DESCARGO DE RESPONSABILIDAD

Todas las técnicas, procesos, procedimientos y productos mencionados y/o explicados en este libro tienen como única intención la formación del lector en materia de ciberseguridad.

En ningún caso se pretende que las habilidades que puedan ser adquiridas mediante esta lectura puedan ser empleadas para cometer acciones ilícitas.

Cada usuario debe conocer las leyes de regulación de delitos telemáticos que hay vigentes en su país, y tiene la obligación de obedecerlas.

Si alguna persona hace uso de lo expuesto en esta obra para cometer cualquier tipo de delito, lo hará exclusivamente bajo su completa responsabilidad.

INTRODUCCIÓN

Cuando la mayoría de la gente escucha hablar sobre Hackers, lo primero que se viene a la cabeza es la imagen de un delincuente, en un callejón oscuro, normalmente con una mochila llena de cables y de todo tipo de aparatos electrónicos y, cómo no, con una sudadera con la capucha sobre su cabeza.

Y en realidad no nos puede extrañar que esto sea así. La industria del entretenimiento se ha ocupado desde hace bastante tiempo, a través de un sinfín de películas o de series (como la reciente Mr. Robot), de estereotipar a los Hackers de este modo, como personajes oscuros, delincuentes cibernéticos en la mayoría de las ocasiones, o como rebeldes justicieros en el mejor de los casos.

Figura 0.1. Fotograma de la serie Mr. Robot (Imagen extraída de la web Yorokobu)

Pero no debemos quedarnos en un análisis tan banal del mundo Hacker. En realidad, un Hacker puede ser un delincuente, un activista, un estudiante con un grado de curiosidad más acentuado que el de la mayoría de sus compañeros de aula o el jefe de seguridad de la información de una multinacional.

Como veremos en el siguiente capítulo a continuación, a un Hacker no lo definen los propósitos que persigue con sus actuaciones (en realidad lo que define esto es el tipo de Hacker que es), sino los conocimientos tecnológicos y las capacidades de investigación e indagación que tenga en este campo.

Es por ello que en el libro tampoco se habla de técnicas de ataque y técnicas de defensa Hacker, ya que todos, independientemente de los fines que busquen, utilizan las mismas herramientas y los mismos procedimientos de modo general.

Lo que se pretende aquí por tanto es dar a conocer las técnicas más usuales que suelen emplear, cómo trabajan al fin y al cabo. De este modo, si sabemos cómo funcionan, podemos emplearlas nosotros mismos para buscar vulnerabilidades en nuestros sistemas, o nos será más sencillo repeler posibles ataques que podamos sufrir.

Bienvenidos al mundo Hacker.

1

EMPEZANDO A CONOCER EL MUNDO HACKER

1.1 ¿QUÉ ES UN HACKER?

Como ya hemos podido irnos dando cuenta, esta es la primera piedra en el camino que nos vamos a encontrar cuando pretendemos dar a conocer el mundo Hacker.

Existe de modo generalizado una visión que describe a los Hackers como delincuentes. Y esto llega a tal punto, que si buscamos la definición de esta palabra en el Diccionario de la Real Academia de la Lengua Española, su primera definición es "Pirata Informático".

Por suerte, después de esta acepción, podemos encontrar una segunda como "Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora".

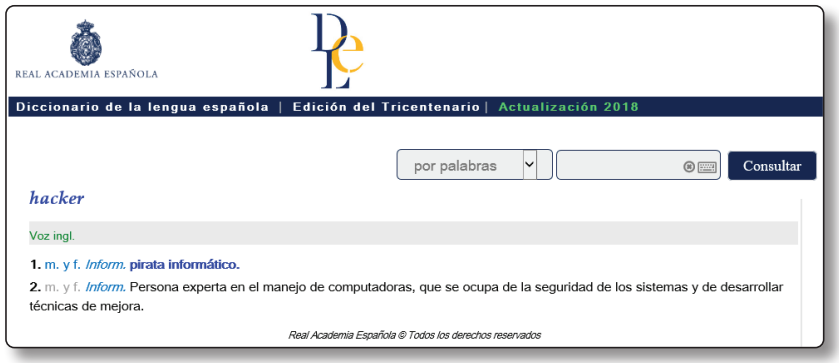

Figura 1.1. Acepciones de Hacker en el diccionario de la RAE

En realidad, el término Hacker nace en la década de los 50 del siglo XX en el ámbito del Instituto Tecnológico de Massachusetts (MIT), haciendo referencia a personas que son entusiastas de algún elemento relacionado con la tecnología (ordenadores, antenas, teléfonos, lenguajes de programación, etc.).

Esta idea nos conduce al concepto que se da hoy en día a los hackers informáticos, que no son más que expertos en distintos aspectos (redes, programación, criptografía, etc.) que dedican su trabajo y su esfuerzo a la búsqueda de fallos de seguridad en sistemas.

Y para conseguir su objetivo, la principal tarea que llevan a cabo es intentar romper la seguridad que tengan dichos sistemas informáticos para "colarse" en ellos sin permiso. Pero sería un error considerarlos como ciberdelincuentes por este motivo; esto lo determinarán los objetivos buscados con sus acciones.

