Piratería informática y ciberintrusión

PID_00270253

Thomas Holt

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Thomas Holt

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Marc Balcells Magrans (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

Cuando se pregunta al público en general sobre los delitos cibernéticos, se suele señalar a los piratas informáticos como los causantes de tales infracciones (Furnell, 2002). Esto puede deberse a las muchas décadas de cobertura mediática que vinculan a los *hackers* con toda una serie de ataques altamente técnicos contra Gobiernos, corporaciones e instituciones financieras. Los *hackers*, además, ocupan un lugar destacado en los medios de comunicación populares como expertos en todo tipo de tecnología, una figura que va desde Neo en la trilogía de *Matrix* hasta el personaje de Nine-ball en *Ocean's 8*. Estas representaciones contradicen la realidad del hackeo, una habilidad que no solo se relaciona con los ataques a redes informáticas, sino también con la protección de esos mismos ataques. Asimismo, no todos los *hackers* son técnicamente competentes, pero sí pueden encontrar formas más fáciles de obtener acceso a un sistema informático (Ponemon Institute, 2018).

Existe una cobertura similar en los medios acerca de las amenazas que representa el *malware* o el software malicioso, que también se atribuye a piratas informáticos (Brenner, 2011; Schell y Dodge, 2002; Wall, 2007). El uso de *malware* está asociado a ataques de sistemas informáticos, al robo de información confidencial, al correo no deseado y a diversas formas de cibercrimen (Holt, 2013; Symantec, 2018; Szor, 2005). No está claro hasta qué punto el público general comprende el alcance del *malware* que fluye a través de internet en cualquier momento o cómo funcionan estas herramientas de ataque.

Este módulo proporcionará una descripción general de las características del hackeo y de la relación entre *hackers*, software malicioso y tecnología en general. Se explorarán las características de los piratas informáticos y sus objetivos, al igual que el vínculo entre piratería y *malware* que permite los delitos informáticos económicos. Asimismo, se tratará la evolución histórica de la tecnología junto con las prácticas de los piratas informáticos y el *malware* para comprender el panorama actual de los ciberdelitos económicos asociados con los actos de ciberintrusión.

1. Definición de hackeo

Uno de los mayores desafíos para los investigadores radica en definir qué constituye piratería, ya que esta definición no es necesariamente coherente entre distintas poblaciones. La definición más amplia de piratería reconoce en ella la manipulación o modificación de tecnología de cualquier tipo, ya afecte al hardware o al software, para que pueda usarse de una manera distinta a la de su propósito inicial (Holt, 2007; Levy, 2001; Schell y Dodge, 2002; Steinmetz, 2015; Turkle, 1984). Un acto de piratería se puede llevar a cabo con fines legítimos o ilegítimos, aunque se utilicen las mismas técnicas, independientemente de la motivación del atacante.

> Por ejemplo, alterar el hardware de una computadora para que funcione a una mayor velocidad de procesamiento sería un ejemplo de hackeo legal. Sin embargo, este acto puede infringir el acuerdo de usuario o la garantía proporcionada por el fabricante (Kravets, 2010).

Los actos de piratería que modifican una aplicación para conseguir subrepticiamente los datos del usuario y reenviarlos a una dirección de correo electrónico o servidor web, o para subvertir los protocolos de seguridad, son ilegales, en gran medida porque no hacen sino conseguir información sin el consentimiento del usuario (Brenner, 2008; Holt, 2007; Schell y Dodge, 2002).

Los *hackers*, no obstante, no solo se centran en la tecnología, sino que también traman formas de obtener la información de distintos grupos de usuarios con éxito. Los empleados de las principales empresas y organizaciones tienen acceso de raíz a sistemas e información confidenciales que suelen estar protegidos solo mediante un nombre de usuario y una contraseña. A menudo, estos datos se pueden adquirir a través de los usuarios sin la necesidad de métodos de piratería técnicamente sofisticados. En cambio, los piratas informáticos pueden utilizar diversas formas de fraude y tergiversación para obtener información sobre su víctima. Los *hackers* generalmente se refieren a estos métodos como de ingeniería social, ya que intentan manipular a un individuo mediante el uso de la comunicación social y de la manipulación psicológica para engañarlos y obtener sin coacción datos que se pueden utilizar para acceder a diferentes recursos (Furnell, 2002; Huang y Brockman, 2010; Mitnick y Simon, 2002).

Ved también

Para más ejemplos, consultad los módulos 3 y 4.

Un *hacker* puede utilizar llamadas telefónicas, correos electrónicos o sitios web para falsificar su identidad y solicitar información de objetivos vulnerables dentro de estas organizaciones. Estos métodos son con frecuencia efectivos, ya que los humanos suelen ser incapaces de reconocer todas las formas en que pueden ser manipulados, y son más difíciles de proteger del riesgo en comparación con los sistemas informáticos o edificios (Huang y Brockman, 2010; Mitnick y Simon, 2002).

Independientemente de si un *hacker* desea atacar a una persona, un programa informático o un dispositivo, utilizará un conjunto único de términos para describir el proceso. En concreto, los piratas informáticos intentan identificar defectos o errores en un dispositivo o en una psique humana fácilmente manipulable, a lo que se refieren como *vulnerabilidades* (Furnell, 2002; Taylor, 1999). Existen vulnerabilidades en prácticamente todas las piezas de hardware y software que existen, con independencia del fabricante (Wang, 2006). Esto también sirve respecto al modo en que las personas piensan y actúan en respuesta a ciertas señales visuales y auditivas, lo que puede aumentar la probabilidad de que cumplamos una solicitud de información (Huang y Brockman, 2010; Mitnick y Simon, 2002). Por lo tanto, los *hackers* en general intentan identificar el mayor número de vulnerabilidades posible al inicio de un hackeo para aumentar su probabilidad de éxito.

Después de identificar las vulnerabilidades que están presentes en su objetivo, los piratas informáticos deben seleccionar una vulnerabilidad específica y encontrar la manera de atacarla. En el contexto de la tecnología informática, esto implica por lo general el uso de un programa informático llamado *exploit*, que puede afectar a tal vulnerabilidad (Furnell, 2002; Taylor, 1999; Wang, 2006).

Un *exploit* es un mero *script* de código informático que aprovecha las limitaciones o errores en el software o hardware para obtener un mayor acceso al sistema (Furnell, 2002).

Dada la gran variedad de vulnerabilidades que existen, hay innumerables *exploits* que han sido previamente escritos y que se pueden descargar de foros de *hackers*, sitios de seguridad o incluso comprar a proveedores en mercados negros virtuales (Chu, Holt y Ahn, 2010). Si un pirata informático es capaz de identificar una vulnerabilidad previamente desconocida o de día cero, ha de crear su propio código de explotación, lo que requiere una gran competencia técnica. Así, este tipo de piratería es vista como una grave amenaza por parte de los profesionales de seguridad.

El uso de vulnerabilidades y *exploits* puede ser complicado, por lo que los piratas informáticos a menudo encuentran formas de simplificar y automatizar su uso en ataques. Uno de los métodos clave para lograr esto es a través del uso de programas que automatizan la ejecución de código de explotación y comandos posteriores al sistema (Nazario, 2003; Szor, 2005).

La terminología común utilizada para describir estas herramientas es *software malicioso* o *malware*, ya que combinan múltiples *exploits*, *scripts* y rutinas en un solo paquete, que automatiza los ataques.

El *malware* generalmente funciona lanzando un *exploit* contra una vulnerabilidad para influir en el objetivo informático a través de la ejecución de una carga útil o un conjunto de códigos que afectan a los procesos del sistema informático (Symantec, 2018; Szor, 2005). La víctima debe interactuar con el programa de alguna manera para activar la carga útil, ya sea ejecutando un programa o haciendo clic en un enlace o aplicación (Dunham, 2008). Una vez activado, el *malware* puede eliminar o cambiar los archivos del sistema, copiar documentos y archivos y enviarlos a una ubicación fuera del sistema informático, recopilar pulsaciones de teclas e información introducida por el usuario, así como cambiar los procesos del sistema para alterar las operaciones generales del ordenador (Dunham, 2008; Szor, 2005).

La naturaleza interconectada de las redes informáticas modernas y los dispositivos con acceso a internet también permiten que las infecciones de *malware* se propaguen por todo el mundo conforme se mueven de un dispositivo a otro (Brenner, 2008; Leyden, 2012).

Hay varias formas comunes de *malware* utilizadas por los piratas informáticos y los atacantes para afectar a las víctimas:

1) Una de las formas más frecuentes son los virus, que pueden ocultar su presencia en los sistemas y redes de ordenadores, pero no son autónomos, lo que significa que requieren algún tipo de interacción con el usuario para activar su carga útil. Por ello, los virus generalmente se propagan a través de archivos adjuntos de correo electrónico y mensajería instantánea, así como mediante archivos descargables que la víctima intenta abrir (Kapersky 2003; Symantec, 2018).

2) Otra forma de *malware* no autónomo son los programas de troyanos, que también llegan por correo electrónico como un archivo descargable o adjunto que la gente está dispuesta a abrir: fotos, vídeos o documentos con títulos engañosos como «XXX Porno» o «Recibo de compra». Cuando se abre el archivo, se ejecuta algún tipo de código malicioso (Furnell 2002; Szor, 2005). En algunos casos, los virus y los troyanos pueden activarse visitando sitios web, sobre todo páginas pornográficas, que aprovechan defectos en los navegadores web (Symantec, 2018; Szor, 2005).

3) Otro tipo de *malware* utilizado por *hackers* son los gusanos, que no implican tanta interacción del usuario, dado que son autónomos o capaces de autogenerarse (Nazario, 2003). Los gusanos no necesariamente poseen una carga útil en el mismo sentido que un virus o un troyano, y generalmente funcionan insertando su código en la memoria del ordenador para luego usar cualquier medio disponible y propagarse a otros sistemas informáticos en la propia red (Nazario, 2003). Como resultado, los gusanos pueden hacer que los ordenado-

res se ralenticen considerablemente debido a la falta de memoria disponible y que reduzcan la velocidad de internet disponible, pues los gusanos ocupan ancho de banda al intentar propagarse (Nazario, 2003).

4) Una cuarta forma de *malware* se denomina *amenaza combinada*, ya que combina las funcionalidades de los virus, los gusanos y los troyanos en un solo paquete de código malicioso, que se puede ejecutar contra un objetivo (Symantec, 2018).

> Uno de los mejores ejemplos de amenaza de *malware* combinado reciente es el *ransomware*, que actúa como un troyano en el sentido de que se propaga a través de archivos infectados adjuntos a correos electrónicos o archivos descargables. Si un usuario abre el archivo, el código malicioso se ejecuta y su carga útil se activa como un virus, insertando un software de cifrado en el sistema para proteger todos los archivos con una contraseña y una clave de descifrado. En algunos casos, el *malware* también puede modificar archivos clave del sistema para que los usuarios no puedan acceder a archivos críticos independientemente del cifrado (Russinovich, 2013). Sin embargo, esta información está oculta para el usuario, por lo que no puede acceder a ninguno de los contenidos. Luego, se alerta al usuario sobre la infección y se le dice que no podrá acceder a sus archivos hasta que pague al atacante una tarifa, o rescate, para descifrar dichos archivos (Russinovich, 2013). Los datos sugieren que muchas víctimas pagan el rescate para minimizar el impacto de la infección en sus redes y funcionalidad (IBM, 2016). El coste de estos rescates es variable, aunque las grandes organizaciones han pagado miles de dólares para poder recuperar el acceso a sus archivos (IBM, 2016). Por lo tanto, el *ransomware* supone un gran impacto económico para las víctimas.

En conjunto, la piratería y el *malware* están intrínsecamente vinculados, pues los *hackers* pueden crear y usar estas herramientas para otros ataques. No obstante, el grado de conocimiento requerido para crear *malware* significa que no todos ellos pueden crear o usar *malware* (Holt, Burruss y Bossler, 2018; Leukfeldt y otros, 2017). Además, no todos los *hackers* usarán *malware*, ya que pueden creer innecesaria la culminación de un hackeo. Los profesionales de seguridad también pueden escribir o usar *malware* en el curso de su trabajo para ver si la herramienta puede poner en riesgo la seguridad de sus sistemas con efectividad (Schell y Dodge, 2002). En cualquier caso, el *malware* y los *hackers* constituyen una gran amenaza para los sistemas informáticos y la información privada en general.

2. Motivaciones del *hacker*

Uno de los factores más importantes que debe tenerse en cuenta en cualquier discusión sobre ciberdelincuentes, especialmente sobre piratas informáticos, es su motivación para atacar. Una de las discusiones más citadas sugiere que hay seis motivaciones clave en la comunidad de *hackers* (Holt y Kilger, 2012; Kilger, 2010):

- dinero
- entretenimiento
- ego
- causas ideológicas
- pertenencia a un grupo social y estatus

Las motivaciones pueden variar según el tiempo y el lugar, de manera que lo que es una fuerza impulsora en un país puede estar ausente en otro. Además, los cambios radicales en la tecnología en las últimas tres décadas han cambiado también la relevancia de ciertos motivos a lo largo del tiempo (Kilger, 2010). Por último, debe tenerse en cuenta que un individuo puede estar motivado por múltiples factores en cualquier momento dado, por lo que es difícil identificar un único motivo subyacente a la participación en un ciberataque (Kilger, 2010).

