cualquiera encuentra nada más aterrizar en TOR o redes alternativas donde se anuncian actividades ilegales generalmente son intentos de fraude para estafar a usuarios sin conocimiento ni experiencia. En vez de venta de armas, pasaportes, drogas, tarjetas de crédito o identidades robadas, en realidad se desarrolla un tipo de actividad delictiva mucho más clásica: ciberdelincuentes que estafan a usuarios mediante ingeniería social.

Además de las actividades ilícitas que llaman más la atención, también existen un montón de sitios alojados en redes anónimas de la Dark Web dedicados a temas más mundanos: blogs personales o políticos, sitios de noticias, foros de discusión de temas varios, sitios religiosos y hasta emisoras de radio clandestinas.

¿Es totalmente anónima la Dark Web?

Obviamente, la utilización de la Dark Web para intercambiar material ilegal y realizar acciones delictivas se ha convertido durante años en objetivo principal de la inspección y el espionaje de gobiernos, agencias de inteligencia y otros actores. El control de la información es un asunto crítico para detectar y prevenir cualquier amenaza que pueda comprometer la seguridad de empresas, organizaciones o países. Es por eso que estas entidades han puesto el foco en intentar romper el anonimato de la red TOR. En el mundo de internet y de la ciberseguridad, como en cualquier aspecto de la vida, no hay nada ciento por ciento seguro.

Como hemos comprobado, el *hacking* consiste en la búsqueda de diferentes aproximaciones hasta lograr el objetivo. Una de ellas se basa en disponer de un alto número de nodos controlados en redes como TOR. La red TOR funciona de manera distribuida repartiendo el tráfico entre nodos de entrada, intermedios y de salida. Cualquiera que tenga interés puede montar un nuevo nodo. Se ha demostrado que, si alguien cuenta con un número elevado de nodos de la red, podría realizar «ataques estadísticos» monitorizando el tráfico de los nodos para correlacionar paquetes. En términos simplificados, aunque el tráfico vaya cifrado al pasar por diferentes nodos, si se identifican patrones en los paquetes en los nodos de entrada y de salida, sería posible reconocer el tráfico de un usuario. Por otra parte, si cada uno de estos nodos controlados incluye en los paquetes enviados una especie de señal, puede rastrearse para trazar la ruta completa del paquete. Se calcula que si se captura el tráfico de los nodos durante varios meses y se hacen análisis estadísticos de las señales, se podrían conocer las rutas que siguen los paquetes, los servidores por los que pasan y dónde se encuentran localizados para el 80 por ciento del tráfico. Es cuestión de tiempo que la ruta de nodos de un usuario involucre los controlados por el atacante. Esto requiere disponer de una infraestructura muy grande de nodos desplegados, y los gobiernos y sus agencias cuentan con recursos suficientes para desplegarlas.

En los últimos años, quienes están detrás del proyecto TOR han confirmado que el anonimato de esta red se ha roto durante determinados períodos concretos debido a ataques estadísticos.

Además de estos ataques estadísticos, como siempre existen otras vías para romper la seguridad de la red TOR y otras análogas. En muchos casos, esto pasa por la explotación de vulnerabilidades que puedan existir en el propio *software* manejado por los usuarios para conectarse a TOR. En el pasado ya se identificaron diversas vulnerabilidades en este sentido, que exponían la identidad de los usuarios. A finales de 2016, se supo que el FBI

había explotado una vulnerabilidad Zero Day en el navegador Tor Browser para comprometer la seguridad de miles de usuarios y desarticular un conocido sitio de pornografía infantil llamado Playpen. El sitio fue creado en TOR en agosto de 2014. Cuando el FBI logró desmantelarlo en febrero de 2015 en una operación llamada «Operation Pacifier», el portal tenía 215 000 usuarios y almacenaba 23 000 imágenes y vídeos de contenido pedófilo. La operación concluyó con el arresto de 900 usuarios del portal.