1.2 TIPOS DE HACKERS

Como acabamos de ver, como norma general todos los tipos de hackers que nos podemos encontrar utilizan las mismas técnicas para realizar su trabajo, y son los objetivos que persiga cada uno los que van a marcarnos las diferencias entre ellos.

Este aspecto es el que nos va a proporcionar la clasificación más extendida y aceptada por todos, la clasificación de los sombreros. La adopción de este nombre viene de la costumbre que había en las películas de vaqueros, en las cuales se ponía un sombrero de color blanco al bueno y uno de color negro al malo, de modo que se aclarasen la trama y los personajes incluso antes de las películas a color.

- Hackers de sombrero blanco (White Hat).

  Son conocidos también con el nombre de Hackers Éticos. Su trabajo tiene como objetivo testear los sistemas en busca de fallos de seguridad y solucionarlos. Normalmente son contratados por las propias empresas dueñas de dichos sistemas, con el objetivo de aumentar la seguridad de los mismos y evitar posibles ataques.

- Hackers de sombrero negro (Black Hat).

  También conocidos como Crackers. Suelen llevar a cabo acciones ilícitas para conseguir alguna recompensa, normalmente monetaria. Sus objetivos pueden ir desde entrar en un sistema para robar cierta información, hasta la propagación de malware o ataques de denegación de servicio a servidores.

- Hackers de sombrero gris (Grey Hat).

  A medio camino entre los White Hat y los Black Hat. Normalmente acceden a sistemas sobre los que no tienen permisos para descubrir fallos de seguridad (como los sombrero negro) para, una vez los tienen identificados, ofrecer sus servicios a la empresa para solucionarlos (trabajo de los sombrero blanco). Se mueven en una fina línea entre lo legal y lo ilegal al acceder sin permiso previo, pero sin llegar a perjudicar a las empresas.

Figura 1.2. Película Colt .45 de 1950 donde se puede ver el uso del color de los sombreros

Además de esta clasificación, también existen otros tipos de hackers que no está de más que conozcamos:

- Phreakers.

  Realizan trabajos muy similares a los de los hackers, pero en este caso centran sus acciones sobre el mundo de la telefonía y no de los sistemas de información. En realidad, son los precursores de los hackers informáticos, ya que la aparición de la telefonía es bastante anterior a la de la informática.

- Lamers o Script-Kiddies.

  Son personas con escasos conocimientos técnicos, que basan sus ataques en el uso de herramientas desarrollados por terceros, sin preocuparse del funcionamiento de los mismos ni de los sistemas que pretenden atacar. Suelen presumir de tener habilidades que en realidad no tienen, ya que lo único que hacen es aprovecharse del trabajo que han realizado otros.

- Newbies.

  Su traducción literal es novato. Es una persona que acaba de iniciarse en el mundo del hacking y que todavía no tiene unos conocimientos amplios sobre el tema.

- Hacktivistas.

  Emplean técnicas de hacking para llevar a cabo reivindicaciones políticas y/o sociales. En los últimos años el grupo Anonymous se ha convertido en el mayor exponente de este tipo de hackers con numerosas acciones en la red.

1.3 BREVE HISTORIA DEL MUNDO HACKER

La mayoría de los estudios coinciden en situar el origen de la comunidad hacker en el MIT (Instituto Tecnológico de Massachusetts) a finales de los años 50, cuando un grupo de alumnos del centro realizan el primer curso sobre programación que se imparte, y se sorprenden de todo lo que se puede llegar a hacer a través de las computadoras.

Alrededor de este grupo de jóvenes comienza a surgir el término hacker, para hacer referencia a aquellos locos de los ordenadores que eran capaces de hacer cosas que para el resto serían impensables.

Figura 1.3. Vista aérea del MIT, lugar de nacimiento de la cultura hacker

El siguiente momento importante en la historia de la cultura hacker tiene lugar en 1962, cuando se crea *ARPANET*, una red que comunica diferentes Universidades de Estados Unidos, con investigadores, comunidades de interés y empresas, lo cual permite a estos programadores colaborar entre sí para conseguir aumentar sus conocimientos.

Fruto de estas colaboraciones surge en 1975 un fichero de jerga empleada por los hackers conocido como *Jargon File*. Por su parte, los estudiantes del MIT creaban un sistema operativo propio para sus ordenadores llamado *IST*, escrito en lenguaje LISP.

A la vez que surgía ARPANET, por un lado, los laboratorios Bell desarrollan su sistema operativo UNIX, el cual permitía conectar máquinas que tuvieran este sistema dentro de la red que denominaron *USENET*, la cual competía directamente con ARPANET.

Cuando en 1983 se canceló la venta de las computadoras sobre las que trabajaba IST, UNIX quedó como el gran sistema de referencia para toda la comunidad hacker. En esa misma época, el proyecto *GNU* comienza a dar sus primeros pasos, plantando la semilla para el nacimiento del concepto de software libre, lo cual encaja a la perfección con la ideología hacker de acceso libre a la información.

Uno de los mayores logros de esta nueva corriente es la aparición en 1991 de Linux, sistema operativo basado en UNIX que desarrolló como software libre LinusTorvalds con el apoyo de cientos de programadores que colaboraron libremente en el proyecto. Al poco tiempo, Linux se convertirá en una de las banderas del movimiento hacker.