El **dinero** es una motivación importante en la comunidad moderna de *hackers* y atacantes. En la década de los ochenta, el dinero tenía inicialmente poco valor entre los piratas informáticos, ya que el volumen de información digital y materiales disponibles era limitado (Kilger, 2010; Levy, 2001). Nuestra mayor dependencia con respecto a los recursos tecnológicos desde el desarrollo de la World Wide Web ha aumentado considerablemente la cantidad de información financiera y confidencial que ahora está disponible en línea (Franklin, Paxson, Perrig y Savage, 2007; Holt, 2013; Holt y Lampke, 2010; Newman y Clarke, 2003). Como consecuencia, los *hackers* se dirigen con frecuencia a clientes e instituciones financieras mediante ataques de *phishing* (Huang y Brockman, 2010; James, 2005), *malware* de *keylogging* (Chu y otros, 2010; Heron, 2007) y correos electrónicos no deseados (Holt y Graves, 2007; King y Thomas 2009; Wall, 2004). A su vez, los datos adquiridos a través de diferentes formas de ataque pueden ser vendidos por *hackers* en mercados abiertos y así generar ganancias (Chu y otros, 2010; Franklin y otros, 2007; Holt y Lampke, 2010). Además, un número cada vez mayor de creadores de *malware* y *hackers* venden acceso a herramientas y servicios de cibercrimen como la distribución de *spam* y ataques de denegación de servicio que van más allá de las habilida-

des de los *hackers* en ciernes (Chu y otros, 2010; Holt, 2011; Holt, 2013). Esto permite que aquellos agentes cualificados se beneficien de sus habilidades a un tiempo que aumenta la eficacia general de toda la comunidad de *hackers*.

El **entretenimiento** es una motivación que ha seguido siendo importante entre los *hackers* desde la aparición de la tecnología informática (Holt, 2007; Kilger, 2010; Steinmetz, 2016). En los años setenta y ochenta, los *hackers* usaban frecuentemente técnicas de piratería para explorar sistemas telefónicos, lo que condujo a la creación de ciertos recursos de interés, como las tecnologías *blue box*, que podían manipular los sistemas telefónicos al producir los tonos de alta frecuencia que controlan los sistemas de conmutación telefónica (Furnell, 2002). Los *hackers* modernos aún desean manipular la tecnología con fines lúdicos, tal y como se señaló en conferencias de *hackers* como la Defcon, donde distintas personas participan en concursos de creación tecnológica para enfriar rápidamente la cerveza o hackear automóviles con el fin de optimizar el sistema de ajuste y funcionamiento del vehículo (Holt, 2007).

El entretenimiento también está estrechamente relacionado con la motivación del **ego**, basado en el aumento de la autoestima y en el valor interno generado tras finalizar con éxito un ataque informático (Holt y Kilger, 2012; Kilger, 2010; Steinmetz, 2016). De hecho, el ego y la identidad de los *hackers* derivan en gran medida de la manipulación exitosa de la tecnología, ya sea para fines legítimos o maliciosos (Holt, 2007; Jordan y Taylor, 1998; Taylor, 1999). Los piratas informáticos suelen experimentar satisfacción psicológica tras un hackeo y pueden incluso obtener recompensas sociales de sus colegas y del público en general, dependiendo del objetivo y el resultado (Holt, 2007; Jordan y Taylor, 1998; Kilger, 2010). De hecho, la comunidad de *hackers* pone un gran énfasis en el dominio de la tecnología, que se demuestra mediante ataques exitosos (Holt, 2007; Jordan y Taylor, 1998; Steinmetz, 2016; Taylor, 1999). A su vez, la satisfacción personal generada por hackeos exitosos constituye un motivo importante a lo largo del tiempo.

La importancia del **estatus** obtenido por medio de la piratería también está intrínsecamente relacionada con el ego y con la **aceptación en determinados grupos sociales** (Dupont y otros, 2017; Kilger, 2010). Los *hackers* pueden ganarse el respeto y reconocimiento de los demás en función de su capacidad para hackear hardware y software de formas novedosas (Holt, 2007; Jordan y Taylor, 1998; Steinmetz, 2016). A la luz de la creciente globalización en la comunidad de *hackers*, existen pruebas de que los *hackers* pueden obtener reconocimiento en todo el mundo en función de la creación o lanzamiento de *malware* y herramientas de *hacking* que no existían anteriormente (Chu y otros, 2010). Alternativamente, los piratas informáticos pueden lograr cierto estatus a través del robo o la adquisición de información confidencial.

Por ejemplo, atacar servidores del gobierno o sistemas protegidos puede demostrar la capacidad general de un individuo y hacerle ganar prestigio entre la comunidad de *hackers* (véase Jordan y Taylor, 2004; y Kilger, 2010 para una discusión sobre este tema).

No obstante, a veces el *hacker* debe revelar cómo se completó dicho ataque o proporcionar esta información al resto para hacer constar sus conquistas (Dupont y otros, 2017). Como consecuencia, al divulgar la información, el método de ataque utilizado deja de ser secreto y puede llamar la atención de las fuerzas del orden involuntariamente, lo que aumenta la probabilidad de que estos *hackers* puedan ser detectados e identificados (Holt, 2007; Taylor, 1999). Por lo tanto, el prestigio basado en actividades maliciosas puede ser difícil de mantener con el tiempo sin que se aumente posteriormente el riesgo de arresto o sanción (Holt, 2007; Taylor, 1999).

Con la expansión de internet y su uso para expresar ideas políticas, nacionalistas y religiosas, el número de ataques impulsados por **causas ideológicas** ha aumentado considerablemente en la última década (Denning, 2010; Holt, 2012; Kilger, 2010; Jordan y Taylor, 2004). De hecho, estas causas varían según la ubicación de un determinado grupo social en el mundo y sus orientaciones culturales, ideológicas, políticas y religiosas. Los *hackers* maliciosos pueden emplear sus conocimientos y habilidades para participar en ataques en nombre de un sistema de creencias particular y ejercer así influencia sobre las políticas o acciones de otro grupo (Denning, 2010; Kilger, 2010).

> Por ejemplo, los *hackers* turcos participaron en una campaña de desfiguración web contra periódicos y medios de comunicación en línea tras la publicación de una imagen del profeta Mahoma con una bomba en su turbante (Holt, Freilich y Chermak, 2017). Esta imagen ofendió mucho a la comunidad musulmana internacionalmente, y los *hackers* turcos actuaron en defensa de su religión. Sus degradaciones hicieron notar su rechazo a la caricatura y expresaron su opinión sobre la percepción que otros tienen de su religión (Holt y otros, 2017). Del mismo modo, existen pruebas de que grupos afiliados a al-Qaeda (Denning, 2010) y colectivos extremistas de extrema izquierda (Holt, Stonhouse, Freilich y Chermak, 2019) han participado en ataques a una serie de sitios web corporativos y gubernamentales en apoyo a sus creencias.

Aquellos *hackers* motivados por una causa ideológica también pueden utilizar sus habilidades para robar información confidencial y así avergonzar a otro grupo social o influir en él (Andress y Winterfeld, 2014; Jordan y Taylor, 2004).

> Por ejemplo, algunos investigadores desmantelaron una red internacional de sistemas infectados pertenecientes a Gobiernos, embajadas y entornos corporativos en 103 países (Information Warfare Monitor, 2009; Markoff, 2009). Esta red de ordenadores afectados, conocida como GhostNet, parece estar controlada por determinados servidores en China con el fin de robar información confidencial y recopilar subrepticiamente datos sobre varios objetivos (Information Warfare Monitor, 2009; Markoff, 2009). Aunque no está claro si estos ataques fueron respaldados por el Gobierno chino, o si más bien se trató de *hackers* independientes, lo que está claro es que estos piratas informáticos intentaban obtener información para beneficiar a su país.

Del mismo modo, los grupos Anonymous y LulzSec perpetuaron varios ataques contra agentes políticos, financieros y gubernamentales para expresar su insatisfacción con las políticas sobre piratería y libertad de información en línea (Correll, 2010; Holt y otros, 2019). Estos ataques implicaron a personas que no necesariamente tienen habilidades de hackeo, pero que son capaces de atacar un sistema empleando herramientas de piratería sencillas y que realizan la mayor parte del trabajo ellas mismas. Por consiguiente, los ataques motiva-

dos por causas ideológicas están cambiando tras la aparición de herramientas simples y de poblaciones interesadas en expresar su opinión en espacios virtuales (Denning, 2010; Holt y otros, 2019; Kilger, 2010).

Algunas personas también participan en ataques informáticos para obtener acceso a varios grupos, ya sea por actividades maliciosas o no maliciosas (Kilger, 2010; Meyer, 1989). Este problema es antiguo y está estrechamente relacionado con las creencias generales de la comunidad *hacker*, una meritocracia en la que los individuos son juzgados en función de sus habilidades y capacidades generales (Holt, 2007; Jordan y Taylor, 1998; Taylor, 1999). Las personas que desarrollan y utilizan sus habilidades de maneras únicas pueden llamar la atención de agentes altamente cualificados en la comunidad de *hackers* (Dupont y otros, 2017; Holt, 2007; Meyer, 1989). Tal reconocimiento puede conllevar la unión a grupos que valoran las habilidades de piratería de dicha persona (Kilger, 2010). Esto es particularmente relevante teniendo en cuenta la cada vez mayor especialización en dispositivos de software y hardware. Los individuos pueden presentar una serie de habilidades que otros no poseen, como la capacidad de codificar en un cierto lenguaje de programación o la destreza en una determinada forma de ataque o en un protocolo de seguridad (Dupont y otros, 2017; Leukfeldt y otros, 2017; Meyer, 1989). Como tal, pueden integrarse en un grupo que no posee tal habilidad, pero que reconoce el valor intrínseco de dicho individuo.

3. Las correlaciones demográficas, conductuales y actitudinales de los *hackers*

Aunque es importante comprender las motivaciones que hay detrás de los ataques informáticos, también lo es identificar la composición demográfica general de la comunidad *hacker*. La diversidad evidente en las destrezas y habilidades de la comunidad de *hackers* lleva a muchos a preguntarse cómo son los piratas informáticos. Existe la creencia generalizada de que los *hackers* son en su mayoría varones jóvenes blancos, empollones antisociales que solo son capaces de relacionarse con otros en línea. Esta idea persiste dada la representación de *hackers* en películas y programas de televisión populares (Thomas, 2002). La investigación empírica centrada en la composición demográfica de la comunidad *hacker* sugiere que esta imagen es hasta cierto punto válida (Bachmann, 2010; Schell y Dodge, 2002). Sin embargo, es difícil documentar con veracidad las características físicas de los *hackers*, pues se trata de una comunidad extremadamente hermética (Holt, 2007; Steinmetz, 2016). Muchos piratas informáticos piensan que tanto los investigadores como los medios de comunicación no comprenderán el significado de la piratería, y no quieren discutir estas cuestiones con ellos por temor a que sean mal citados o difamados. Además, los *hackers* que participan en actividades ilegales evitan cualquier divulgación de información personal por temor a ser detectados o arrestados por la policía (Holt, 2007; Leukfeldt y otros, 2017). Por lo tanto, cualquier discusión acerca de la comunidad *hacker* debe tratarse cuidadosamente, dada la dificultad inherente de acceder a este sector de la población.

Una de las primeras preguntas que a menudo se plantean los sociólogos está relacionada con el tamaño total de la población de *hackers* en un momento dado. Esto es muy difícil de determinar, ya que los piratas informáticos permanecen en la clandestinidad y pueden usar múltiples identidades en línea para ocultar sus actividades y minimizar la probabilidad de detección.

Por ejemplo, Jordan y Taylor (1998) estimaron que existen al menos 100.000 *hackers*, aunque esta cifra puede haber aumentado considerablemente en la última década.

Un dato que los piratas informáticos y la investigación científica confirman constantemente acerca de la piratería es que existe una proporción muy pequeña de *hackers* altamente cualificados dentro de la comunidad de piratas informáticos. En general, estas personas son extremadamente difíciles de identificar porque ocultan sus verdaderas identidades a los extraños.

Por ejemplo, Holt, Strumsky, Smirnova y Kilger (2012) encontraron menos de 10 *hackers* altamente cualificados dentro de una muestra de casi 400 *hackers* rusos.

