

Hackers

Los piratas del Chip y de Internet

Claudio Hernández

Copyright

© 1999-2000-2001 de Claudio Hernández. Todos los derechos reservados.

Este documento puede ser distribuido libre y gratuitamente bajo cualquier soporte siempre que se respete su integridad.

Queda prohibida su venta sin permiso expreso del autor.

Agradecimientos

El primer agradecimiento es siempre para esos lectores fieles, los cuales están puntualmente donde deben de estar, en su sillón favorito o en este caso delante del monitor leyendo cada una de las páginas que componen este libro. Para todos ellos, he aquí una obra que les enseñará muchas cosas. Sobre todo, conocer la nueva cibercultura y protegerse de ella...

El siguiente agradecimiento es para Kriptópolis, la mejor WEB de temas de seguridad y criptografía.

Finalmente mis agradecimientos a todos los profesionales y editores que siempre han confiado en mí, publicando todo aquello que escribo.

A todos ellos, gracias

Un reportero de la revista “ Forbes “ asegura, en el newsgroup alt.conspiracy, que un grupo de Hackers de la CIA, llamo “ la Quinta columna “, descubrió el número de cuenta de Vince Foster, presuntamente implicado en los negocios oscuros de los Clinton, se suicidó en 1995. La revista Forbes no quiso publicar la historia.

En la actualidad el Pentágono es la sede que está siendo mas atacada por los Hackers. Echelon, es la versión “ oficial “ de los Hackers aupados al gobierno por excelencia. Anualmente los Hackers desvían de los bancos, mas de 60.000 millones de pesetas hacia sus cuentas. El virus I Love You ha sido el más “ peligroso “ desde que Morrison soltara su Gusano en la ReD en 1988, contagiando mas de 6.000 sistemas de todo Internet. En la actualidad la plataforma española digital CSD, ha llegado al millón de abonados, gracias al uso de tarjetas piratas capaces de abrir los canales de esta plataforma.

Y esto es solo el principio.

Prólogo

Hakim Bey, el famoso gurú de la red que alcanzó fama -allá por los 70, recuerdo- con el desarrollo de la rebelde teoría TAZ (Zonas Autónomas Temporales) y cuyo auténtico nombre podría ser Peter Lamborn Wilson, escritor, filósofo y poeta que reside, al parecer, en algún lugar cercano a la ciudad de New York, se interrogaba -con motivo del simposio: Incidencias y disidencias. Utopías y antiutopías de la cibercultura, celebrado en la Universidad de Alicante-... Hakim Bey se decía: “he estado esperando años a que los hackers hiciesen algo y ¿dónde están?”

Aún cuando corriera el riesgo -que lo corro- de ser considerado despectivamente un triste lammer -o lamer, según- de los que se asegura no tienen ni p.i. o bien ser tachado de wannabe, siento no coincidir con Hakim, esta vez. Porque los hackers han estado, están y -modestamente pienso- estarán donde deben. Y entre otros, en Internet. Cuestionarse la ubicación intentando tracearlos es inútil. ¿Es así o no, Claudio?

Claudio Hernández - (que se sepa) - no es un hackers, ni un craker, ni tan siquiera un phreaker. Con el máximo respeto a todos debo anunciar que Claudio es, también, otro auténtico experto que viene a unirse al mundo informático. Y, para mi, todo un descubrimiento de última hora. Yo no le he conocido a través de ningún agujero, bug u hole que se precie. Tampoco he usado de backdoor alguna que pudiera servirme en un exploit. Ni ataques asincrónicos, ni las llamadas bombas lógicas. A él hay que entenderle por sus textos. Sus extraordinarios, complejos y científicos textos. Los libros que Claudio escribe no tienen firewall que impida el acceso a su comprensión, muy al contrario. Leerle no es hacer ingeniería social, ni se precisa conocer PPP, TCP/IP o UDP. Para recepcionarse en sus páginas no se hace necesario login protocolario alguno, ni asumir el rol del pirata informático. Que no. Si se me permite la expresión, aseguraría que Claudio Hernández es, tal vez, un sysop del conocimiento informático a la par que un root literario que describe a los personajes con acierto.