1.4 ACTUACIONES FAMOSAS

Todos los casos tratados en este punto forman parte de acciones llevadas a cabo por hackers de sombrero negro. Evidentemente, aquellas inspecciones de seguridad realizadas por hackers de sombrero blanco no suelen salir a la luz, ya que queda dentro del ámbito de la organización o la empresa en cuestión, quien se encargará se solucionar los problemas de seguridad que pueda tener sin dar a conocer información de los mismos.

A lo largo de los años han sido muy numerosos los casos de ataques de hackers sobre diferentes plataformas en Internet, teniendo entre ellos un amplio abanico de objetivos diferentes: ataques contra gobiernos, robos de credenciales, publicación de información sensible, ataques a estructuras críticas, etc.

Sería imposible hablar de todos los casos en los que se han producido en los últimos años, pero para hacernos una idea de lo que estamos hablando, a continuación vamos a ver algunos de los más famosos.

I LOVE YOU (2000)

Uno de los primeros grandes ataques con malware de la historia. *I Love You* fue un gusano escrito en lenguaje VBScript, que durante el mes de mayo del año 2000 infectó a más de 50 millones de ordenadores en todo el mundo.

Se trataba de un malware que se replicaba y transmitía a través del correo electrónico de sus víctimas, eliminando archivos con unas determinadas extensiones y reemplazándolos por otros con el mismo nombre, pero con sus propias extensiones de VBScritp.

La infección se producía mediante un email cuyo asunto era "ILOVEYOU" y dentro llevaba como adjunto un supuesto archivo de bloc de notas con extensión .txt, pero que en realidad era el código en Visual Basic enmascarado. Una vez infectado el equipo, creaba varias copias del virus en el disco duro, y se reenviaba automáticamente a todas las direcciones que el usuario tenía almacenadas en su agenda.

El gusano llegó a infectar a grandes organizaciones como el Pentágono o la CIA estadounidenses, así como a un elevado número de empresas, causando graves pérdidas económicas estimadas en más de 5000 millones de dólares.

Figura 1.4. Correo electrónico con el famoso gusano I Love You

WIKILEAKS (2007)

WikiLeaks no es propiamente dicho un ataque hacker en sí mismo, sino que se trata de un portal de información donde se encuentran disponibles miles de documentos con información sensible para la opinión pública que han sido obtenidos, muchos de ellos, mediante técnicas de hacking. Esa es la razón de que aparezca en esta lista.

Comenzó su actividad en 2007, de la mano de su creador Julian Assange (entre otros), y ha ido creciendo año tras año hasta llegar a nuestros días con más de un millón de documentos alojados en sus servidores, y asegurando siempre el anonimato de quienes proporcionan la información.

Su actividad se centra en denunciar acciones éticamente reprochables de organismos y organizaciones, como gobiernos, empresas, religiones, etc. Sus mayores contenidos se han centrado en el gobierno de los Estados Unidos, especialmente en la participación de este país en las guerras de Irak y Afganistán, lo cual ha creado grandes polémicas y ha desatado importantes escándalos.

Figura 1.5. Julian Assange, uno de los creadores de WikiLeaks

STUXNET (2010)

Stuxnet es un malware que infecta sistemas operativos Windows, y cuyo objetivo es controlar sistemas SCADA (*Supervisory, Control And Data Adquisition*) que monitorizan el funcionamiento de estructuras industriales.

Fue descubierto en la central nuclear iraní de Natanz, donde ya había infectado a un millar de equipos. Tras la investigación posterior se comprobó que se había extendido a infraestructuras críticas de 13 países.

El malware fue descubierto antes de que fuera demasiado tarde, ya que de no haber sido así podría haber llegado a destruir la propia central nuclear, con consecuencias absolutamente catastróficas.

La autoría del ataque y el origen del virus nunca pudieron ser demostradas.

Figura 1.6. De no haber sido descubierto a tiempo, Stuxnet habría podido destruir la central nuclear de Natanz

PLAY STATION NETWORK (2011)

En el mes de abril de 2011, la compañía Sony recibió un duro golpe a través de este ataque a la plataforma de juegos y compras On-Line para Play Station, a través del cual los atacantes tuvieron acceso a la información almacenada en las cuentas de unos 77 millones de usuarios.

Además de la mala imagen mostrada y la gran pérdida de reputación que sufrieron, la compañía se vio obligada a mantener la plataforma cerrada durante 23 días, lo que le supuso unas considerables pérdidas de ingresos, sumadas a la multa de un cuarto de millón de libras que le impuso el *Information Comissioners Office* del gobierno de Gran Bretaña.

HEARTBLEED (2012-2014)

No se trató de un ataque en sí mismo, sino que Heartbleed (o hemorragia de corazón por su traducción al español) fue un bug dentro de OpenSSL, que hasta que fue descubierto en 2014 por el equipo de seguridad de Google, permitió a los atacantes colarse en bases de datos de multitud de sistemas para robar información contenida en ellas.

Está considerado como uno de los ciberataques más grandes de la historia, ya que se calcula que casi un 20% de los sitios web fueron víctimas de Heartbleed.

Figura 1.7. El corazón sangrante que sirve de logo para Heartbleed

YAHOO (2013-2014)

En 2014 Yahoo sufrió el robo de información de las cuentas de unos 500 millones de usuarios de la plataforma, lo que obligó a la compañía a pedir que todos ellos cambiaran sus contraseñas, aunque su información ya había sido comprometida.