Una razón para esta variación en las habilidades técnicas de los *hackers* puede ser la edad a la que un individuo está expuesto a la tecnología. Los piratas informáticos mayores suelen mostrar una exposición temprana a la tecno-

logía, ya sea jugando a videojuegos o empleando procesos de comunicación simples (Bachman, 2010; Holt, 2007; Holt, 2010; Holt et al., 2017; Schell y Dodge, 2002; Taylor, 1999). Los piratas informáticos señalan frecuentemente que disponen de ordenador propio o que pueden acceder a la tecnología antes de los 10 años o más tarde, en la adolescencia temprana, lo que parece ser un elemento indispensable para despertar el interés de alguien joven. Del mismo modo, muchos piratas informáticos se consideran curiosos o inquisitivos, y quieren entender cómo funcionan las tecnologías a niveles fundamentales (Holt, 2007; Jordan y Taylor, 1998; Taylor, 1999). La curiosidad fue particularmente valiosa para los *hackers* de los años ochenta y principios de los noventa, cuando la tecnología era menos accesible al usuario general, al tratarse de una habilidad indefectible para desarrollar cualquier comprensión del hardware y software informáticos (Meyer, 1989; Kilger, 2010; Taylor, 1999). La curiosidad sigue siendo un factor fundamental entre los piratas informáticos, a pesar de que la interfaz de usuario y el software de la informática moderna son cada vez más simples (Holt, 2007; Steinmetz, 2016).

El deseo de aprender cómo se comunican los dispositivos y el funcionamiento de las aplicaciones puede despertar el deseo de estas personas de comprender mejor la funcionalidad de la tecnología informática en general.

La mayoría de los piratas informáticos expertos suele encontrarse en la adolescencia o rondar los 20 años, aunque los piratas informáticos más veteranos suponen un sector cada vez mayor en la comunidad *hacker* (véase, por ejemplo, Bachmann, 2010; Steinmetz, 2016). Los piratas informáticos de mayor edad también parecen tener un empleo remunerado, y muchos trabajan en el ámbito de la seguridad informática, mientras que los *hackers* más jóvenes pueden no tener trabajo (Schell y Dodge, 2002). Los miembros de la comunidad *hacker* suelen presentar una combinación de educación formal e informal, ya que los *hackers* fomentan la búsqueda del conocimiento mediante la lectura y el aprendizaje experimental (Bachmann, 2010; Holt, 2007; Steinmetz, 2016). La limitación de los datos disponibles sugiere que una parte de los *hackers* cualificados tendría al menos un grado de formación profesional, mientras que un número menor dispondría de títulos universitarios de cuatro años (Bachmann 2010; Holt y otros, 2010; Schell y Dodge, 2002).

Asimismo, la mayoría de los estudios señalan que los piratas informáticos son predominantemente hombres, independientemente de su participación en el hackeo malicioso o en el *cracking* (Gilboa, 1996; Grabosky, Russell, Smith y Urbas, 2004; Jordan y Taylor, 1998; Schell y Dodge, 2002). Se considera que menos del 20 % de los *hackers* son mujeres, aunque es difícil identificar su verdadero número, ya que tienden a proteger su género de los demás mientras

están en línea para reducir el riesgo de sufrir acoso (Gilboa, 1996; Hutchings & Chua, 2017; Schell & Dodge, 2002; Taylor 1999). Por lo tanto, se desconoce cuántas mujeres participarían en realidad en la piratería informática.

Los *hackers* también informan constantemente de cómo establecen relaciones con otras personas que comparten sus intereses, a pesar del mito generalizado de que los piratas informáticos son solitarios y pasan mucho tiempo socializando únicamente con otros usuarios en línea (Holt, 2009; Holt y Kilger, 2008; Leukfeldt y otros, 2017; Meyer, 1989; Schell y Dodge, 2002). Numerosos estudios sugieren que los *hackers* mantienen relaciones con personas tanto en el mundo real como en entornos en línea, aunque sus compañeros virtuales pueden tener más importancia, ya que suelen ser incapaces de identificar a otros en el mundo real que compartan sus mismos intereses en la informática (Holt, 2009; Holt y Kilger, 2008; Meyer, 1989; Schell y Dodge, 2002; Steinmetz, 2016). Aquellos cuyas amistades están interesadas en la informática son en realidad un predictor muy importante de participación en el *hacking* (Bossler y Burruss, 2010; Holt, 2009; Holt, Bossler, y Burrus, 2010; Marcum y otros, 2014; Skinner y Fream, 1997). Establecer amistades con otras personas que puedan aumentar tu conocimiento y proporcionarte información que no tienes y, en general, respaldar tus intereses puede garantizar un interés a largo plazo en la tecnología (Bossler y Burruss, 2010; Holt, 2009; Holt y otros, 2010; Skinner y Fream, 1997).

Al mismo tiempo, las relaciones entre compañeros son fundamentales para la participación en delitos e infracciones cibernéticas, ya que proporcionan información sobre los métodos y justificaciones para tales conductas en la red (Bossler y Burruss, 2010; Higgins y Makin, 2004; Higgins y Wilson, 2006; Holt y otros, 2010; Ingram e Hinduja, 2008; Skinner y Fream, 1997). De hecho, las relaciones de amistad entre *hackers* maliciosos pueden servir como fuentes de inspiración para los más jóvenes, que pueden imitar las acciones de sus compañeros. Skinner y Fream (1997) describieron sucintamente esta cuestión y afirmaron que los compañeros que participan en ciberdelitos ayudan a sus amigos a «aprender no solo cómo operar un equipo altamente técnico, sino también procedimientos específicos, programación y técnicas para usar un ordenador de manera ilegal» (Skinner y Fream, 1997, 498).

Además, las amistades entre *hackers* maliciosos suponen una importante fuente de validación para la creencia de que no existen leyes reales sobre el comportamiento en línea y que tanto el buen uso como el uso indebido de un ordenador puede ser aceptable dependiendo de ciertas circunstancias (véase, por ejemplo, Holt y otros, 2010; Ingram y Hinduja, 2008; Skinner y Fream, 1997).

Por ejemplo, Gordon (2000) descubrió que, con frecuencia, los creadores de virus no estaban preocupados por los efectos de sus productos, incluso si sabían que eran ilegales y dañinos. Además, los *hackers* argumentan que sus acciones generalmente no causan daño (Gordon y Ma, 2003; Turgeman-Goldschmidt, 2005), y culparían a las víctimas de tener poca habilidad o seguridad para evitar tal ataque (Chua y Holt, 2017; Jordan y Taylor, 1998).

Mantener relaciones con los demás compañeros dentro de la comunidad *hacker* también es fundamental, ya que se refuerza la participación en malas conductas cibernéticas a lo largo del tiempo a través de la aceptación social y la aprobación para participar en ataques exitosos y en la recopilación de materiales pirateados.

Por ejemplo, aquellos que hacen comentarios positivos sobre la participación en un delito cibernético aumentan la probabilidad de que se cometan futuros delitos (Bossler y Burruss, 2010; Holt, y otros, 2010; Ingram e Hinduja, 2008; Skinner y Fream, 1997).

El refuerzo social por cometer delitos es un factor indispensable en el crimen tanto en línea como en entornos reales, razón por la cual las relaciones sociales entre los piratas informáticos son un aspecto importante en su participación a largo plazo en ataques informáticos.

Además de las relaciones entre *hackers* maliciosos, la investigación reciente también ha comenzado a considerar el papel del autocontrol sobre la probabilidad de participar en un ciberdelito (Bossler y Burruss, 2010; Gordon y Ma, 2003; Holt, Bossler y May, 2012; Holt y Kilger, 2008). En los estudios criminológicos, el autocontrol se trata como un rasgo individual que se desarrolla durante la primera infancia a través del control y corrección de los padres en respuesta a malas conductas (Gottfredson y Hirschi, 1990). Los padres que controlan, reconocen y castigan los malos comportamientos cuando estos se dan tienen más probabilidades de vincularse emocionalmente con sus hijos. A su vez, los niños desarrollan altos niveles de autocontrol o la capacidad de regular y controlar su propio comportamiento ante la oportunidad de cometer delitos (Gottfredson y Hirschi, 1990). Los hijos cuyos padres no consiguen controlar su comportamiento tienen más probabilidades de desarrollar un bajo autocontrol y, por lo tanto, son más proclives a participar en actividades de riesgo o incluso delictivas. Las personas con poco autocontrol son impulsivas, insensibles, no verbales, asumen riesgos y prefieren las tareas simples (Gottfredson y Hirschi, 1990). De esta manera, no son capaces de valorar completamente las consecuencias y los beneficios de sus acciones, por lo que son propensos a cometer delitos y a mostrar comportamientos arriesgados.

Las personas con bajo autocontrol muestran una mayor tendencia a participar en actos de delincuencia callejera (Pratt y Cullen, 2000) y en ciberdelitos, como la descarga ilegal de música y de software (véase Higgins y Makin, 2004; Higgins y Wilson, 2006). No está claro qué papel puede desempeñar el autocontrol en el hackeo, dada la diversidad de ataques que pueden calificarse como pirateo (Bossler y Holt, 2010; Holt y Kilger, 2008).

Por ejemplo, la piratería puede abarcar desde prácticas simplistas, como deducir contraseñas, hasta delitos más graves y tecnológicamente sofisticados, como la producción de *malware*.

Como resultado, el autocontrol puede variar según las habilidades y la actitud general del *hacker*. Por ejemplo, Holt y Kilger (2008) hallaron que los piratas informáticos, tanto en entornos universitarios como en la población en general, tenían niveles relativamente altos de autocontrol. Además, un estudio de

Bossler y Burruss (2010) encontró una relación interesante entre el autocontrol, los compañeros de la comunidad *hacker* y la piratería. Más concretamente, aquellas personas que establecían relaciones con otros *hackers* presentaban niveles más altos de autocontrol. Las personas con compañeros *hackers* tenían niveles más bajos de autocontrol y se beneficiaban de estas relaciones sociales con otros piratas para reforzar sus actividades y aprender métodos de piratería (Bossler y Burruss, 2010). Bossler, Holt y May (2011) señalaron resultados similares en una muestra de estudiantes de secundaria y bachillerato que participan en delitos informáticos.

Estos hallazgos proporcionan información inicial sobre la influencia que teóricamente ejerce un bajo nivel de autocontrol en el desarrollo general de las habilidades y capacidades de toda la comunidad *hacker*. Aquellos piratas informáticos con poco autocontrol pueden comenzar a participar en ciberdelitos porque ven la oportunidad de colaborar en actividades peligrosas o de riesgo, incluidos los actos de *hacking* más simples, como descifrar contraseñas y agregar o eliminar información de los sistemas. Sin embargo, con el tiempo, los piratas informáticos con poco autocontrol también pueden ser capaces de no ir más allá de estos ataques básicos porque, por lo general, tendrán poco interés en dedicar su tiempo al hackeo. Su incapacidad para concentrarse y comprender mejor la complejidad de ciertos actos de piratería puede limitar su capacidad general. Las personas con niveles más altos de autocontrol no necesariamente se enfrentan a estos problemas, y les resulta más fácil perfeccionar sus conocimientos y habilidades con el paso del tiempo. A su vez, pueden perpetrar ataques más sofisticados y sobrepasar a sus colegas *hackers* con un bajo nivel de autocontrol. Debería estudiarse más a fondo esta cuestión para aclarar la relación entre bajos niveles de autocontrol y la piratería, aunque se entiende que esta puede ser una correlación clave para comprender las características generales de la comunidad de *hackers*.

4. La subcultura *hacker*

Tal y como se señaló, los *hackers* establecen vínculos sociales con otros piratas tanto en línea como en el mundo real. Se cree que las relaciones entre ellos son el origen de una subcultura corrupta y, en algunos casos, criminal basada en valores e intereses compartidos que guían la acción individual de estos *hackers* (véase Miller, 1959; Short, 1958). Los estudios acerca de la subcultura *hacker* son extremadamente valiosos, ya que muestran las normas y creencias de los piratas informáticos e identifican variaciones en su estructura a lo largo del tiempo. No obstante, existen tres cuestiones clave que parecen influir en los comportamientos de los *hackers*, la primera de las cuales es la importancia de la tecnología (Holt, 2007; Jordan y Taylor, 1998; Meyer, 1989; Steinmetz, 2016; Taylor, 1999; Thomas, 2002). Los intereses y actividades de los *hackers* se centran en el software y el hardware informáticos, así como en otras formas tecnológicas asociadas a la informática. Asimismo, la conexión de un individuo con la tecnología ayuda a desarrollar su capacidad de hackeo (Holt y otros, 2017; Jordan y Taylor, 1998; Steinmetz, 2016; Taylor, 1999). Para establecer dicha conexión, los piratas informáticos deben desarrollar «una relación fácil, si no voraz», con la tecnología informática y de comunicaciones, así como la voluntad de explorarla y utilizarla de maneras novedosas (Jordan y Taylor, 1998, pág. 764).

Por lo tanto, el conocimiento y el dominio de la tecnología desempeñan un papel importante en la subcultura *hacker* (Holt, 2007; Meyer, 1989, Thomas, 2002).

Los *hackers* pasan una cantidad significativa de tiempo aprendiendo sobre tecnología para conocer con detalle cómo funcionan los dispositivos informáticos. Esto aumenta la importancia de la destreza tecnológica en la subcultura *hacker*, demostrada en actos de piratería en el mundo real (Furnell, 2002; Holt, 2007; Steinmetz, 2016). Los *hackers*, además, demuestran sus conocimientos sobre la cultura *hacker* haciendo referencias a la historia de la piratería o empleando el argot *hacker* cuando se comunican con sus compañeros (Loper, 2000, pág. 66). Tales demostraciones destacan la conexión de los *hackers* con la tecnología y les permiten ganar prestigio entre los miembros de la comunidad (Holt, 2007; Loper, 2000).