Kevin Mitnick, por ejemplo, es una de esas figuras legendarias que tan inteligentemente están explícitas en los textos de Claudio Hernández. Con minuciosidad, paso a paso, sin necesidad de usar superzapping, sin tener que sacar password alguna de entre las líneas ortográficas, Claudio nos narra, nos hace como un criptoanálisis del verbo en si.

En un alarde de paciente conocimiento nos va adentrando en esa pedagogía de altura casi sin darnos cuenta. Cuando lo adviertes ya estás participando de su ciencia ávidamente. Página a página. Es difícil comenzar un texto de Claudio Hernández y no leérselo de un tirón. Te entusiasma, se queda en tu mente como un caballo de troya cualquiera que hubiese madrugado para hacer trashing electrónico en tu cerebro físico. Y te cuesta olvidarle porque sus obras son magistrales.

Recomendar el libro de Claudio Hernández no es ninguna obligación, es un placer. Como pedagogo puedo aseverar con rotundidad que se aprende mucho prestando la debida atención a su contenido. Y quién sabe si, saturados de su ciencia, algún día podamos llegar a navegar por ese lado oscuro de la red y curiosamente olisquear... sin causar daño a nadie ni a nada. Porque hay que ser tan respetuosos con los demás como con uno mismo. Que quede suficientemente claro. Y a nadie le apetece ser crackeado, aparte -es obvio- de lo delictivo que supone esa tarea ilegal. Quiero terminar diciendo, como al principio, que Claudio Hernández no es ningún hackers, (ni yo tampoco) aunque... ¿Tu qué piensas de ello, querido lector?

Sinceramente creo que ha llegado el momento de marcarme un logout, lo más rápidamente posible. Pero antes del adiós informar que el libro de Claudio Hernández, por gentileza del autor, se encuentra disponible gratuitamente (entre otros lugares) en mi página web cuya url figura al pie. Hasta siempre...

Profesor J. Jesús Parras
e-mail: jparras@inforvip.es
Webmaster de La Casa de Jara
<http://www.lacasadejara.org>

Introducción

Últimamente, escribir un libro sobre Hackers se ha convertido en una labor de “clasificación” de contenidos y datos. Digo esto porque, es obvio que encontrará, a lo largo de la bibliografía sobre Hackers, libros escritos que enseñan el arte de Hackear sistemas y libros en los que se basan en historias de Hackers. El orden no es necesariamente este. Al principio, solo unos cuantos escritores como John Markoff, Steven Levi o Paul Mungo entre otros, se aventuraban a revelar algunos aspectos del Hacking. En realidad, lo que hacían, era relatar las hazañas de los Hackers. Por esta razón, solo podías saber que cosas eran capaces de hacer, pero no como se podían hacer. Eran tiempos de relatos y de historias de Hackers, pero era un buen comienzo.

A día de hoy ya es posible encontrar otro tipo de libros en los cuales te enseñan con pelos y señales las tácticas y técnicas de los Hackers. Son los nuevos escritores, en realidad Hackers convertidos a escritores, que con la excusa de escribir un manual técnico para el Administrador de Redes, revelan las técnicas maspreciadas por los Hackers. Este es el segundo paso, lo que significa que en parte, el miedo ha pasado a un segundo plano. Ahora el miedo se convierte en poder. El libro que más técnicas recopile, es el mejor. Fuera, están esperando toda una tribu de principiantes de Hacker, que patalean si no les cuentas todo. Es posible que a estos personajes les importe poco las hazañas de los demás, ellos solo quieren poner en practica las técnicas de los Hackers, y convertirse algún día, en Hackers respetados.