Pero esto no fue lo peor, un año antes había sufrido otro ataque en el que también le fueron sustraídos los datos de sus usuarios. En un primer momento se cifraron en 1000 millones las cuentas afectadas, pero en las últimas auditorías llevadas a cabo por Verizon (su nuevo dueño desde 2017 después de hacerse con la plataforma), estas podrían haber llegado hasta los 3000 millones.

SONY PICTURES ENTERTAIMENT (2014)

Coincidiendo con el anunciado estreno de la película *The Interview*, comedia que parodiaba el régimen político de Corea del Norte, la compañía cinematográfica fue objeto de un ciberataque que paralizó sus sistemas y obtuvo de modo fraudulento gran cantidad de información clasificada, tanto de la compañía como de proyectos, trabajadores o actores.

Las pérdidas económicas estimadas que sufrió Sony llegaron hasta los 200 millones de dólares. A pesar de que todas las sospechas se centraron sobre el gobierno del país asiático, nunca se puedo probar la autoría real del ataque.

Figura 1.8. Cartel de la película The Interview, que generó el ciberataque a Sony en 2014

ASHLEY MADISON (2015)

Muy sonado fue el caso del ataque al portal Ashley Madison, cuyo cometido era el de poner en contacto a personas que querían ser infieles a sus parejas.

El grupo *Impact Team* logró hacerse con los datos de las cuentas de alrededor de 37 millones de usuarios, y amenazó a la empresa responsable de la plataforma de su publicación si no cerraban la misma. Tras no aceptar el chantaje, todos estos datos se hicieron públicos.

Esto conllevó muchos problemas a las personas que aparecían en la lista (llegando a producirse hasta casos de suicidios), aunque muchos de los que aparecían

nunca hubieran sido usuarios de la página, ya que esta no pedía ninguna prueba de verificación de los datos introducidos al crear la cuenta.

PARTIDO DEMÓCRATA DE ESTADOS UNIDOS (2016)

Durante la campaña electoral para la elección del Presidente de los Estados Unidos en 2016, un grupo de hackers consiguió entrar en los servidores del partido demócrata y robar una gran cantidad de correos electrónicos de Hillary Clinton, candidata a dichas elecciones.

Cuando estos correos fueron filtrados a la opinión pública, desataron un fuerte escándalo alrededor de la figura de Clinton, en el que llegó a intervenir hasta el propio FBI.

El final de la historia es bien conocido. Donald Trump fue elegido Presidente de los Estados Unidos de América, muy posiblemente ayudado por la pérdida de popularidad que sufrió su contrincante debido a este ataque.

Todos los indicios mostraron a Rusia como origen del ataque, consiguiendo que el propio Trump les alentara durante la campaña a seguir publicando mensajes de su rival.

El ataque se llevó a cabo mediante un correo electrónico con técnicas de ingeniería social a la cuenta de John Podesta, jefe de campaña de los demócratas para esas elecciones. A través de él se consiguió introducir un malware en los servidores que dio acceso a los mismos a los atacantes.

Figura 1.9. Imagen de John Podesta con Hillary Clinton

NETFLIX Y DISNEY (2017)

Son dos casos que no tienen relación entre sí, ni siquiera en los grupos que los han realizado, pero en los que el *modus operandi* ha sido el mismo.

Los atacantes consiguieron colarse en los servidores de ambas compañías y hacerse con contenido no publicado todavía, exigiendo grandes sumas de dinero para no hacerlos públicos en Internet antes de sus respectivos estrenos.

En el caso de Netflix se trató de la quinta temporada de la serie *Orange is the new black*, mientras que Disney sufrió el secuestro de su película *Pirates of the Caribbean: Salazar's Revenge*.

WANNACRY (2017)

Sin lugar a dudas este ha sido uno de los peores ciberataques que han sucedido, y uno de los que mayor repercusión han tenido a lo largo de todo el mundo. El 12 de mayo de 2017 este ransomware infectó a más de 360.000 ordenadores ubicados en 180 países distintos.

El virus secuestraba toda la información del disco duro, cifrando todos los archivos que encontraba en él, y propagándose a otros equipos a los que la víctima estuviera conectada por red. Para poder recuperar la información, los atacantes exigían el pago de una cierta cantidad de dinero a través de un pago mediante criptomonedas.

El ataque afectó a un gran número de organismos y empresas de todo el planeta, ocasionando unas pérdidas estimadas en más de 200 millones de euros. En España, uno de los más perjudicados fue Telefónica, quienes sufrieron la infección de gran parte de sus ordenadores y se vieron obligados a apagar toda su red para contener al virus.

Figura 1.10. Ventana mostrada en los ordenadores que habían sido infectados mediante el ransomware WannaCry

1.5 LOS HACKERS MÁS RECONOCIDOS

Al igual que ocurre con los ataques realizados a lo largo de las últimas décadas, la lista de hackers famosos es tan sumamente amplia que es imposible hablar de todos ellos aquí, por lo que vamos a hacer un breve repaso a algunos de los que más influencia o más repercusión han tenido en estos años.

JOHN DRAPER

Fue uno de los Phreakers más famosos, estudiando el funcionamiento de la red telefónica en Estados Unidos durante la década de los años 70.