Con todo, la naturaleza ilegal de algunas formas de piratería puede explicar la importancia del anonimato en la cultura *hacker* (Holt, 2007; Jordan y Taylor, 1998; Taylor, 1999; Thomas, 2002). En concreto, los piratas informáticos intentan proteger sus actividades con respecto a las fuerzas policiales y los agentes del Gobierno (Taylor, 1999, pág. 29). El uso de identificadores o apodos en

entornos en línea y en el mundo real hace más difícil conocer la verdadera identidad de un *hacker* (Dupont y otros, 2017 Furnell, 2002; Jordan y Taylor, 1998). Los hackeos y ataques que se efectúan con éxito se atribuyen a su identidad y habilidad en línea, lo que suscita un deseo de presumir y compartir con los demás tales destrezas (Dupont y otros, 2017; Holt, 2007; Jordan y Taylor, 1998). Esto puede ayudar a un individuo a ganar prestigio dentro de la comunidad *hacker*, aunque pone al *hacker* en riesgo de ser detectado por la policía (Furnell, 2002; Leukfeldt y otros, 2017). Por lo tanto, los piratas informáticos deben mantenerse en una línea muy fina entre compartir información y mantener la privacidad de ciertos conocimientos (Holt, 2007; Jordan y Taylor, 1998). A su vez, el anonimato refuerza y mantiene la barrera entre los piratas informáticos y la policía (Dupont y otros, 2017; Taylor, 1999).

5. La diferencia entre *hackers* basada en su prestigio en línea y fuera de línea

Los motivos para hackear pueden variar según el individuo y sus intereses y habilidades. Las técnicas que emplean los piratas informáticos pueden diferir en parte en función de su capacidad para acceder a sistemas informáticos e información clave.

Con ese fin, los *hackers* pueden clasificarse dependiendo de si ya desempeñan un papel importante dentro de una organización o empresa, o si actúan de manera independiente.

Aquellas personas que ya están trabajando dentro de una institución corporativa o gubernamental y que deciden participar en ataques informáticos pueden ser vistas como «personas con información privilegiada», en el sentido de que tienen acceso exclusivo a ciertos recursos y la capacidad de moverse en un entorno fiable como administradores de sistemas o profesionales de seguridad (Cappelli, Moore, Shimeall y Trzeciak, 2006; Dhillon y Moores, 2001; Shaw, Post y Ruby, 1998). Sus esfuerzos y actividades quedan fácilmente en secreto cuando ostentan este control administrativo, aunque sus ataques también pasarían desapercibidos porque tienden a robar subrepticiamente información o a instalar *malware* inactivo en caso de que los despidan (Cappelli y otros, 2006; Dhillon y Moores, 2001).

Dada la naturaleza general de las amenazas internas, es posible que tengan motivaciones diferentes a las de los *hackers* externos.

Por ejemplo, una investigación de Shaw, Ruby y Post (1999) encontró diversos comportamientos típicos que definirían al *hacker* infiltrado. En concreto, son introvertidos y carecen de buenas habilidades sociales, lo que les dificulta interactuar con otros dentro y fuera de las estructuras corporativas tradicionales. Además, los *hackers* infiltrados muestran una actitud negativa hacia la autoridad como consecuencia de problemas familiares a largo plazo (Shaw y otros, 1999).

Estos problemas se unen a la fuerte necesidad de socializar con otros en entornos virtuales, donde pueden interactuar más cómodamente. También muestran una ética cambiante y una falta de empatía por los demás, por lo que niegan su participación en comportamientos ilegales (Shaw y otros, 1999). También se perciben a sí mismos con derecho a hackear, lo que les lleva a buscar formas de recibir el reconocimiento y el privilegio que sienten que otros les deben. Sus diferencias psicológicas y actitudinales suelen dificultarles responder en situaciones estresantes de manera constructiva. En su lugar, suelen responder en estos momentos de tensión con comportamientos irracionales o

peligrosos. Por último, los *hackers* infiltrados tienden a utilizar ataques simples dependiendo del objetivo y el servicio que aprovechan, aunque en ocasiones se han empleado métodos más complejos (Cappelli y otros, 2006).

Las amenazas internas fueron la preocupación más común entre los profesionales de la seguridad cibernética durante los años ochenta y noventa debido a la pequeña población de usuarios cualificados y a las limitaciones en la conectividad a internet en general (Andress y Winterfeld, 2014). La amenaza externa aumentó a finales de la década de 1990, a medida que la tecnología informática se volvió cada vez más accesible, lo que supuso un aumento significativo en el número de ataques contra corporaciones y Gobiernos (Taylor, 1999). Hasta la fecha, la mayoría de los ataques cibernéticos procederían de personas externas, aunque aquellas con información interna aún pueden representar una amenaza para los sistemas y la información confidenciales.

6. Las correlaciones de la piratería y de la victimización por *malware*

Aunque cada vez hay más investigación sobre los predictores conductuales y actitudinales para la participación en ciberdelitos, los estudios sobre la victimización son escasos. Esto se debe en parte a las dificultades para identificar víctimas de piratería informática y ciertas formas de cibercrimen (Bossler y Holt, 2009, 2010; Holt, 2003; Yar, 2005). Es posible que las víctimas no sepan que han sido atacadas, ya que las infecciones de software malicioso pueden emular fallos de sistemas informáticos y hardware (Bossler y Holt, 2009, 2010; Holt y Bossler, 2013; Holt, van Wilsem, van de Weine y Leukfeldt, 2019). Además, los usuarios solo pueden darse cuenta de que algún tipo de pirateo les ha afectado después de que su información se haya eliminado o corrompido de alguna manera (Holt, 2003; Ngo y Patternoster, 2011). Del mismo modo, algunos casos de victimización están completamente fuera del control de un individuo, como el filtrado de datos a gran escala en una empresa donde se roban los datos del cliente (Bossler y Holt, 2009; Holt y Lampke, 2010). La institución que administra los datos es responsable de esta desprotección, por lo que las víctimas quedan exentas de cualquier responsabilidad con respecto al ataque. Por último, cuando un ataque se lleva a cabo, este puede no ser reportado a la policía dada la preocupación sobre si dicho ataque se tomará en serio o si alguien podrá investigar el delito (Holt, 2003; Newman y Clarke, 2003; Wall, 2001).

Por lo tanto, supone todo un desafío comprender completamente el número de *malwares* y víctimas de ciberdelitos que se producen cada año. Diversas estadísticas sugieren que estas formas de cibercrimen son extremadamente costosas, ya que van desde millones hasta miles de millones, dependiendo del objetivo.

> Por ejemplo, la Oficina de Estadísticas Judiciales de los Estados Unidos (o BJS, Bureau of Justice Statistics) señaló que 2/3 de las empresas sufrieron algún tipo de delito cibernético, lo que suponía un total en pérdidas de 867 millones de dólares en 2007, la mayoría de ellos relacionados con *malware* (Rantala, 2008).

Las encuestas corporativas más recientes sugieren que un solo ataque de *malware* puede costar un promedio de cinco millones de dólares a las grandes organizaciones, lo que mayormente resulta de la pérdida de productividad de los empleados (Fruhlinger, 2018). Estas son, no obstante, estimaciones limitadas, puestas en cuestión por parte de algunos estudiosos debido a sus tamaños de muestra y a las fuentes de financiación de dichos estudios (véase, por ejemplo, Levi y otros, 2018).

Dada la limitación de datos disponibles acerca de las víctimas de ciberdelitos, los investigadores han intentado explorar su correlación utilizando datos «autorreportados», o proporcionados por las propias víctimas (Bossler y Holt,

2009; 2010; Choi, 2008; Holt y otros, 2019; Ngo y Patternoster, 2011). Los análisis de estos datos sugieren que existen pocas correlaciones para la infección de software malicioso, el fraude y las víctimas de piratería. La edad, la raza y el género no suponen una relación real con el riesgo de infección o daño, lo que reflejaría los deseos de los creadores de *malware* y *hackers* de afectar a tantos objetivos como sea posible (Bossler y Holt, 2009, 2010; Holt y otros, 2019). Con el fin de tener éxito, los piratas informáticos lanzan redes amplias para atacar a miles, si no a millones de usuarios, ya que es probable que solo quedara infectada una pequeña parte de todos los ordenadores (Chu y otros, 2010; Furnell, 2002; Gordon y Ma, 2003). Por lo tanto, puede ser difícil discernir tendencias demográficas únicas en el riesgo de victimización.

Además, el tiempo que se está en línea y el uso de software de protección, como antivirus y otras herramientas, parecen tener un impacto mínimo en el riesgo de victimización (Bossler y Holt, 2009; Choi, 2008; Holt y Bossler, 2013; Holt y otros, 2019). La relativa escasa importancia del tiempo que se pasa conectado es lógica, puesto que las infecciones y los ataques pueden perpetuarse independientemente de si un individuo está interactuando con otros en línea o no (Yar, 2005). En cambio, los *hackers* solo necesitan un sistema que esté conectado a internet para poder infectarlo. El ordenador en cuanto que objetivo disponible es todo lo que el *hacker* requiere para intentar acceder a información confidencial (Yar, 2005). Además, la naturaleza asincrónica de algunas formas de comunicación en línea, como el correo electrónico, dificulta la identificación de correlatos de riesgo basados en el uso de la tecnología (Bossler y Holt, 2009). Un *malware* puede enviarse a una dirección de correo electrónico y permanecer inactivo hasta que el usuario abre el correo electrónico y ejecuta el archivo (Szor, 2005). Esto puede tardar diez segundos o diez horas, dependiendo de la frecuencia con la que el individuo comprueba sus mensajes. Por lo tanto, la exposición a delincuentes en entornos en línea a través del uso de la tecnología en general puede constituir un factor más pertinente en el riesgo de victimización que el tiempo que se pasa en foros o en Facebook.

El uso de software de protección, como antivirus y otras herramientas, también parecen desempeñar un papel mínimo en la reducción del riesgo de victimización (Bossler y Holt, 2009; Holt y otros, 2019). Aunque los programas de seguridad pueden defender a los usuarios de ataques aleatorios, la eficacia de estos programas está limitada en función de la administración de estas herramientas por parte de los propios usuarios (Brenner, 2008).

> El software antivirus, por ejemplo, debe actualizarse y ejecutarse regularmente para garantizar que el usuario está protegido en todo momento por versiones más actualizadas del programa (Bossler y Holt, 2009). Con todo, muchos usuarios no dedican tiempo a estas prácticas de seguridad, lo que dificulta predecir con qué frecuencia estas herramientas protegen a los usuarios. De hecho, un estudio reveló que casi el 25 % de los ordenadores personales con programas de seguridad en todo el mundo tienen software malicioso, como un virus, almacenado en su memoria (PandaLabs, 2007). Por lo tanto, muchas personas resultan ser víctimas de ataques informáticos a pesar de la presencia y el uso de software antivirus y otros programas de protección para defender su equipo contra hackeos maliciosos cometidos aleatoriamente.

Uno de los pocos predictores fiables de victimización por piratería y *malware* es la participación del individuo en ciertas formas de cibercrimen (Bossler y Holt, 2009, 2010; Holt y Bossler, 2013). Esto reflejaría el riesgo general de exposición a ciberdelincuentes que resultaría de actividades como la piratería digital o la descarga ilegal de películas o música. Los creadores de *malware* reconocen que, dado que las personas frecuentemente descargan materiales pirateados o ven pornografía en línea, insertan código malicioso en lo que parece ser un archivo de música o multimedia con la esperanza de que alguien descargue el elemento y ejecute el código (Chu y otros, 2010). De hecho, uno de los pocos correlatos de infección de *malware* en un estudio de Bossler y Holt (2009) señaló que aquellos que se dedican a la piratería presentan un mayor riesgo de infección.

Otro correlato de victimización son las actividades de amigos y compañeros en línea. En entornos virtuales, las actividades de una persona exponen a otras a daños, ya sea directa o indirectamente.

> Por ejemplo, si el ordenador de un individuo está infectado con *malware*, algunos programas intentarán replicarse y propagarse enviando archivos infectados a otros a través de *spam*. En este sentido, Bossler y Holt (2009) descubrieron que las personas cuyos amigos veían pornografía en línea tenían un mayor riesgo de infecciones de *malware*. Bossler y Holt (2010) obtuvieron resultados similares con respecto a la victimización por *malware*, el fraude y la piratería. Las personas con compañeros que participan en diversas formas de cibercrimen tenían más probabilidades de perder información y datos de tarjetas de crédito o de ser atacados como consecuencia de que sus amigos los atacaran voluntariamente o que aumentaran indirectamente su riesgo de ser atacados debido a un comportamiento negligente.