Sin embargo me pregunto a mi mismo, acaso no interesan las “batallitas” de los demás?. Acaso un libro que solo recopile anécdotas o historias, no es un libro realmente bueno?. Mi experiencia propia me ha demostrado dos cosas. Primero, que un libro que narra las aventuras de unos cuantos Hackers es bien aceptado dentro y fuera de los movimientos Underground. Segundo, que los libros que revelan técnicas son los mas perseguidos por esta misma comunidad, ya que están ansiosos por aprender y devorar todas las combinaciones de teclas posibles.

Estas conclusiones, me han llevado a la decisión de escribir un libro como este, el que tienen entre sus manos. Un libro que mezclara de forma hábil, historias y aspectos técnicos del Hacking. Una combinación explosiva, que permitirá mantener el interés de toda la comunidad Underground y que así se espera. Así, en este libro encontrara relatados algunas batallitas de Hackers, lo que le servirá de fuente de inspiración, al tiempo que encontrara capítulos que traten sobre temas más específicos como la Criptografía, los Virus informáticos o el Cracking. En definitiva, este es, un libro estudiado y escrito para abarcar a un mayor numero de lectores posible, desde el interesado por las nuevas tecnologías, el que quiere conocer algo mas acerca de esta explosión informática y el avezado que quiere ser Hacker de mayor.

La necesidad de escribir un libro como este era evidente. La actividad del Hacking fuera del ordenador y de la red de Internet, a cobrado fuerza y es quizás aun más peligrosa que tal como la conocemos a través de los medios de información. Sin embargo, voy a abordar en este libro todos los grados del hacktivismo, dentro y fuera del ordenador personal, dentro y fuera del espionaje industrial y en definitiva en todos sus aspectos más conocidos y los menos conocidos. Así, la clandestinidad impera por todas partes, pero no es ese el tono que elegiré en el presente libro.

El Hacking es una realidad y quiero exponer sus fundamentos. Escrito desde España, el libro quiere demostrar como el Hacking también ha hecho furor en nuestro País. Al contrario de lo que se creía, en nuestro país, el grado de piratería es superior al resto de los países de todo el mundo. Sin embargo hay que saber diferenciar lo que es la piratería y lo que es el verdadero rol del Hacking.

Cualquiera de nosotros, cuando intentamos copiar una película de video, esta atentando con la piratería. Eso no es un Hacking. Si no un grado de clandestinidad y un acto de violación de los derechos de autor. El Hacking rivalida este hecho con otra intromisión. El Hacking simplemente nació como un estado de diversión y satisfacción personal y durante muchos años a revestido diversos significados. Obviamente todos los comentarios acerca del Hacking han resultado siempre acusadores y negativos. Pero la culpa no esta en el hecho de hacer Hacking, sino en el uso que se hace de él.

Hacker es una palabra prácticamente intraducible que ha revestido, a lo largo de los años, diversos significados como ya se ha dicho. Pero parece ser que este acrónimo se vincula muy especialmente a los llamados Hacks o dicho de otra manera, así se llaman los golpes secos que efectuaban los técnicos de telefonía cuando intentaban reparar alguno de sus aparatos. Estos golpes secos recibían el nombre de " *hachazos* " o en el

argot ingles Hacks y es mas que probable que quiénes lo hacían se denominaban Hackers. De cualquier forma nunca sabremos con certeza el origen de esta palabra, pero eso hoy por hoy prácticamente da igual, ya que la mayoría de nosotros sabemos que es un Hacker según se nos muestran en los medios de comunicación.

Lo que no se nos ha dicho sobre el Hacking, es quienes son en realidad y que hacen. A menudo leer sorprendentes fechorías o trastadas que un grupo de chicos tímidos de gafas gruesas han hecho a tal o cual ordenador, es a su vez una vaga forma de camuflar el verdadero Hacking. Sin embargo hay que reconocer que eso también es Hacking, pero permítame que le diga que estamos entrando en otros terrenos que van mas allá de la especulación y el saber. Si bien es un grado de clandestinidad o delito introducirse en otro ordenador remoto, lo es también hacer una fotocopia en cualquiera de las páginas de este libro. De cualquier forma ante unas leyes nacidas por el bien de unos pocos, la mayoría de nosotros somos unos verdaderos delincuentes.