Es también conocido como "Capitán Crunch" ya que, modificando un silbato de plástico que regalaban dentro de una caja de cereales de esta marca, consiguió reproducir una señal que utilizaba el sistema de AT&T pudiendo engañarlo y realizar multitud de llamadas telefónicas gratis. A partir de este estudio construyó la primera *BlueBox*, dispositivo utilizado en Phreaking que se encarga de emitir tonos a la línea telefónica.

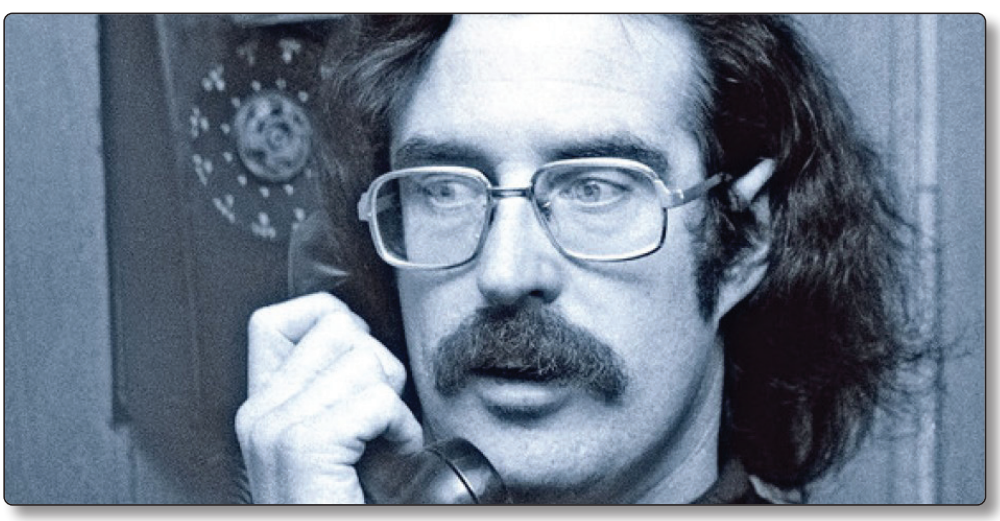

Figura 1.11. John Draper, uno de los primeros Phreakers de la historia

RICHARD STALLMAN

Formado en el Laboratorio de Inteligencia Artificial del MIT, es considerado como el fundador del movimiento *Free Software*, estableciendo las consideraciones tanto legales como morales que debe seguir el mismo.

Fue uno de los grandes actores del proyecto *GNU* y el fundador de *Free Software Foundation*, los cuales perseguían el desarrollo de un sistema operativo libre para cualquier usuario y constituirían el germen de Linux.

También fue el creador del concepto *Copyleft* que pretendía hacer frente al privativismo del Copyright. Esta idea sentaba las bases de un modo de licenciamiento para obras con derecho de autor, garantizando siempre los permisos de uso y modificación sobre ellas a todo aquel que quiera hacerlo. El desarrollo de Copyleft desembocó finalmente en la aparición de la *Licencia Pública General GNU (GPL)*, bajo la cual Linus Torvalds desarrolló su sistema operativo Linux.

Siempre ha mostrado una importante faceta activista en todo lo que respecta al acceso libre a la información y la privacidad de los usuarios, lo cual le ha llevado a verse inmerso en múltiples controversias con muchos profesionales de la informática que no comparten su misma visión filosófica radical sobre este tema.

Figura 1.12. Richard Stallman durante una de sus múltiples conferencias

KEVIN MITNICK

Sin lugar a dudas el gran gurú del hacking mediante ingeniería social. Lo veremos con mayor profundidad en el capítulo dedicado a estas técnicas.

KEVIN POULSEN

Comenzó su carrera como hacker de sombrero negro, saltando a la fama gracias a un ataque sobre las líneas telefónicas de la cadena de radio de Los Ángeles

KIIS-FM durante un sorteo para asegurarse de realizar la llamada 102 y obtener el premio, un Porsche 944 S2.

Tras realizar ataques a varios sistemas federales, fue arrestado por el FBI y condenado a una pena de 5 años de prisión y otros 3 años de prohibición de uso de ordenadores e Internet después de su salida de la cárcel.

En la actualidad, Poulsen ha reencaminado su carrera como hacker. Desde 2005 es director de la revista especializada en seguridad digital *Wired News*, tras haber trabajado antes como periodista para publicaciones de la empresa SecurityFocus.

En 2006 publicó información sobre cómo había identificado a 744 delincuentes sexuales a través de MySpace, lo que condujo al arresto de alguno de ellos.

Figura 1.13. Imagen de Kevin Poulsen

ADRIAN LAMO

Es conocido como el hacker vagabundo debido a su estilo de vida nómada, lo que le llevaba a realizar sus actividades desde redes públicas como las de bibliotecas, centros okupas o cibercafés.

Sus ataques más famosos tuvieron como objetivo las redes de Microsoft, Yahoo, Lexis-Nexis y The New York Times. Seguramente esta última es su actuación más famosa, consiguiendo penetrar en los servidores del diario e introducir su nombre en las bases de datos de fuentes de expertos que utilizaba el periódico.