Dada la falta de datos sobre predictores y correlatos conocidos de victimización por cibercrimen, cabe considerar por qué hay tan pocos predictores de ataques informáticos. Una de las explicaciones más significativa radica en el hecho de que los sistemas informáticos individuales pueden ser atacados de innumerables maneras en línea. Los mensajes de *spam* enviados a un individuo pueden contener software malicioso, al igual que los sitios web que utilizan herramientas como el *malware* iFrame, que infecta el navegador con la simple conexión al sitio web (Chu y otros, 2010; Holt y Graves, 2007; Wall, 2004). Aunque este tipo de ataques son bien conocidos, los usuarios mayormente ingenuos se ven afectados (Wall, 2007). Todos los días se lanzan a la red ataques más peculiares que utilizan *exploits* y *malware* nuevos y desconocidos, por lo que es difícil protegerse por completo del ataque (Chu y otros, 2010; Gordon y Ma, 2003). Además, las filtraciones de datos a gran escala en empresas afectan al usuario individual, lo que dificulta que las víctimas puedan lidiar con algunos riesgos. Por lo tanto, sabemos mucho más acerca de los delincuentes que de las víctimas, pese al significativo daño potencial que el público en general puede experimentar a manos de piratas informáticos y creadores de *malware*.

7. Historia de la piratería y el *malware*

7.1. Los comienzos

Aunque la comunidad moderna de *hackers* está compuesta por individuos con varios niveles de habilidad y diversos principios éticos, dicha comunidad ha cambiado significativamente desde sus humildes orígenes. Para observar cómo ha evolucionado la piratería, es importante situar su aparición en el contexto de la innovación social y tecnológica. Los *hackers* han existido desde los principios de la informática, a finales de la década de 1950, aunque la tecnología era muy diferente a la disponible actualmente. De hecho, algunos investigadores sostienen que el término *piratería* o *hacking* surgió entre los estudiantes de ingeniería del Instituto de Tecnología de Massachusetts (MIT) en la década de 1950 (Levy, 2001). Los estudiantes emplearon este término para referirse a manipulaciones lúdicas, aunque hábiles, de la electrónica, y fue en gran parte sinónimo de «divertirse» o «hacer el tonto».

Con el tiempo, los estudiantes comenzaron a usar este término para describir una novatada universitaria, única en el entorno altamente técnico del MIT. Sin embargo, estos ataques nunca fueron abiertamente maliciosos, y a menudo requerían una demostración de destreza técnica para ser considerados y vistos como un acto de *hacking*. Pronto, los estudiantes del MIT usaron el término *hackeo* para describir más actividades inquisitivas en el campus, incluidas las incursiones en los túneles de vapor del campus, como el «hackeo de túneles», y la manipulación del sistema telefónico, llamada «hackeo de teléfonos». Además, el Tech Model Railroad Club (TMRC) del MIT tomó el término como parte de un lenguaje cada vez más especializado para describir su trabajo en los sistemas ferroviarios del club. Para este grupo, la piratería fue un proceso desordenado y lúdico de resolución de problemas que contrastaba con las técnicas convencionales (Levy, 2001). De hecho, la edición de 1958 del diccionario del TMRC proporciona la siguiente entrada para el término *piratear*: «1) algo hecho sin un fin constructivo; 2) un proyecto llevado a cabo con un mal asesoramiento; 3) un generador de entropía; 4) cometer, o intentar cometer, un hackeo».

Aunque el MIT desempeñó un papel fundamental en la creación del término *pirateo* y su significado, también se relacionó con la aparición de la informática en la década de 1950 en entornos universitarios. En ese momento, las unidades centrales (o *mainframes*) informáticas eran sistemas enormes que ocupaban por completo salas climatizadas y que presentaban una memoria y potencia de procesamiento general relativamente limitadas (Levy, 2001). Los ordenadores eran, además, extremadamente caros y se encontraban solo en las universidades, como MIT, Cornell y Harvard. Estos dispositivos tampoco estaban vincu-

lados entre sí de ninguna manera, y cualquier utilización innovadora de los recursos solía ser de cosecha propia. De hecho, los programadores informáticos responsables de estas infraestructuras tecnológicas intentaron identificar técnicas para acelerar y avanzar en estos sistemas lentos. La creación de soluciones sofisticadas e innovadoras para estos problemas se denominó *hacks*, y los programadores responsables fueron identificados como *hackers* de acuerdo con el concepto original generado entre el alumnado del MIT (Levy, 2001).

La percepción del pirata informático como un programador y manipulador experto continuó durante la década de 1960, aunque la agitación social y los disturbios civiles alterarían la forma en que los piratas informáticos veían su relación con la tecnología y el mundo en general. A medida que la tecnología informática pasó de las universidades a las aplicaciones militares, los llamados piratas informáticos mostraron insatisfacción por lo que vieron como un uso inapropiado de un recurso maravilloso (Thomas, 2002). Por consiguiente, los programadores comenzaron a desarrollar una serie de ideales, conocidos como ética *hacker* (Levy, 2001; Thomas, 2002). Esta serie de seis principios puede resumirse de la siguiente manera (Furnell, 2002, pág. 64; Levy, 2001):

- El acceso a ordenadores, y cualquier cosa que pueda enseñarte algo sobre cómo funciona el mundo, debe ser ilimitado y total.
- Toda la información ha de ser libre.
- Desconfía de la autoridad: promueve la descentralización.
- Los piratas informáticos tienen que ser juzgados por sus habilidades de piratería, no por falsos criterios como la titulación, la edad, la raza o la posición social.
- Puedes crear arte y belleza con un ordenador.
- Los ordenadores pueden cambiar tu vida para mejor.

La creencia básica de que la información debería ser de libre acceso y gratuita para todos era fundamental para que todo el mundo pudiera entender cómo funcionan las cosas e identificar las maneras en que podrían mejorarse (Thomas, 2002, pág. 15). De hecho, la tecnología tendría que ser un medio de información para otros. Esta ética guió las actividades de los *hackers* en aquel momento y sentó las bases de la cultura *hacker* contemporánea (Levy, 2001).

7.2. Los años setenta

En la década de 1970, la percepción de la piratería como un fin ético comenzó a cambiar con el surgimiento de dos actividades: el *phreaking* y el *homebrew computing*. La aparición del «*phreaking* telefónico», o la manipulación de la tecnología telefónica para comprender y controlar los sistemas telefónicos, fue

promovida por sectores contraculturales de los años sesenta (Landreth, 1984). El *phreaking* permitió a las personas hacer llamadas gratuitas a cualquier persona en el mundo controlando los interruptores del sistema telefónico. Por lo tanto, el *phreaking* es visto como una de las primeras formas principales de fraude electrónico, pues implica el uso ilegal y el robo de servicios de telefonía (Grabosky, 2001). Esta actividad tiene su origen en las protestas de Abbie Hoffman, el Technology Assistance Party (TAP) y el Youth International Party Line (YIPL) contra el monopolio de la telefonía por parte de las empresas (Landreth, 1984). El *phreaking* también llegó al público en general de la mano de un hombre llamado Cap'n Crunch (John Draper), que sopló un silbato de una caja de cereales en el receptor de su teléfono (Landreth, 1984). El silbato creó el tono perfecto de 2.600 megahercios, el cual, en ese momento, se usaba para conectar a un individuo a líneas de larga distancia. Este simple juguete abrió una nueva área tecnológica para que las personas exploraran, utilizaran y defraudaran a las compañías telefónicas de acuerdo con los orígenes de la piratería.

La práctica del *phreaking* se volvió maliciosa a raíz de la publicación de un artículo en la revista *Esquire* sobre Draper y otros *phreaks* en 1971. La atención que llamó este artículo sobre la actividad condujo a una serie de medidas enérgicas contra los *phreaks* aunando los esfuerzos de la policía y de los funcionarios de seguridad telefónica. En ese momento no existían leyes reales contra la exploración y manipulación de ordenadores y teléfonos, aunque el robo de servicios podía ser procesado. Sin embargo, la publicación de este artículo y su posterior investigación por parte de los principales medios de comunicación llamaron cada vez más la atención del poder legislativo y de la policía a finales de la década de 1970 (Parker 1980). De hecho, una de las primeras leyes de delitos informáticos en Estados Unidos se aprobó en Florida en 1978, lo que convertía el acceso no autorizado a los sistemas informáticos en un delito grave de tercer grado. Con todo, la implantación de estas leyes no se hizo con seriedad hasta mediados de los años ochenta.

La década de 1970 también vio el surgimiento de grupos de aficionados centrados en el desarrollo de hardware y en la programación informática, especialmente el Homebrew Computer Club en 1975. Estas reuniones informales se centraron en la construcción y discusión de ordenadores personales, bien mediante diseños personalizados e innovadores, bien a través del cada vez mayor número de *kits* comerciales disponibles en anuncios de revistas hasta principios de los años setenta. La mayoría de los miembros eran, efectivamente, *hackers*, pues usaban métodos y principios de piratería para avanzar aún más en el estado de la informática personal. Sin embargo, estos grupos rara vez emplearon el término *hacker* para referirse a sí mismos o a sus actividades en sus propios boletines informativos.

Gracias en gran parte a los esfuerzos de los *hackers* en el hogar y en la industria privada, el ordenador personal logró lanzarse en 1977 (Ceruzzi, 1998). La adopción de esta tecnología fue inicialmente lenta y no se estableció hasta

principios de la década de 1980, cuando las familias de clase alta y media comenzaron a comprar cada vez más ordenadores para sus hogares. La creación y venta de tecnología de módem, que conecta unos ordenadores con otros y distintas redes a través de líneas telefónicas, también mejoró y se volvió más accesible de inmediato para el usuario común. Como resultado, aquellas personas que nunca antes habían tenido acceso a la tecnología informática ahora podían detectar y explorar redes informáticas (Furnell, 2002). Asimismo, la explosión simultánea de videojuegos y otros sistemas de entretenimiento electrónico en el hogar puso en contacto a los jóvenes con la tecnología como nunca antes.

7.3. Los años ochenta

El auge de los ordenadores personales a principios de los años ochenta despertó el interés de los jóvenes, especialmente de los hombres, que comenzaron a explorarlos y usarlos de maneras que excedían su propósito como herramientas de aprendizaje o ayudas educativas. Esto marcó el comienzo de la unión de la cobertura mediática, centrada en el rápido avance y adopción de tecnologías informáticas, y del uso de dichas tecnologías con fines maliciosos y delictivos. El principal catalizador de esta cobertura fue el estreno de la película *WarGames* (*Juegos de guerra*), que presentaba a Matthew Broderick como un *hacker* adolescente que, sin sospechar, obtiene acceso a sistemas informáticos militares y casi produce un holocausto nuclear (Schneider, 2008).

Un mes después del estreno de la película, el FBI comenzó a registrar y a presentar demandas contra los miembros de un grupo local de piratas informáticos conocidos como los «414», el código de área de Milwaukee (Krance, Murphy y Elmer-Dewitt, 1983). Aunque estos muchachos participaron en intrusiones relativamente inocuas de redes protegidas y no causaron daños físicos a los sistemas o datos, la policía intentó publicitar las redadas (Hollinger y Lanza-Kaduce, 1988). Los medios de comunicación publicaron rápidamente historias sobre estas investigaciones para sacar provecho del interés público por el uso indebido de ordenadores, derivado de la película *WarGames* (Marbach, 1983). Además, los medios se referían a los miembros del grupo como *hackers*, ya que era este el término que usaban para caracterizar sus acciones. Esto marcó, pues, un antes y un después en el uso del término *hacker*, que cambió con respecto a su connotación original en los años cincuenta y sesenta, relacionada con ajustes informáticos éticos. El vínculo entre piratería y delincuencia proporcionado por los medios de comunicación ayudó a persuadir tanto al público como a los legisladores de que era necesario aplicar sanciones legales para hacer frente a las actividades de los *hackers*.

Conforme la gente empezó a adoptar las tecnologías de PC y a explorar otros sistemas conectados a través de módems, las comunidades en línea comenzaron a surgir a través de los sistemas de boletines electrónicos o BBS (*Bulletin Board Systems*). En concreto, los BBS se convirtieron en un recurso importante para los nuevos *hackers*, impulsados en parte por las hazañas observadas en los

medios y en relatos de ficción como *WarGames*. Tanto los usuarios tecnológicos experimentados como los *hackers* en ciernes compartieron información detallada sobre los sistemas que exploraron y se jactaron de sus proezas (Landreth, 1984). Estos sistemas también permitieron a los piratas informáticos formar grupos con redes privadas y crear paneles protegidos con contraseña para mantener a raya a los iniciados y salvaguardar su privacidad (Landreth, 1984; Meyer, 1989). Los grupos de *hackers* locales también se hicieron prominentes en función de sus hazañas e intrusiones en sistemas informáticos sensibles, como los *Masters of Disaster* y la *Legion of Doom* ('maestros del desastre' y 'legión de la perdición', respectivamente).