Lo que queda claro es que a día de hoy la privacidad de las comunicaciones en internet no es algo sencillo de conseguir. Las redes anónimas como TOR, Freenet, Hyperboria o I2P pueden proporcionarnos una sensación de anonimato que no siempre se ajusta a la realidad. Es cierto que aportan un nivel de privacidad y anonimato mayor que el que se obtiene navegando por los medios convencionales, pero en ningún caso lo garantizan totalmente. Desde el punto de vista de la lucha contra la ciberdelincuencia, supone una noticia positiva.

Posiblemente como usuario o responsable de una empresa no hayas accedido nunca a la Deep Web, ni tengas la necesidad de hacerlo. Es posible, sin embargo, que en el futuro quieras utilizar la red TOR para navegar con mayor privacidad y sin ser monitorizado. Sea como sea, ahí van una serie de recomendaciones:

- Si quieres utilizar TOR para navegar de forma anónima, utiliza un equipo dedicado o una máquina virtual.
- Mantén actualizado tu sistema operativo con todos los parches de seguridad, así como la última versión del resto de programas.
- Descárgate siempre la última versión del *software* que utilices para acceder.
- Extrema la precaución a la hora de navegar.
- Recuerda que gran parte de los sitios web son fraudulentos y simplemente buscan comprometer tu seguridad.
- No intentes acceder a sitios donde se promociona, distribuye o desarrollan actividades delictivas para satisfacer tu curiosidad. Podrías acabar siendo detenido por ello.
- Nunca pienses que eres totalmente anónimo por utilizar TOR u otras redes anónimas.

1

El Internet de las Cosas y el futuro que nos depara

La sociedad digital en la que estamos inmersos crece continuamente y lo hace a un ritmo vertiginoso. Además de ordenadores y *smartphones*, manejamos un sinfín de nuevos dispositivos tecnológicos inteligentes que los fabricantes incorporan cada día al mercado: asistentes virtuales como Alexa, robots que limpian nuestra casa como la Roomba, pulseras de actividad física que monitorizan el ritmo cardíaco… Son tantos los gadgets que se cuelan en nuestra vida diaria que se hace ya imposible para cualquier usuario estar al tanto de todas las novedades.

Los aparatos electrónicos tradicionales, como televisores, frigoríficos, tostadoras o cepillos de dientes también están evolucionando y haciéndose inteligentes. Principalmente, porque ahora incorporan nuevas funcionalidades relacionadas con la conectividad y la interacción con otros servicios. Aportan valor al producto, facilitan la vida al usuario y, en última instancia, los hacen más atractivos. Es el caso de las smart TV. Otros «avances» resultan más cuestionables. Las versiones inteligentes del clásico cepillo eléctrico incorporan Bluetooth y, mediante una aplicación en el móvil, el usuario puede conocer parámetros de su proceso de cepillado, como el tiempo que invierte en la tarea. Es posible que algún usuario que le dé una gran importancia a la optimización del tiempo vea en esto una ventaja. Yo en particular, no se la veo.

Independientemente de si aportan mayor o menor valor, todos estos dispositivos forman parte de lo que se conoce como el Internet of Things o Internet de las Cosas. El concepto engloba cualquier aparato que esté conectado a internet.

Como es evidente, estos dispositivos que incorporan tecnología y conectividad son susceptibles de tener vulnerabilidades y de representar un

peligro para la seguridad de los usuarios. De ahí que sea importante que las funcionalidades o capacidades de los nuevos productos tengan utilidad práctica real. Cuantas más funcionalidades, conectividad y servicios existan, más puntos de exposición habrá y más probabilidades de que alguno de ellos sea vulnerable. Máxime, cuando los productos se lanzan al mercado con unos plazos de desarrollo ajustadísimos para adelantarse a la competencia.

Vulnerabilidades en vehículos conectados y marcapasos

A lo largo de los últimos años, muchos *hackers* han investigado la seguridad de diferentes dispositivos del Internet de la Cosas y han encontrado vulnerabilidades en muchos de ellos. Desde algunos tan aparentemente inofensivos como muñecas inteligentes, hasta otros tan complejos como los últimos vehículos conectados.