Pero quiero dejar bien claro el tratamiento que se le puede dar a este pequeño grupo de " *sabios* " antes de continuar explorando los inicios de esta nueva generación. Un Hacker es una persona, sin importancia de edad con amplios conocimientos informáticos o electrónicos que a su vez descubre la intolerancia de algunos organismos por proteger ciertas cosas o intereses. Un Hacker no solo habita en los suburbios de una gran red como lo es Internet, ni navega continuamente entre los discos duros de los ordenadores, que aunque se les conocen en estos entornos mayoritariamente, los Hackers también fisgonean sistemas fuera de una CPU. Solo tenemos que echar una ojeada a nuestro alrededor para saber cuantas cosas mas atentan contra la curiosidad.

Hacer una llamada de teléfono supone un reto muy importante para alguien que no tiene dinero, pero no es esa la intención. Sin embargo si lo que se desea es conocer bien los sistemas de conmutación de una red de telefonía inteligente, que mejor que dejarse atrapar por ella para beber de sus consecuencias. Ya en la segunda Guerra mundial se cifraban los mensajes y las comunicaciones y hoy por hoy todas las comunicaciones de los Satélites están encriptadas. Llegados a este punto un Hacker descubre que todo es una farsa y una gran manta secreta que lo oculta todo. El mundo esta lleno de misterios y de demasiados secretismos.

Sin embargo la gula se lo come todo. El hambre no se sacia y se culmina con una proeza delictiva. Violar los secretos de una comunicación convierten a uno en un Cracker, algo más devastador que un simple fisgoneo de Hacker. Como una extensión mas, surge el Carding, otro fenómeno capaz de clonar las tarjetas de crédito bancarias y

tarjetas de acceso inteligentes de canales de pago. Después se crean los Warez, programas informáticos duplicados para sobrevivir en este devastador mundo de la información.

Solo en España el uso fraudulento de estos conocimientos ha conocido un ascenso espectacular. Y en Estados Unidos el pasado año se dejaron de percibir mas de 63.000 millones de pesetas por estos conceptos. Por otro lado se estima que cada día nacen o se crean entre tres y cuatro nuevos virus informáticos y uno de cada dos estudiantes de informática entra en el ordenador de su compañero robándole el password. Todo esto es lamentable, porque la tendencia a desaprovechar las energías positivas va en aumento. Un buen conocimiento debe ser empleado para mejorar los sistemas en los que se trabaja, pero es más fácil hincharse de satisfacción con un rictus en los labios demostrando que acabas de joder un ordenador o un teléfono.

Estas son las decisiones mal intencionadas y las que más perjudican al verdadero Hacker. Una imagen borrosa sobre este personaje puede echar por la borda todo el buen saber de estas “entes”. Otro caso negro para el Hacking son los 15.000 millones de pesetas que se dejaron de percibir en Europa por el uso fraudulento de tarjetas de acceso inteligentes clonadas de los canales de televisión de pago Europeas. Un Buen Hacker no habría puesto en circulación estas tarjetas, pero si hubiera enseñado a los demás, dentro de su pequeño foro disciplinario, como funcionan este tipo de tarjetas por el mero hecho de decir lo se todo sobre ella y creo que posee un fallo...

Un bug, una codificación mediocre, son las fuentes de interés para un Hacker para mejorarlo. Una complejidad en los mecanismos de seguridad de cualquier sistema informático o electrónico despiertan en él un interés creativo. Después toma notas, las notifica y alguien hace mal uso de ellas.

Es el lado oscuro del Hacking.

Nadie es de fiar allí dentro” me refiero a Internet “ y fuera se dan los conocimientos que se quieren por un puñado de periodistas inexpertos en el tema. Después todo hace explosión en un cóctel sin sabor y todo el mundo te señala como alguien realmente perverso e irónico.