Según iban creciendo la población de *hackers*, una nueva escisión surgió con la publicación de un breve texto llamado «La conciencia de un hacker» o «El manifiesto del hacker». El documento fue publicado por el Mentor (The Mentor) en 1986, como diatriba contra los adultos, la policía y las escuelas (Furnell, 2002, pág. 59). El Mentor señalaba que los *hackers* buscan el conocimiento, incluso si eso significa irrumpir u obtener acceso ilegal en sistemas informáticos para protegerlos. Estas actividades, sin embargo, no convierten a los *hackers* en delincuentes. Estos, en cambio, suelen recibir la incomprensión y el rechazo de la población adulta desconocedora del valor de la tecnología. El Mentor, además, instigó a los piratas informáticos a participar en actos de *phreaking*, puesto que las compañías telefónicas están «dirigidas por avariciosos y aprovechados» (Furnell, 2002, pág. 59; The Mentor, 1986). Este documento respaldó en cierto modo la concepción cada vez más delictiva de la piratería, en contraste, pues, con la noción del *hacking* de los años sesenta y la «ética *hacker*». Como consecuencia, una brecha empezó a abrirse entre los *hackers* que apoyaban el citado manifiesto y aquellos otros más alineados con la ética *hacker*, así como también cambió la percepción que se tenía de la piratería maliciosa y exploratoria.

El énfasis cada vez mayor en la faceta delictiva de la piratería comenzó a cambiar la percepción de los *hackers*, que pasaron de agentes éticos cualificados a entidades criminales maliciosas. Esta concepción se respaldó, a su vez, en la Ley de Abuso y Fraude Informático en Dispositivos de Acceso Fraudulento de 1984, así como en su posterior revisión en 1986. La ley de 1984 se centró inicialmente en el uso y uso indebido de la información contenida en tarjetas de crédito, y estableció que cualquier delito de 5.000 $ de pérdida o más se consideraría un delito federal que pasaría a controlar el Servicio Secreto. La revisión de 1986 de esta ley, sin embargo, amplió la protección legal a toda aquella información computarizada en bancos e instituciones financieras. Asimismo, la ley añadió tres nuevas infracciones, incluido el acceso no autorizado a sistemas informáticos con vistas a estafar y causar perjuicios, así como el tráfico de contraseñas informáticas con intención de fraude. Al incluir estas actividades, los legisladores criminalizaron muchas de las acciones efectuadas por *hackers* jóvenes y que no necesariamente tenían mala fe.

La proclamación de estas nuevas leyes proporcionó a las fuerzas de seguridad mejores herramientas para investigar y enjuiciar eficazmente los ataques de *hackers* en todo el país (Sterling, 1992). De hecho, numerosas investigaciones de altos cargos policiales se llevaron a cabo a finales de los años ochenta y principios de los noventa, como la batalla entre los grupos *hackers* Legion of Doom y Masters of Deception (Slatalla y Quittner, 1995), así como los actos ciberdelictivos de Kevin Mitnick (Shimomura y Markoff, 1996) y Kevin Poulson (Littman, 1997).

La década de 1980 también vio la aparición de las primeras formas de software malicioso, o *malware*, diseñado para infectar los sistemas de PC y los usuarios domésticos. Las primeras formas de *malware* solían reproducir melodías simples o eliminaban letras de documentos, y se propagaban de uno a otro ordenador a través de disquetes. Sin embargo, la creación y distribución del primer gusano conocido de internet demostró el daño que podía causar un software malicioso.

En 1988, Robert Morris quiso comprender y documentar el tamaño de internet y el número de ordenadores conectados al mismo tiempo (Holt, Bossler y Seigfried-Spellar, 2017). Escribió un fragmento de código diseñado para recopilar esta información de manera remota moviéndose lentamente de un ordenador a otro, aunque debido a un fallo en su programación aprovechó sin percatarse de ello las vulnerabilidades de desbordamiento de búfer en el software. Como consecuencia, el gusano se propagó más rápido de lo previsto y el *exploit* causó un ataque de denegación de servicio, o DoS (*denial of service attack*), que dejó, en ese momento, todo internet inactivo (Holt, 2003). Morris recibió una multa de 10.050 $, obtuvo una sentencia de libertad condicional de tres años y fue obligado a 400 horas de servicio comunitario por sus acciones, una sentencia significativa en aquel momento (Holt y otros, 2017). Este incidente tuvo un mayor impacto en la creación de comunidades de seguridad informática, al dar lugar a la formación del primer Computer Emergency Response Team ('equipo de respuesta a emergencias informáticas', CERT) en la Carnegie Mellon para responder a nuevas amenazas en línea (Holt, 2003).

7.4. Los años noventa

El daño significativo que el gusano de Morris produjo en el procesamiento del sistema sentó las bases para un nuevo tipo de *malware* a fines de los años ochenta y principios de los noventa. Conforme la tecnología se hizo cada vez más accesible y asequible a principios de la década de 1990, la población de *hackers* continuó expandiéndose y el término *hacking* se relacionó cada vez más con actividades maliciosas. A principios de la década de 1990, los funcionarios de las fuerzas del orden público estatales y federales trataron de eliminar sistemáticamente las redes informáticas de lo que se percibía como un número cada vez mayor de *hackers*. Este proceso, denominado por Sterling (1992) «la represión de los *hackers*» (o «The Hacker Crackdown»), consistió en gran medida en operaciones encubiertas por parte de investigadores que actuaban como *hackers* en tablones de anuncios y salas de chat falsos para ganarse la confianza de los piratas informáticos.

A pesar de la creciente brecha cultural y generacional entre los *hackers* originales del MIT y la nueva generación de piratas informáticos en el internet de los noventa, todos ellos compartieron elementos comunes con la cultura *hacker* original. Por ejemplo, los piratas informáticos modernos generalmente inten-

tan reunir documentos internos después de acceder a un sistema, tanto para fanfarronear como para permitir el libre intercambio de información a través de la red de *hackers* (Holt y Kilger, 2012). Este deseo de difundir información y debatir métodos de ataque permitió a la policía reunir pruebas de actividades ilegales. Como consecuencia, el libre intercambio de información dentro de la comunidad *hacker* comenzó a evolucionar para disminuir la probabilidad de ser detenidos o recibir condenas. Los grupos de *hackers* locales comenzaron a apoyar conferencias sobre piratería, incluidas Defcon, Hackers On Planet Earth y PhreakNIC (Holt y otros, 2017).

Estas reuniones ofrecieron a los *hackers* la oportunidad de relacionarse en el mundo real y otorgó a los piratas informáticos cierto aire de respetabilidad ante las cada vez más frecuentes condenas a grupos de *hackers*. Al mismo tiempo, los piratas informáticos establecieron vínculos directos con la comunidad *underground* debido a las presentaciones sobre actividades de piratería que infringirían la ley (Holt, 2007).

> Por ejemplo, el grupo de *hackers* llamado Cult of the Dead Cow (cDc) lanzó un programa de *malware* troyano creado durante un panel en el Defcon de 1999 (Messmer, 1999). Lanzaron CD con el *malware* al público y alentaron a la gente a usar la herramienta porque podía aplicarse a la seguridad informática. En concreto, el programa permitió a los usuarios controlar de manera remota los ordenadores que tenían el software instalado en su sistema. Podían ayudar al usuario controlando su ratón o sus archivos sin la necesidad de estar presentes en la misma habitación. Asimismo, el programa instalaba puertas traseras en el sistema que no podían eliminarse, y permitía eliminar o alterar los archivos del sistema y capturar todas las pulsaciones de teclado y contraseñas (Sourceforge, 1999). Como resultado, esta herramienta se utilizó más como un recurso de ataque de *malware* que como una herramienta legítima de seguridad (Messmer, 1999).

El lanzamiento del BO2K es un buen ejemplo de la relación dinámica entre seguridad y piratería maliciosa que comenzó a finales de los años noventa. Esta relación se vio agravada en parte cuando los profesionales de la seguridad informática incorporaron un uso ético de las técnicas de piratería para defenderse de los atacantes. A medida que las empresas y las agencias gubernamentales usaban con cada vez mayor frecuencia ordenadores conectados a redes internas y al resto de sistemas en todo el mundo, la necesidad de proteger los activos sensibles de la amenaza de los piratas informáticos y del uso indebido de la informática aumentó considerablemente (Taylor, 1999). La comercialización masiva de ordenadores personales también aumentó la necesidad de medidas de seguridad personal y el aislamiento con respecto a atacantes de todo el mundo.

> Por ejemplo, el virus Melissa infectó ordenadores en todo el mundo al enviar correos electrónicos infectados diseñados para propagar el virus, lo que supuso al menos 80.000.000 $ en daños (Furnell 2002). Del mismo modo, los gusanos ILOVEYOU y Code Red supusieron pérdidas de miles de millones de dólares en los primeros años del nuevo milenio (Holt y otros, 2017).

La evolución de la comunidad de seguridad informática en la década de 1990 se produjo a raíz de la incorporación de *hackers* cualificados que entendían el proceso de identificación y protección de software y hardware vulnerables en cargos de la industria privada y del gobierno. Esto generó una nueva tensión dentro de la comunidad de *hackers* entre los piratas informáticos supues-

tamente éticos que trabajaban para la industria privada y en empresas de seguridad de nueva creación y aquellos otros *hackers* poco éticos que utilizaban las mismas técnicas para explorar y atacar sistemas (Taylor, 1999). Mientras que algunos percibieron este hecho como un retorno a la idea original de la ética *hacker*, otros consideraron que la transición del *hacker* al profesional de seguridad era vender el alma al diablo y traicionar la propia naturaleza de la apertura de información en la comunidad *hacker*.

La condena y detención de Kevin Mitnick avivó esta tensión a mediados de los años noventa. Mitnick fue considerado un héroe en la comunidad *hacker* por su gran habilidad para la piratería y por el trato excesivamente severo que recibió a manos de la policía y los fiscales. De hecho, los fiscales federales prohibieron a Mitnick usar ordenadores o dispositivos conectados a internet durante varios años después de haber salido de una prisión federal por el temor a que pudiera causar un gran daño a la telefonía o la industria privada (Loper, 2000). Muchos *hackers* donaron dinero al fondo de defensa legal de Mitnick, y sintieron que era un mero chivo expiatorio del miedo de los legisladores y las fuerzas del orden a la comunidad *hacker*. Poco después de su salida de prisión, Mitnick fundó una consultoría de seguridad informática, lo que algunos vieron como una traición a los principios básicos de la comunidad *hacker* (Loper, 2000). Como resultado, perdió respeto entre los miembros de la comunidad *hacker*, aunque sirvió de modelo para que otros pasaran de ser delincuentes conocidos a expertos de seguridad informática en una sociedad cada vez más dependiente de la tecnología.

A fines de los noventa, la World Wide Web y los PC habían cambiado radicalmente la naturaleza de los negocios y las comunicaciones. La expansión global y la conectividad que ofrece internet condujeron a la digitalización de información confidencial financiera y gubernamental, y a la creación de enormes bases de datos accesibles en línea. Los proveedores de servicios financieros, las redes sociales y las plataformas comerciales se trasladaron a entornos en línea para ofrecer directamente servicios a los usuarios de PC, ofreciéndoles comodidad para la comunicación y las compras. Como consecuencia, el panorama y la dinámica del hackeo, así como la industria de seguridad informática, cambiaron.

La gente comenzó a aplicar técnicas y habilidades de piratería en ataques motivados política y socialmente contra objetivos gubernamentales y de la industria privada.

Por ejemplo, los miembros del colectivo de *hackers* Electronic Disturbance Theatre crearon y lanzaron una herramienta de ataque llamada FloodNet (Jordan y Taylor, 2004; Schell y Dodge, 2002). Este programa fue diseñado como una herramienta independiente para permitir a piratas no cualificados participar en ataques de denegación de servicio a varios servicios gubernamentales como una forma de «desobediencia civil» (Schell y Dodge, 2002). Un ataque así impide que la gente pueda usar los servicios de comunicaciones, lo que los vuelve inútiles. Asimismo, numerosos *hackers* de EE. UU. y de China participaron en una serie de desfiguraciones de red atacándose los unos a los otros como forma de expresión política cuando un avión espía estadounidense se estrelló en China (Denning, 2003). Las desfiguraciones web permiten al atacante reemplazar la página web original con contenido propio, incluyendo texto e imágenes.

Un ataque así es ideal para que los *hackers* con motivación política muestren sus actitudes y creencias a todo el mundo (Andress y Winterfeld, 2014). Por lo tanto, el número de desfiguraciones aumentó dramáticamente durante este período a medida que más países se conectaron a internet y vieron en este un medio para expresar sus ideas políticas y religiosas.

Durante este período, se lanzó un notable programa de *malware* troyano llamado Sub7, famoso por su capacidad para infectar todas las variantes de los sistemas operativos Windows (Crapanzano, 2003). El *malware* podía enviarse como archivo adjunto de correo electrónico y emular distintos tipos de archivos populares, como .doc o .ppt, así como archivos de imagen. Una vez se ejecutaba el programa, su carga útil permitía a un atacante administrar el ordenador infectado a distancia, lo que incluía la capacidad de añadir o eliminar archivos, capturar pulsaciones de teclas y contraseñas almacenadas en caché, y controlar la cámara del sistema, el micrófono, las unidades de disco y las pantallas del escritorio (Crapanzano, 2003). Además, el *malware* proporcionaría actualizaciones al atacante en tiempo real, lo que les permitía saber cuándo se estaba usando el sistema y la víctima se encontraba en línea. Así, esta herramienta se hizo muy popular entre los *hackers* por su facilidad de uso y su poder sobre sistemas específicos.