Es conocido el vídeo de Charlie Miller y Chris Valasek hackeando en remoto un Jeep Cherokee que intentaba conducir un reconocido periodista de la revista Wired. Estos brillantes investigadores demostraron el impacto que pueden tener las vulnerabilidades en un vehículo. Descubrieron fallos en el Cherokee que les permitieron tomar el control remoto de varios elementos del vehículo, como la radio o el aire acondicionado, tranquilamente sentados en el sofá de su casa. Además, neutralizaron los pedales de forma que el conductor no pudiese frenar o acelerar por su cuenta. Reportaron sus hallazgos a Jeep, que tuvo que corregir las vulnerabilidades en casi un millón y medio de vehículos. Al año siguiente, Miller y Valasek encontraron nuevas vulnerabilidades aún más peligrosas en el mismo modelo: aceleraciones involuntarias, frenazos bruscos o giros de volante a cualquier velocidad. Errores que podían costar vidas humanas. En ambas ocasiones, contaron al mundo los resultados de su impactante investigación en DEFCON que, junto con BlackHat, es una de las conferencias más importantes de *hackers* a nivel mundial. Las dos se celebran anualmente en Las Vegas, con una semana de diferencia.

Precisamente en la edición de 2013 de BlackHat tuvo lugar uno de los sucesos más escalofriantes relacionados con el tema de las investigaciones acerca de dispositivos conectados. Barnaby Jack, un reconocido *hacker*, «fue encontrado muerto» en su apartamento de San Francisco, días antes de su conferencia en BlackHat. Falleció de manera repentina días antes de revelar al mundo los resultados de su última investigación. Había encontrado vulnerabilidades que permitían manipular en remoto, de forma inalámbrica,

marcapasos y otros implantes médicos. Las especulaciones acerca de su trágica muerte no se hicieron esperar. Quizá alguien no quería que Barnaby Jack revelara al mundo cómo *hackear* un marcapasos. Curiosamente, meses después se supo que el exvicepresidente de Estados Unidos Dick Cheney llevaba un marcapasos del mismo modelo que había comprometido el *hacker*. Cheney había decidido quitarle todas las opciones de conexión remota a su marcapasos por seguridad. Para añadir más surrealismo a esta historia, en un capítulo de la popular serie Homeland, que en aquel entonces ya había sido emitido, casualmente asesinaban al vicepresidente de los Estados Unidos hackeando en remoto su marcapasos. Cuando menos resulta curioso.

La curiosa historia de las mesas de mezclas Pioneer

Además de vehículos o marcapasos, son muchos los dispositivos del Internet de las Cosas a los que se les han diagnosticado problemas de seguridad: televisores, aparatos vigilabebés y hasta rifles inteligentes. Yo mismo descubrí en 2016 una serie de vulnerabilidades que afectaban a diversos modelos de mesas de mezclas Pioneer. La multinacional japonesa es el fabricante líder en el sector de productos profesionales para artistas y *disc-jockeys*. En los mejores espectáculos y salas de fiesta de todo el mundo, los equipos que se utilizan son Pioneer. En principio, a nadie se le ocurriría que una mesa de mezclas pudiese ser hackeada, ni que formara parte del Internet de las Cosas. Las mesas de mezclas Pioneer pueden ser controladas mediante una aplicación móvil llamada Rekordox, desarrollada por el propio fabricante. Desde ella es posible transferir música a la mesa de mezclas y manipular algunos parámetros de la reproducción. La conexión se establece mediante una red *wifi* que genera la propia mesa, aunque también puede configurarse con cualquier otra red *wifi*.