Será siempre recordado por ser la persona que delató a la soldado Chelsea Manning como autora de múltiples filtraciones sobre las guerras de Irak y Afganistán y las relaciones diplomáticas de Estados Unidos, las cuales fueron publicadas en el portal WikiLeaks.

Figura 1.14. Adrian Lamo delató a Chelsea Manning por filtraciones a Wikileaks

ANONYMOUS

El colectivo Anonymous tuvo su origen entre *4CHAN* y *ForoHacker*, naciendo con un objetivo inicial puramente de diversión. Precisamente de estos foros toman su nombre, de aquellos usuarios anónimos que acceden a ellos, pudiendo expresar sus opiniones manteniendo su privacidad.

Con el paso del tiempo, grupos de usuarios se van uniendo y organizando, y su postura en Internet va tomando un cariz más activista. Son famosos sus ataques contra la Iglesia de la Cienciología, el grupo terrorista Daesh o asociaciones a favor de los derechos de autor, sus protestas contra el cierre de Megaupload, su persecución a pedófilos en Internet y su apoyo a WikiLeaks.

Actualmente es uno de los grupos de hackers más extendidos en todo el mundo, aunque no dispone de una jerarquía definida o unos líderes que lo dirijan, sino que diferentes usuarios se coordinan en un momento determinado con un objetivo común. Es frecuente, por lo tanto, encontrar personas con ideas e ideologías muy distintas que se consideren "miembros" de Anonymous, luchando cada una de ellas por algo opuesto a la otra.

Han conseguido una iconografía ampliamente extendida y reconocible. Entre sus símbolos habituales tienen como logo un personaje en traje que, en lugar de cabeza, tiene un signo de interrogación, en una clara alusión a la ausencia de líderes que caracteriza a la organización. También se asocia a este grupo el uso de la máscara de *Guy Fawkes*, tremendamente popular tras su aparición en la película *V de Vendetta*.

Figura 1.15. El hombre sin cabeza y la máscara de Guy Fawkes, referencias del colectivo Anonymous

LULZSEC

Fue un grupo formado por seis personas, que durante el año 2011 llevaron a cabo varios ataques a través de Internet, con objetivos como Sony, Fox, la CIA, el FBI, PBS, la NASA, el senado de la Unión Europea, MediaFire, etc.

Alguno de sus miembros también colaboró en acciones con Anonymous, lo cual, unido a la persecución que ya sufrían de por sí, ayudó a identificarles y arrestarles entre 2011 y 2013, lo que conllevó el final de sus acciones.

Tras pasar por prisión, varios de ellos se han "reconvertido" a hackers de sombrero blanco y en la actualidad trabajan para empresas de consultoría de seguridad informática y como consejeros de organismos públicos en esta materia.

Figura 1.16. Logotipo del grupo hacker LulzSec

FANCY BEARS

Este colectivo, también conocido como APT28 (Amenaza Persistente Avanzada 28), se dio a conocer en 2016 tras afirmar haber conseguido penetrar en los servidores de la Agencia Mundial Antidopaje.

Se presentan como un grupo de hackers que buscan un deporte igualitario, mediante las filtraciones de las irregularidades que descubren en sus actividades, aunque el mundo deportivo no ha sido el único que ha sufrido sus ataques. La Casa Blanca o la OTAN también han sido víctimas de Fancy Bears, ambas enfrentadas con Rusia al igual que la AMA, por lo que se especula que ese puede ser el origen de este grupo.

Rafa Nadal, las hermanas Williams, Simone Biles o los ciclistas Wiggins y Froome han sido algunos de los deportistas famosos que han sido acusados de dopaje desde las publicaciones de Fancy Bears, aunque nunca se haya podido llegar a demostrar la veracidad de estas informaciones.

Figura 1.17. Página de presentación del grupo hacker Fancy Bears

SHADOW BROKERS

Saltaron a la fama en el año 2016 cuando, tras hacer pública información sobre varias herramientas de hacking que, supuestamente, empleaba la NSA estadounidense para obtener información sobre los ciudadanos. Según explicaban, consiguieron hacerlo penetrando en los ordenadores de *Equation Group*, otro grupo hacker al que se relacionaba con la NSA en esos momentos, y que tendría en su poder todo este software.

Durante esta actuación se destapaba información sobre varios proyectos de espionaje a través de dispositivos inteligentes (como televisores o teléfonos móviles inteligentes) y de equipamiento de red de los principales fabricantes del mercado (CISCO, Topsec, Fortigate, etc.).

Tras esto, han intentado en varias ocasiones sacar provecho económico de la información que dicen haber obtenido de los servidores de la NSA, especialmente mediante la venta de *exploits* que permitían atacar sistemas Windows saltándose las protecciones de antivirus.

El malware usado por el famoso ransomware WannaCry, utilizaba la vulnerabilidad conocida como *EternalBlue*, la cual se dio a conocer dentro de esta filtración. Shadow Brokers emitió un comunicado posterior, negando tener nada

que ver con este ataque. El software que publicaron ha sido relacionado con otras acciones famosas, como el ataque a la NSA de Fancy Bears, el ataque en 2017 con ransomware Petya a la planta nuclear de Chernobyl, o la supuesta intervención de Rusia en las elecciones a la presidencia de los Estados Unidos en 2016.