7.5. De los 2000 hasta hoy

La década de los 2000 supuso aún más cambios en la piratería, más concretamente la transición hacia la profesionalización de los *hackers*. Las motivaciones de la piratería pasaron de la adquisición de prestigio y aceptación social en la comunidad *hacker*, que predominaron en los años ochenta y noventa, a la búsqueda del beneficio económico (Holt y Lampke 2010; Chu y otros, 2010). La complejidad de las herramientas utilizadas por *hackers* aumentó, y su propósito pasó de infección y degradación de redes globales al ataque y robo subrepticios de información confidencial. Por ejemplo, la creación y adopción de *malware* de *botnet* tuvo un gran impacto en las prácticas de piratería y de *malware* (Bacher y otros, 2005). El código de *botnet* constituye una amenaza combinada, ya que aúna *malware* de troyanos y virus, propagándose de la misma manera que los programas de troyanos u otros métodos de infección (Chu y otros, 2010). Al ejecutar la carga útil del *malware*, el código instala un programa *bot*, lo que convierte el dispositivo en un *zombi* que puede controlarse a distancia por medio de un protocolo de mensajería instantánea llamado Internet Relay Chat (IRC) (Bacher y otros, 2005; Chu y otros, 2010). El canal IRC para controlar el sistema infectado está preprogramado en el código, lo que permite al operador de *botnet* enviar comandos al sistema. Además, se pueden infectar varios dispositivos con este *malware* y contactar simultáneamente con el canal, creando una red *bot* o una red de dispositivos *zombis*. A su vez, el controlador del *bot* puede emplear su red de dispositivos infectados para enviar *spam* o participar en ataques DDoS contra varios objetivos (Chu y otros, 2010).

El surgimiento de *botnets* fue de gran ayuda a la comunidad *hacker*, pues proporcionaba una plataforma de ataque estable fácil de administrar y mantener.

Por ejemplo, los sistemas infectados controlados por el operador de *botnet* pueden usarse para enviar correo no deseado, verificar tarjetas de crédito obtenidas de manera fraudulenta o arrendar los sistemas infectados como servicios *proxy* para ocultar un tráfico web malicioso (Holt, 2013).

Ved también

Para más información sobre el robo de datos, ved el módulo 3.

Además, las *botnets* pueden emplearse para participar en ataques de denegación de servicio, donde cada ordenador en la red intenta contactar el mismo ordenador o servidor de contenido en línea. Las solicitudes se pueden ajustar para que ocurran en un período de tiempo determinado, por ejemplo, cada 0,5 milisegundos, para así saturar el ordenador con dichas solicitudes. Por lo tanto, el sistema en cuestión no puede resolver las solicitudes que llegan y no quedará disponible hasta que las solicitudes se detengan (Holt, 2013). Estos ataques pueden ser extremadamente costosos para las empresas si los clientes no pueden usar sus recursos durante largos períodos de tiempo (Bacher y otros, 2005; CSI, 2010).

Asimismo, los *hackers* comenzaron a alquilar sus *botnets* a otros para obtener beneficios de su infraestructura (Chu y otros, 2010; Franklin y otros, 2007). Los operadores de *botnets* podrían ganar con ello miles de dólares cada semana o mes, dependiendo de su alcance a sistemas infectados y recursos operativos (Holt, 2013). La aparición de este mercado ha perjudicado gravemente a la comunidad *hacker*, ya que se requiere una habilidad menor para hackear (Holt, 2013). Por el contrario, los usuarios pueden pagar a otros *hackers* para que ataquen en su nombre sin la necesidad de crear sus propias herramientas o infecciones. Como resultado, algunos miembros de la comunidad de ciberseguridad se refirieron al *malware* de *botnet* como *crimeware*, pues estos permiten a las partes interesadas una vía directa para participar en ciberdelitos a bajo coste (Bacher y otros, 2005).

El modelo proporcionado por el *malware* de *botnet* también supuso que una serie de *malwares* y servicios de piratería estuvieran disponibles a bajo coste en diferentes mercados clandestinos (Holt, 2013). Los atacantes vendían el acceso a códigos exclusivos de software malicioso, troyanos y otras herramientas, como paquetes de *exploits*, que infectan sistemas informáticos a través de *exploits* en navegadores web. Del mismo modo, la gente vende bases de datos de correo electrónico que podrían usarse para enviar correo no deseado, datos confidenciales obtenidos a partir de troyanos espía y otros servicios que podrían usarse para participar en ataques informáticos y ciberdelitos económicos (Holt, 2013).

La evolución de los *smartphones* y otros dispositivos conectados a la red wifi a mediados de los 2000 también llevó a los *hackers* a atacar estos sistemas, atraídos por la información confidencial que contienen. Por ejemplo, la capacidad de acceder a cuentas bancarias y sitios de comercio electrónico a través de aplicaciones móviles ofrece la oportunidad a los atacantes de que adquieran esta información. Los *hackers* y los escritores de *malware* comenzaron a interesarse en piratear estos dispositivos y adaptaron el *malware* a estas plataformas (BitDefender, 2009). Una de las herramientas de *malware* más notables utilizadas para atacar teléfonos móviles era conocida por los proveedores de

ciberseguridad como Zeus (Panda Security, 2015). Este troyano se adaptó a los dispositivos móviles utilizando sistemas operativos Android, y se diseñó y publicó como una aplicación bancaria (Leyden, 2012). El programa capturaba los mensajes SMS para autenticar transacciones entre la institución financiera y el cliente (FBI, 2010; Leyden, 2012). Una vez adquirido, el *malware* podía usar estos detalles financieros para realizar transferencias bancarias fraudulentas sin que los clientes lo supieran. Como resultado, estos ciberdelincuentes han podido ganar con éxito decenas de millones de dólares a través de transacciones bancarias fraudulentas en Europa y Estados Unidos (FBI, 2010; Leyden, 2012).

Los Estados nación también comenzaron a participar en operaciones sofisticadas de piratería para adquirir información confidencial y propiedad intelectual de empresas, universidades y agencias gubernamentales.

Ved también

Para más información sobre este tema, ved el módulo 5.

Por ejemplo, un grupo que se hace llamar Guardians of Peace ('Guardianes de la paz') atacó la sede de Sony Pictures en 2014 utilizando una sofisticada cantidad de herramientas de *malware* y técnicas de piratería (Robb, 2014). Los atacantes obtuvieron *terabytes* de datos, desde información sobre los empleados hasta correos electrónicos confidenciales, guiones y películas sin estrenar (Robb, 2014). Toda esta información se publicó en línea en un intento de avergonzar a la compañía y avergonzarlos para que no estrenasen la película llamada *The Interview*, que hablaba de un complot para asesinar al líder norcoreano Kim Jong-un (Robb, 2014). Los análisis posteriores al ataque realizados por las fuerzas del orden y las agencias de inteligencia vincularon el ataque al Gobierno de Corea del Norte, o al menos a *hackers* que trabajan en su nombre (Zetter, 2016).

Por lo tanto, la piratería ha cambiado drásticamente desde su uso inicial en universidades y organizaciones.

Resumen

Por lo general, los actos de ciberintrusión relacionados con la piratería informática y el software malicioso son el resultado directo de nuestra cada vez mayor dependencia social con respecto a la tecnología. No todos los *hackers* son delincuentes, aunque las técnicas empleadas por ellos pueden utilizarse para participar en actividades ilegales. El hackeo en general supone usar conocimientos sobre los sistemas y programas informáticos, aunque su resultado puede ir desde la modificación de los procesos del sistema hasta la interrupción de la red y el daño económico grave. La evolución de la piratería en los últimos cincuenta años demuestra cómo las motivaciones de los *hackers* maliciosos han cambiado para centrarse más en la ganancia económica, ya sea a través de la venta de herramientas y servicios de piratería, ya por el uso indebido de información confidencial. Es probable que esta tendencia continúe, siempre que los piratas informáticos puedan beneficiarse de sus acciones, aunque deben seguir elaborándose estudios para evaluar estas cuestiones (ved el módulo 6).

Bibliografía

Andress, J.; Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.

Bacher, P.; Holz, T.; Kotter, M.; Wicherski, G. (2005). *Tracking botnets: Using honeynets to learn more about bots* [en línea]. The Honeynet Project and Research Alliance. <www.honeynet.org/papers/bots/>

Bachmann, M. (2010). «The risk propensity and rationality of computer hackers». *The International Journal of Cyber Criminology* (núm. 4, págs. 643-656).

BitDefender (2009). «Trojans continue to dominate BitDefender's top ten e-threats». *BitDefender*. [en línea]. <www.bitdefender.com/news/trojans-continue-to-dominate-bitdefender%E2%96%93s-top-ten-e-threats-for-october-1208.html>

Bossler, A. M.; Burruss, G. W. (2011). «The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?». En: T. J. Holt y B. H. Schell (eds.). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (págs. 38-67). Hershey, PA: ISI Global.

Bossler, A. M.; Holt, T. J. (2009). «On-line activities, guardianship, and malware infection: An examination of routine activities theory». *International Journal of Cyber Criminology* (núm. 3, págs. 400-420).

Bossler, A. M.; Holt, T. J. (2010). «The effect of self-control on victimization in the cyberworld». *Journal of Criminal Justice* (vol. 38, núm. 3, págs. 227-236).

Bossler, A. M.; Holt, T. J.; May, D. C. (2012). «Predicting online harassment among a juvenile population». *Youth and Society* (núm. 44, págs. 500-523).

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State*. Nueva York: Oxford University Press.

Brenner, S. W. (2011). «Defining Cybercrime: A Review of Federal and State Law». En: R. D. Clifford (ed.). *Cybercrime: The Investigation, Prosecution, and Defense of a Computer Related Crime* (3.ª ed., págs. 15-104). Raleigh, NC: Carolina Academic Press.

Cappelli, D. M.; Moore, A. P.; Trzeciak, R. F.; Shimeall, T. J. (2008). «Common Sense Guide to Prevention and Detection of Insider Threats». *CERT Insider Threat Study Team*. Carnegie Mellon University.

Ceruzzi, P. (1998). *A History of Modern Computing*. Cambridge, MA: MIT Press.

Choi, K. S. (2008). «Computer crime victimization and integrated theory: An empirical Assessment». *International Journal of Cyber Criminology* (vol. 2, núm. 1).

Chu, B.; Holt, T. J.; Ahn, G. J. (2010). *Examining the Creation, Distribution, and Function of Malware On-Line* [en línea]. Washington, DC: National Institute of Justice. <www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf>

Chua, Y. T.; Holt, T. J. (2016). «A cross-national examination for the techniques of neutralization to account for hacking behaviors». *Victims & Offenders* (vol. 11, núm. 4, págs. 534-555).

Correll, S. P. (2010). «An interview with Anonymous». *PandaLabs Blog* (núm. 29).

Crapanzano, J. (2003). «Deconstructing SubSeven, the Trojan Horse of Choice» [en línea]. *SANS Reading Room*. <https://www.sans.org/reading-room/whitepapers/malicious/deconstructing-subseven-the-trojan-horse-of-choice-953>

Denning, D. E. (enero de 2003). «Cyber Security as an Emergent Infrastructure». En: *World Conference on Information Security Education* (págs. 1-2).

Denning, D. E. (2010). «Cyber-Conflict as an Emergent Social Problem». En: T. J. Holt y B. Schell (eds.). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (págs. 170-186). Hershey, PA: IGI-Global.

Dhillon & Dhillon, G.; Moores, S. (2001). «Computer crimes: theorizing about the enemy within». *Computers & Security* (vol. 20, núm. 8, págs. 715-723).

Dunham, K. (2008). *Mobile Malware Attacks and Defense*. Burlington, MA: Syngress.

Dupont, B.; Côté, A. M.; Boutin, J. I.; Fernandez, J. (2017). «Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world"». *American Behavioral Scientist* (vol. 61, núm. 11, págs. 1219-1243).

Federal Bureau of Investigation (2010). «Cyber banking fraud: Global partnerships lead to major arrests» [en línea]. <www.fbi.gov/news/stories/2010/october/cyber-banking-fraud>

Franklin, J.; Paxson, V.; Perrig, A.; Savage, S. (2007). «An inquiry into the nature and cause of the wealth of internet miscreants». *CCS07* (29 de octubre-2 de noviembre, Alexandria, VA).

Fruhlinger, J. (2018). «What Is WannaCry Ransomware, How Does It Infect, and Who Was Responsible?». *CSO* [en línea]. <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Londres: Addison-Wesley.

Gilboa, N. (1996). «Elites, Lamers, Narcs, and Whores: Exploring the Computer Underground». En: L. Cherny; E. R. Weise (eds.). *Wired_Women* (págs. 98-113). Seattle: Seal Press.