Junto con el *hacking*, la música es otra de mis grandes pasiones. Toco el órgano desde pequeño y siempre me ha gustado mezclar música, aunque hace ya muchos años que dejé de practicar. A mediados de 2015, decidí hacerme con uno de estos nuevos modelos de Pioneer para retomar mi afición en los pocos ratos libres que tenía. Al ver las funcionalidades que ofrecía mediante Rekordbox, no tardé en empezar a destripar su funcionamiento. Tras investigar el protocolo de comunicación entre la mesa de mezclas y la aplicación móvil, descubrí una serie de vulnerabilidades que me permitían varias cosas. La primera de ellas era robar la información de la pista musical que se estaba reproduciendo y también el fichero de audio de la propia pista.

Esto podría suponer un peligro para artistas que pinchan sus temas exclusivos antes de haberlos lanzado al mercado.

Además, era posible realizar otro tipo de ataques para confundir al dj, enviándole a la aplicación información falsa sobre el estado de los reproductores. Pero sin duda alguna, la vulnerabilidad más importante me permitía parar en directo la sesión del *disc-jockey* simulando la transferencia de una nueva pista musical desde la aplicación móvil. Es decir, que podía detener en seco su actuación simplemente enviándole un paquete desde mi equipo. Imaginemos lo que sucedería en una macrofiesta con miles de personas bailando al son de las mezclas.

Aunque no tiene el mismo impacto que las vulnerabilidades en un vehículo o en un marcapasos, el caso Pioneer es útil para subrayar que cualquier dispositivo tecnológico es susceptible de presentar vulnerabilidades.

El futuro de nuestra sociedad digital

La tecnología está cambiando nuestras vidas. Nos permite vivir una sociedad digital que evoluciona constantemente. Cada vez serán más los dispositivos conectados en nuestro día a día. Sectores como el e-health están en auge y expansión. Todo este progreso sin duda alguna nos brinda muchas ventajas, avances que hace apenas un lustro o una década eran inaccesibles o casi impensables. Pero no debemos olvidar que también implican un riesgo para nuestra seguridad. Los fabricantes deben hacer un esfuerzo para desarrollar tecnologías más seguras, en configuraciones por defecto, sin delegar en los usuarios la responsabilidad de garantizar la seguridad de sus datos o dispositivos.

Lograr este objetivo no es tarea sencilla. Hemos realizado un recorrido completo por este entramado de la seguridad en internet: hemos abordado desde la base todo lo que puede suponer un riesgo para usuarios y organizaciones; hemos intentado entender por qué se producen los ataques; hemos introducido conceptos como los de vulnerabilidad y exploit, y hemos identificado los peligros que entraña la ingeniería social o el arte del engaño para los usuarios. Son muchas las amenazas a las que estamos expuestos. Cuanto más responsables seamos a la hora de manejar e interactuar con la tecnología, más seguros podremos estar. Sin embargo, cuando hablamos de tecnología, nunca podemos estar totalmente seguros. Lo que hoy es seguro, mañana puede no serlo. Mientras la tecnología esté desarrollada por humanos, será falible.

Mientras tanto, como hemos ido apuntando en cada capítulo, existen una serie de medidas de seguridad y buenas prácticas que nos ayudarán a evitar gran parte de los problemas. Si tomamos conciencia de todas estas directrices y las aplicamos en nuestro día a día, podremos lograr un nivel de seguridad confiable para vivir más tranquilos en la red.

Muchísimas gracias por llegar hasta aquí y espero que este breve pero apasionante viaje por el ciberespacio te haya resultado provechoso. Recuerda que los *hackers* son los buenos, y los ciberdelincuentes, los malos; que nadie te da o te quita el título de *hacker*; que al final, se trata de una actitud, de explorar e investigar constantemente para desafiar los límites de la tecnología o de cualquier ámbito de nuestra existencia; que tú puedes ser un *hacker* de la tecnología, de la economía, de la medicina, del derecho… pero sobre todo, que puedes ser un *hacker* de tu propia vida. Disfruta siempre con lo que hagas, sea lo que sea. Y no ceses en la búsqueda del conocimiento. Nunca. Porque el día que dejes de hacerlo, nada tendrá sentido.