GUARDIANS OF PEACE (GOP)

Fue el grupo responsable del ataque a Sony Pictures en 2014, en el cual se hicieron con una importante cantidad de información confidencial de la empresa, y secuestraron la red interna de la compañía.

Los empleados únicamente podían ver una pantalla de advertencia en sus ordenadores, en la que se les amenazaba con hacer pública toda esa información privada si no cumplían con las exigencias marcadas.

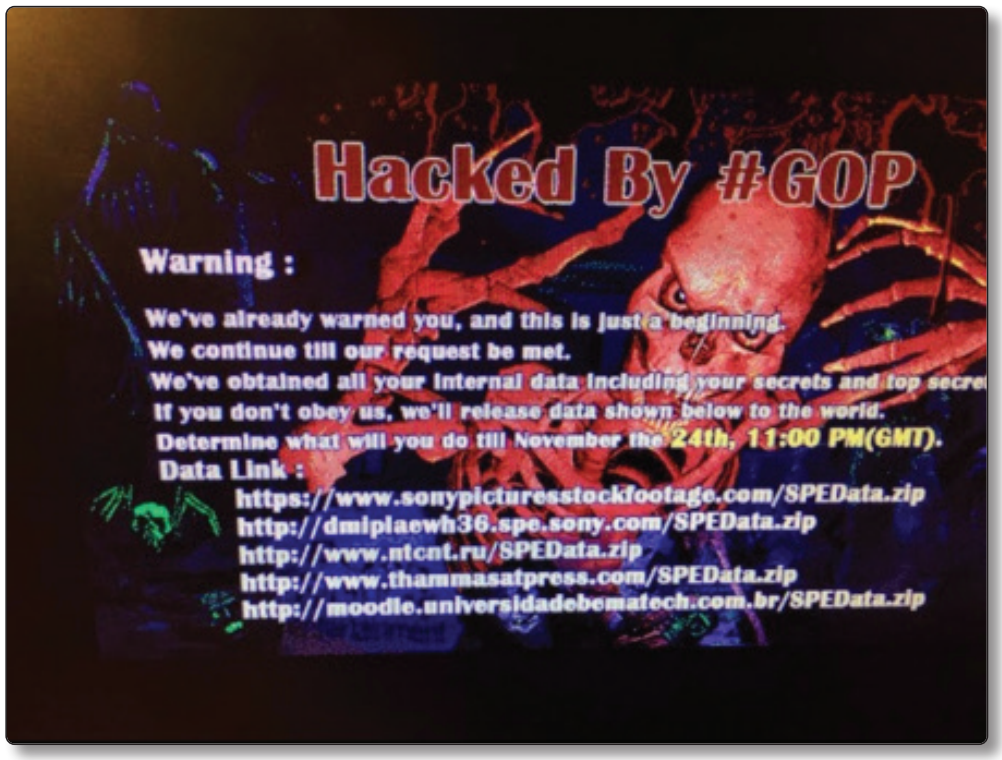

Figura 1.18. Imagen mostrada en los ordenadores de Sony durante el ataque de GOP

TARH ANDISHAN

Tras el ataque sufrido mediante el gusano Stuxnet a las centrales nucleares en Irán, surgió este grupo de unos 20 hackers relacionado con los servicios secretos de este país.

Fueron los responsables de los ataques conocidos como "*Operación Cleaver*", que tenían como objetivo infraestructuras críticas de países considerados enemigos del régimen iraní como Estados Unidos o Israel.

Fueron llevados a cabo entre los años 2012 y 2014, y toman el nombre de la palabra *cleaver*, que aparece de forma recurrente en el código de las herramientas empleadas en la operación. Buscaban el acceso a los sistemas, para una vez dentro escalar privilegios y dejar puertas traseras, creando una APT que les permitiera extraer información sensible periódicamente.

Llegaron a penetrar en los sistemas de más de 50 organizaciones a lo largo de 16 países, entre las que se incluían servicios militares, servicios de salud, aerolíneas, compañías energéticas, de comunicaciones, de transporte, etc.

Figura 1.19. Logotipo de la Operación Cleaver llevada a cabo por el grupo iraní Tarh Andishan

INCLUSO QUIEN MENOS TE LO ESPERAS

La lista de hackers famosos es sumamente amplia, como ya hemos comentado anteriormente, pero incluso podríamos llevarnos más de una sorpresa con algunos de los nombres que encontraríamos en ella. Algunos de los personajes más famosos en el mundo de la informática hicieron sus primeros pinitos en el mundo del hacking.

Por ejemplo, Bill Gates, uno de los fundadores de la empresa Microsoft, confesó haber penetrado en el sistema informático de su instituto para modificar los listados de alumnos en cada clase, de modo que únicamente tuviera chicas como compañeras y poder ligar más fácilmente. De modo decepcionante para él, su plan no tuvo el éxito esperado.

Y si el fundador de Microsoft inició su carrera como hacker, los fundadores de su principal competidor no fueron menos. Steve Jobs y Steve Wozniak, responsables ambos del nacimiento de Apple, dedicaron sus años de juventud al desarrollo (y venta) de BlueBox para realizar Phreaking, inspirados en los descubrimientos hechos anteriormente por John Draper.