Gordon, S. (2000). *Virus Writers: The End of the Innocence?* [en línea]. <http://vxheaven.org/lib/asg12.html>

Gordon, S.; Ma, Q. (2003). *Convergence of virus writers and hackers: Factor or fantasy*. Cupertino, CA: Symantec Security White Paper.

Gottfredson, M. R.; Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Grabosky, P. N. (2001). «Virtual criminality: Old wine in new bottles?». *Social & Legal Studies* (vol. 10, núm. 2, 243-249).

Grabosky, P.; G. Smith, Russell; Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge University Press.

Higgins, G. E.; Makin, D. A. (2004). «Does social learning theory condition the effects of low self-control on college students' software piracy». *Journal of Economic Crime Management* (vol. 2, núm. 2, págs. 1-22).

Higgins, G. E.; Wilson, A. L. (2006). «Low self-control, moral beliefs, and social learning theory in university students' intentions to pirate software». *Security Journal* (vol. 19, núm. 2, págs. 75-92).

Hollinger, R.; Lanza-Kaduce, L. (1988). «The process of criminalization: The case of computer crime laws». *Criminology* (núm. 26, págs. 101-126).

Holt, T. J. (2003). «Examining a transnational problem: An analysis of computer crime victimization in eight countries from 1999 to 2001». *International Journal of Comparative and Applied Criminal Justice* (vol. 27, núm. 2, págs. 199-220).

Holt, T. J. (2007). «Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures». *Deviant Behavior* (núm. 28, págs. 171-198).

Holt, T. J. (2009). «Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers». En: F. Schmalleger; M. Pittaro (eds.). *Crimes of the Internet* (págs. 336-355). Upper Saddle River, NJ: Pearson Prentice Hall.

Holt, T. J. (2012). «Exploring the intersections of technology, crime, and terror». *Terrorism and Political Violence* (vol. 24, núm. 2, págs. 337-354).

Holt, T. J. (2013). «Examining the forces shaping cybercrime markets online». *Social Science Computer Review* (núm. 31, págs. 165-177).

Holt, T. J.; Bossler, A.; Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction* (2.ª ed). Londres: Routledge.

Holt, T. J.; Burruss, G. W.; Bossler, A. M. (2010). «Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world». *Journal of Crime and Justice* (núm. 33, págs. 15-30).

Holt, T. J.; Burruss, G. W.; Bossler, A. M. (2018). «Assessing the macro-level correlates of malware infections using a routine activities framework». *International journal of offender therapy and comparative criminology* (vol. 62, núm. 6, págs. 1720-1741).

Holt, T. J.; Freilich, J. D.; Chermak, S. M. (2017). «Exploring the subculture of ideologically motivated cyber-attackers». *Journal of contemporary criminal justice* (vol. 33, núm. 3, págs. 212-233).

Holt, T. J.; Graves, D. C. (2007). «A qualitative analysis of advance fee fraud e-mail schemes». *International Journal of Cyber Criminology* (vol. 1, núm. 1, págs. 137-154).

Holt, T. J.; Kilger, M. (2008). «Techcrafters and makecrafters: A comparison of two populations of hackers». *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing* (págs. 67-78).

Holt, T. J.; Kilger, M. (2012). «Know your enemy: The social dynamics of hacking». *The Honeynet Project* [en línea]. <https://honeynet.org/files/Holt%20and%20Kilger%20-%20KYE%20-%20The%20Social%20Dynamics%20of%20Hacking.pdf>

Holt, T. J.; Lampke, E. (2010). «Exploring stolen data markets on-line: Products and market forces». *Criminal Justice Studies* (núm. 23, págs. 33-50).

Holt, T. J.; Stonhouse, M.; Freilich, J.; Chermak, S. M. (2019). «Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups». *Terrorism and Political Violence* (págs. 1-22).

Holt, T. J.; Strumsky, D.; Smirnova, O.; Kilger, M. (2012). «Examining the Social Networks of Malware Writers and Hackers». *International Journal of Cyber Criminology* (vol. 6, núm. 1).

Holt, T. J.; van Wilsem, J.; van de Weijer, S.; Leukfeldt, R. (2018). «Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization». *Social Science Computer Review* (0894439318805067).

Huang, W.; Brockman, A. (2010). «Social Engineering Exploitations in Online Communications: Examining Persuasions used in Fraudulent E-mails». En: Holt, T. J. (ed.). *Crime Online: Causes, Correlates, and Context* (págs. 87-112). Raleigh, NC: Carolina Academic Press.

Hutchings, A.; Chua, Y. T. (2016). «Gendering cybercrime». En: *Cybercrime Through an Interdisciplinary Lens* (págs. 181-202). Londres: Routledge.

IBM (2016). *IBM study: Businesses more likely to pay ransomware than consumers* [en línea]. <http://www-03.ibm.com/press/us/en/pressrelease/51230.wss>

Information Warfare Monitor (2009). «Tracking ghostnet: Investigating a cyber espionage network» [en línea]. <https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5f-e7708d543651>

Ingram, J. R.; Hinduja, S. (2008). «Neutralizing music piracy: An empirical examination». *Deviant Behavior* (vol. 29, núm. 4, págs. 334-365).

James, L. (2005). *Phishing Exposed*. Rockland: Syngress.

Jordan, T.; Taylor, P. (1998). «A sociology of hackers». *The Sociological Review* (núm. 46, págs. 757-780).

Jordan, T.; Taylor, P. (2004). *Hacktivism and Cyber Wars*. Londres: Routledge.

Kaspersky, E. V. (2003). «The classification of computer viruses» [en línea]. Berna: Metropolitan Network BBS Inc. <www.avp.ch/avpve/classes/classes.stm>

Kilger, M. (2010). «Social Dynamics and the Future of Technology-Driven Crime». En: T. J. Holt y B. Schell (eds.). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (págs. 205-227). Hershey, PA: IGI-Global.

King, A.; Thomas, J. (2009). «You can't cheat an honest man: Making $$$ and sense of the Nigerian Email Scams». En: F. Schmalleger y M. Pittaro (eds.). *Crimes of the Internet* (págs. 206-224). Upper Saddle River, NJ: Pearson Prentice Hall.

Krance, M.; Murphy, J.; Elmer-Dewitt, P. (1983). «The 414 Gang Strikes Again» [en línea]. *Time*. <www.time.com/time/magazine/article/0,9171,949797,00.html>

Kravets, D. (2010). «U. S. declares iPhone jailbreaking legal, over Apple's objections» [en línea]. *Wired Threat Level* <www.wired.com/threatlevel/2010/07/feds-ok-iphone-jailbreaking/>

Landreth, B. (1985). *Out of the Inner Circle*. Seattle, WA: Microsoft Press.

Leukfeldt, R.; Kleemans, E. R.; Stol, W. (2017). «Origin, growth, and criminal capabilities of cybercriminal networks». An international empirical analysis». *Crime Law and Social Change* (núm. 67, págs. 39-53).

Levi, M.; Reuter, P.; Halliday, T. (2018). «Can the AML system be evaluated without better data?». *Crime, Law and Social Change* (págs. 1-22).

Levy, S. (2001). *Hackers: Heroes of the Computer Revolution*. Nueva York: Penquin.

Leyden, J. (2012). «Major £30m cyberheist pulled off using MOBILE malware» [en línea]. *The Register* (7 de diciembre). <www.theregister.co.uk/2012/12/07/eurograbber_mobile_malware_scam/>

Littman, J. (1997). *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen*. Nueva York: Little Brown.

Loper, K. (noviembre de 2000). «Profiling hackers: beyond psychology». En: *Annual meeting of the American Academy of Sociology*.

Marbach, W. (1983b). «Cracking Down on Hackers». *Newsweek* (núm. 34).

Marcum, C. D.; Higgins, G. E.; Ricketts, M. L.; Wolfe, S. E. (2014). «Hacking in high school: Cybercrime perpetration by juveniles». *Deviant Behavior* (vol. 35, núm. 7, págs. 581-591).

Markoff, J. (2009). «Vast spy system loots computers in 103 countries». *The New York Times* (núm. 29).

Kaspersky, E. V. (2003). «The classification of computer viruses» [en línea]. Berna: Metropolitan Network BBS Inc., Bern, Switzerland. <www.avp.ch/avpve/classes/classes.stm>

Meyer, G. R. (1989). *The Social Organization of the Computer Underground* (tesis de máster). Northern Illinois University.

Miller, W. B. (1958). «Lower class culture as a generating milieu of gang delinquency». *Journal of Social Issues* (vol. 14, núm. 3, págs. 5-19).

Mitnick, K. D.; Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Nueva York: Wiley Publishing.

Nazario, J. (2003). *Defense and Detection Strategies against Internet Worms*. Artech House.

Newman, G.; Clarke, R. (2003). *Superhighway Robbery: Preventing E-commerce Crime*. Cullompton, NJ: Willan Press.

Ngo, F. T.; Paternoster, R. (2011). «Cybercrime victimization: An examination of individual and situational level factors». *International Journal of Cyber Criminology* (núm. 5, págs. 773-793).

PandaLabs (2013). «Malware infections in protected systems» [en línea]. <http://research.panadasecurity.com/blogs/images/wp_pb_malware_infections_in_protected_Systems.pdf>

Panda Security (2015). *Annual Report PandaLabs 2015 Summary* [en línea]. <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>

Parker, D. B. (1980). «Computer abuse research update». *Computer/LJ* (núm. 2, pág. 329).

Ponemon Institute (2018). *2018 Cost of Data Breach Study: Impact of Business Contiunity Management* [en línea]. <https://ibm.co/2L7Th4P>

Pratt, T. C.; Cullen, F. T. (2000). «The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis». *Criminology* (núm. 38, págs. 931-964).

Rantala, R. R. (2008). *Cybercrime against businesses, 2005* (NCJ 221943) [en línea]. Bureau of Justice Statistics <www.bjs.gov/content/pub/pdf/cb05.pdf>

Robb, D. (2015). «The Sony Hack one year later: Just who are the Guardians of Peace?» [en línea]. *Deadline* (24 de noviembre). <https://deadline.com/2015/11/sony-hack-guardians-of-peace-one-year-anniversary-1201636491/>

Russinovich, M. (2013). «Hunting down and killing ransomware (scareware)» [en línea]. *Microsoft TechNet Blog*. <http://blogs.technet.com/b/markrussinovich/archive/2013/01/07/3543763.aspx>

Schell, B. H.; Dodge, J. L. (2002). *The Hacking of America: Who's Doing it, Why, and How*. Westport, CT: Quorum Books.

Schneider, H. (2008). *Wargames*. United Artists.

Shaw, E. D.; Ruby, K. G.; Post, J. M. (1998). «The insider threat to information systems». *Security Awareness Bulletin* (vol. 2, núm. 98, págs. 1-10).

Shimomura, T.; Markoff, J. (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw –by the Man Who Did It*. Nueva York: Hyperion.

Short, J. F. (1968). *Gang Delinquency and Delinquent Subcultures*. Oxford: Harper & Row.

Skinner, W. F.; Fream, A. M. (1997). «A social learning theory analysis of computer crime among college students». *Journal of Research in Crime and Delinquency* (núm. 34, págs. 495-518).

Slatalla, M.; Quittner, J. (1995). *Masters of Deception: The Gang that Ruled Cyberspace*. Nueva York: Harper Collins Publishers.

Sourceforge (1999). *Basic BO2K setup tutorial* [en línea]. <http://bo2k. sourceforge.net/docs/bo2k_1_1_5/BasicTutorial.html>

Steinmetz, K. F. (2015). «Craft(y)ness: An ethnographic study of hacking». *British Journal of Criminology* (55, págs.125-145).

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime*. NYU Press.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Nueva York: Bantam Books.

Symantec (2018). *Internet Security Threat Report 2018* [en línea] (vol. 23). <https://resource.elq.symantec.com/LP=6819?inid=symc_threat-report_istr_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS>

Szor, P. (2005). *The Art of Computer Virus Research and Defense*. Nueva York: Addison-Wesley.

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime*. Londres: Routledge.

Thomas, D. (2002). *Hacker Culture*. Mineápolis, MN: University of Minnesota Press.

Turgeman-Goldschmidt, O. (2005). «Hacker's accounts: Hacking as a social entertainment». *Social Science Computer Review* (núm. 23, págs. 8-23).

Turkle, S. (1984). *The Second Self: Computers and the Human Spirit*. Nueva York: Simon and Schuster.

Wall, D. S. (2004). «Digital realism and the governance of spam as cybercrime». *European Journal on Criminal Policy and Research* (núm. 10, págs. 309-335).

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Wang, W. (2006). *Steal This Computer Book 4.0: What They Won't Tell You About the Internet*. Boston, MA: No Starch Press.

Yar, M. (2005). «The novelty of "cybercrime": An assessment in light of routine activity theory». *European Journal of Criminology* (vol. 2, núm. 4, págs. 407-427).

Zetter, K. (2016). «The Sony Hackers were causing mayhem for years before they hit the company» [en línea]. *Wired* (24 de febrero) <https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/>