Happy Hacking. Nos vemos en la red.

Decálogo de buenas prácticas

A lo largo de este libro, hemos ido recogiendo las diferentes recomendaciones o medidas cuando abordamos cada problemática o amenaza concreta, tanto desde la perspectiva de un usuario como desde la del responsable de una organización. Algunas son comunes y otras son específicas para cada caso. Puedes consultarlas con detenimiento cada vez que tengas dudas al respecto. En cualquier caso, aquí tienes una recapitulación de las directrices que hemos ido apuntando, un decálogo de buenas prácticas que te ayudará como usuario a navegar más seguro en la red.

1. Mantén siempre actualizado tu sistema operativo con todos los parches de seguridad instalados. Es lo que te protegerá frente a las últimas vulnerabilidades.
2. Asegúrate de tener actualizados todos los programas que tengas instalados en el equipo o dispositivo móvil a la última versión.
3. Utiliza un antivirus comercial de reputación y prestigio contrastados que se actualice constantemente con las firmas del malware que se van identificando.
4. Utiliza contraseñas robustas, que no incluyan palabras reconocibles. Deben tener una longitud considerable, entre ocho y diez dígitos, e incluir mayúsculas, minúsculas y símbolos especiales siempre que sea posible. Modifícalas frecuentemente y no utilices la misma contraseña para diferentes servicios.
5. No hagas clic en enlaces que te envíen por correo electrónico, sistemas de mensajería o redes sociales. Es preferible abrir el navegador y teclear la dirección para saber que estamos yendo al sitio web original en lugar de a una página maliciosa de *phishing*. Igualmente, no abras archivos adjuntos que vengan en correos electrónicos que no esperas.
6. Extrema la precaución a la hora de navegar en redes *wifi* públicas de hoteles, cafeterías, aeropuertos y lugares por el estilo. Si vas a usar

servicios personales como correo electrónico, redes sociales o aplicaciones corporativas, implementa o contrata una VPN.
7. No descargues *software* comercial crackeado en internet para ahorrar en costes. La mayoría de esos programas de pago que se ponen a disposición de los usuarios de forma gratuita incluyen malware.
8. Modifica las contraseñas por defecto de todas las aplicaciones y dispositivos que utilices: routers, puntos de acceso, cámaras IP… Actualiza también el firmware de todos estos dispositivos.
9. Controla la información que expones sobre ti en la red y configura adecuadamente las opciones de privacidad de redes sociales, aplicaciones y dispositivos. Recuerda que cuanta más información expones, más facilidades le das a cualquiera que se proponga comprometer tu seguridad.
10. Por norma desconfía siempre de cualquier actividad sospechosa y de correos o comunicaciones no esperadas, incluso aunque procedan de remitentes conocidos. También de cualquier oferta o ganga que puedas encontrar en la red. Recuerda el concepto de ingeniería social y las técnicas utilizadas por los ciberdelincuentes para comprometer nuestra seguridad. Contrasta siempre la información por canales o vías alternativas.

Del mismo modo, hemos establecido orientaciones básicas desde el punto de vista del responsable de una empresa o directivo. Lo sintetizamos aquí con un decálogo para gestionar correctamente la seguridad de tu organización:

1. Establece políticas de seguridad y directrices claras en la organización para que los trabajadores conozcan las medidas de seguridad que deben adoptar en su desempeño diario.
2. Asegúrate de que el sistema operativo y el *software* de los equipos de todos los usuarios se mantiene siempre actualizado.
3. Además de establecerlo en las políticas, habilita medidas para obligar a los usuarios a utilizar contraseñas robustas, con requisitos mínimos de longitud y complejidad, así como a modificarlas en el plazo que establezcas. No hagas excepciones para ningún usuario de la organización, por muy alto que esté en la cadena de mando.
4. Habilita o contrata soluciones de VPN para que los trabajadores de la organización que requieran de movilidad puedan conectarse desde el exterior con seguridad.
5. Realiza auditorías de seguridad periódicas sobre los activos tecnológicos de la organización para identificar y mitigar vulnerabilidades en sistemas o aplicativos.