Figura 1.20. Steve Jobs y Bill Gates. Dos gurús de la informática que comenzaron como hackers

1.6 ÉTICA HACKER

Se conoce como Ética Hacker a un concepto desarrollado por el periodista estadounidense Steven Levy en 1984, a través de su ensayo *Hacker: Heroes of the Computer Revolution*.

En el mismo expone los principios morales que rodean el surgimiento del movimiento Hacker en el MIT de la década de los 50, y que han acompañado a la comunidad a lo largo de estos más de 70 años de existencia.

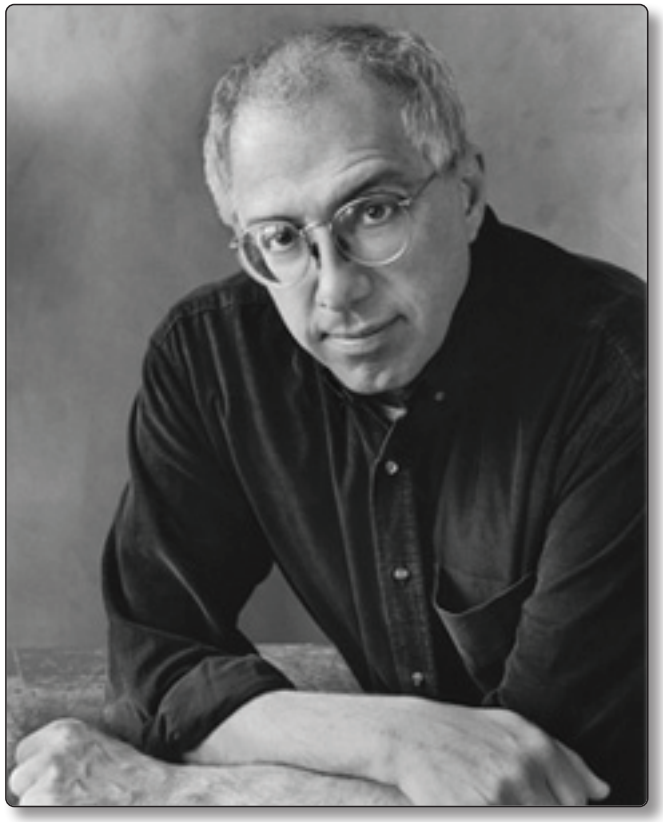

Figura 1.21. Steven Levy, autor de Hackers: Heroes of the Computer Revolution

Básicamente, la obra se apoya en una serie de valores que convergen en todos los Hackers (libertad, conciencia e igualdad social, trabajo colaborativo, lucha contra las injusticias, creatividad, curiosidad, etc.) para proyectar a través de ellos los seis postulados que conforman, desde la perspectiva de Levy, la ética por la que se rigen todos los miembros de la comunidad.

POSTULADOS DE LA ÉTICA HACKER

1. El acceso a todo aquello que pueda enseñar algo debe ser total e ilimitado, para que cualquiera pueda estudiarlo y mejorarlo en beneficio de la comunidad.
2. La información debe ser libre y accesible por todo el mundo.
3. Desconfianza de la autoridad y despliegue de una estructura descentralizada para compartir la información.
4. La única característica por la que se juzga a un Hacker es por su capacidad y sus conocimientos, no por otras razones como la edad, el sexo o la raza.
5. Se puede crear arte mediante la programación. No basta con crear un código que realice una acción, los hackers buscan que lo hagan con la menor cantidad de líneas posible, lo que ellos denominan la belleza del código.
6. Los ordenadores son una herramienta para mejorar el mundo, y como tal se los quieren mostrar al mundo. Por esta razón, el entendimiento de la tecnología es un pilar básico para su control y modificación para que haga aquello que beneficie a todos.

1.7 EL EMBLEMA HACKER

El *Glider*, o planeador de su traducción del inglés, fue el símbolo propuesto en 2003 por Eric S. Raymond como emblema que representase a toda la comunidad Hacker.

El origen de este símbolo tenemos que buscarlo en el The *Game of Life*, un famoso juego matemático desarrollado por el inglés John Horton Conway en el año 1970, el cual se componía de un autómata que mediante unas reglas establecidas marcaba las casillas de un tablero como ocupadas o como vacías en función del estado que tenían en el instante anterior dicha celda y las adyacentes.

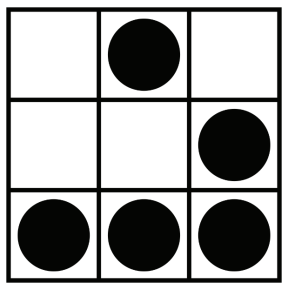

Figura 1.22. El Glider, emblema de la comunidad Hacker

Richard K. Guy fue el descubridor de este símbolo, que representa un planeador, la forma más simple de vida dentro del juego. Se desplaza de forma diagonal, es muy fácil de crear y puede ser colisionada con sí misma para crear estructuras más complejas.

Pero, ¿por qué fue este el símbolo escogido como emblema hacker? Principalmente Raymond propone el Glider porque nace al mismo tiempo que lo hacen Internet y Unix, ambos muy ligados a la cultura Hacker. Además, la aparición de este juego supuso un gran reto para los programadores de la época, quienes pasaban horas delante de sus ordenadores tratando de programar secuencias de celdas que fueran infinitas.