6. Implementa un plan de respuesta a incidentes acorde al tamaño de la organización. Tanto si se trata de una pequeña empresa como de una gran multinacional, necesitas tener previsto un protocolo de actuación ante cualquier tipo de incidente.
7. Realiza acciones formativas para los trabajadores de la organización, tanto a través de cursos como mediante sesiones de concienciación impartidas por expertos en la materia, donde les expongan de manera práctica los peligros a los que se pueden enfrentar. Es fundamental formar a los usuarios y concienciarlos para que asimilen medidas de seguridad imprescindibles en el ámbito corporativo, pero también en el personal.
8. Planifica campañas de *phishing* o *vishing* contra los trabajadores para evaluar el nivel de resiliencia que tiene la organización ante ataques de ingeniería social.
9. Dedica esfuerzos y recursos a monitorizar el tráfico de la red interna, así como los registros de los servidores y aplicativos en busca de cualquier actividad sospechosa.
10. Recuerda que la ciberseguridad es una disciplina muy compleja que requiere de un alto grado de especialización, conocimiento y dedicación. El administrador de sistemas o responsable TIC generalmente no puede abarcar todas estas capacidades. Aunque en algunos casos podrá encargarse de gestionar la seguridad, debe apoyarse en profesionales o empresas externas para realizar auditorías, preparar respuestas a incidentes, promover campañas de concienciación o cualquier otra actuación que requiera de un conocimiento experto en la materia.

Agradecimientos

No me gustaría concluir este libro sin agradecer a todas las personas que me han ayudado a llegar hasta aquí. A los referentes que me inspiraron para perseguir mi sueño de dedicarme al *hacking* y a la ciberseguridad. A los mentores que tantas veces me han asesorado y guiado en el camino. También a los profesionales que me dieron la oportunidad de colaborar con ellos y ayudarme a crecer. Gracias a mi familia, compañeros y amigos que durante años me han apoyado, aguantado, escuchado mis dudas, problemas o delirios. A las personas especiales que desde que llegaron a mi vida siempre han estado a mi lado, en la luz o en la sombra, dejando una huella imborrable en mí. Sería imposible citarlos a todos. Estoy seguro de que al leerme sabrán quiénes son. Sin la ayuda de todos y cada uno de ellos no habría sido posible ni tendría sentido.

Por último, muchas gracias a todos los que estáis siempre al otro lado, leyendo mis publicaciones, interesados en mis conferencias, dedicándome siempre buenas palabras y muestras de cariño que tanto se agradecen cuando faltan fuerzas. Este libro lo he escrito yo, pero es también vuestro. Muchísimas gracias de verdad.

Deepak Daswani (Tenerife, España) es ingeniero superior en Informática por la Universidad de La Laguna, y experto en ciberseguridad. En la actualidad trabaja como profesional independiente, prestando servicios relacionados con la ciberseguridad a empresas y organismos. Con anterioridad, desarrolló su carrera en el sector de las TIC en Canarias, en empresas como CajaCanarias o GRAFCAN, ocupó el cargo de Security Evangelist en el Instituto Nacional de Ciberseguridad (INCIBE) y el de Experto en Ciberseguridad para la firma multinacional Deloitte. Es uno de los *hackers* más reconocidos de nuestro país. Participa habitualmente como conferenciante y docente en los Congresos de Ciberseguridad más importantes a nivel internacional, en escuelas de negocio, másters universitarios, formaciones y sesiones para empresas, conferencias de *hackers* o eventos como las charlas TED. Asimismo, sostiene una amplia labor de divulgación y concienciación en diversos medios de comunicación de prensa, radio y televisión (TVE, cadena SER, Antena 3, La Sexta, CNN, Telemundo Washington) y en TVE2.