Pero hay que tener en cuenta ciertas cosas interesantes para mejorar la seguridad de los sistemas de nuestro complejo mundo. Un sistema de seguridad de por sí no tiene mucha consistencia si no es atacado por alguien de fuera. En este proceso se demuestra la fuerza del sistema. Si el intruso entra es porque existe un error en el diseño. Así, si no es por el intruso los creadores del sistema de seguridad nunca sabrían que existe un agujero

negro en su sistema. Después el intruso es sometido a un estudio y se le pide colaboración ya que normalmente siempre tendrá mas conocimientos que el propio creador y esto es porque se preocupa realmente de la seguridad del sistema. Es un reto demostrar todo lo contrario y lo consigue.

Y al contrario de lo que se pretendía, no se castiga al intruso, sino que se le contrata en la gran empresa. Esta es la política que persigue un buen Hacker. Sin embargo buenos, lo que se dicen buenos los hay bien pocos.

El mal uso de los conocimientos y el poder casi infinito que uno puede tener con ellos, en un mundo dominado por el conocimiento y la tecnología, ponen en tela de juicio cualquier intento de Hacking. Ya que hoy por hoy cualquier modificación en un fichero informático o una conmutación en un decodificador de señales de televisión, es un acto de consistente violación de los derechos de copyright.

Por ello la dominación de la tecnología es absoluta.

Hasta aquí he replanteado la posibilidad de que no todo el Hacking es malo y de que no solo los Hackers habitan en los ordenadores. Aunque es cierto que los ordenadores han popularizado enormemente a los hackers en los últimos años, no es cierto que solo habitan en ese submundo, ni tampoco es cierto que se emplean bien los conocimientos con fines científicos y no lucrativos. Por desgracia el hacking se ha convertido en el índice de un gran libro de insolencias e intromisiones peligrosas. Por lo que definir correctamente el Hacking se hace especialmente complicado.

Que aunque existen desde hace muchísimo tiempo, es ahora cuando conocen su propio acrónimo en el argot técnico y es ahora cuando la tecnología brinda la oportunidad de serlo con mas fuerza, ya que hay que reconocer que la proliferación de ordenadores personales, la red de Internet y los miles de comunicaciones encriptadas, son un gran caramelo sin saborear. Las tecnologías evolucionan y con ella los Hackers se ven forzados al limite de sus actuaciones. Fisgonear un ordenador o tratar de decodificar un canal de pago es siempre un acto delictivo, por lo que por mucho que hablemos, siempre estaremos catalogados como delincuentes informáticos y tratar de quitarse esa mascara es tarea imposible.

Hoy por hoy todo cuanto se crea, reposa sobre la base de los códigos y las encriptaciones para sacar el mayor rendimiento de la tecnología y el producto. Los programas de ordenadores son un buen ejemplo de ello. Las televisiones se han convertido en canales de pago temáticas y a la carta que requieren de sistemas complejos de encriptación y control para asegurarse una rentabilidad del canal. Los

nuevos soportes de grabación ya son digitales para todos los sistemas ya sean de vídeo, audio o datos y poseen códigos de protección contra copias piratas. A su vez todos estos soportes digitales, tales como un simple CD, DVD o Minidisc pueden estar encriptados y reducidos a un puñado de códigos que hacen de ellos una forma de pago por visión. Esto es, pagas y ves.

Ante este panorama se hace obvio que siempre habrá cierta curiosidad por " estudiar " estos códigos y estas propias tecnologías. Vivimos en un mundo de códigos, encriptaciones y rupturas de sistemas. Sin embargo como creo haber dicho ya, este fenómeno se remonta mucho tiempo atrás, desde que se emplearan las palomas como mensajeras. En cierta época los mensajes eran cifrados y convertidos a un puñado de palabras indescifrables y ya existían quienes descifraban el mensaje del enemigo. Por aquel entonces no se conocían como Hackers y ni tan siquiera estaban penalizados. Solo la llegada del ordenador ha revolucionado este sector y solo desde los ordenadores se ha hablado mucho sobre los Hackers.

Desde aquí queda poco más que contar. Podría estar contando batallitas de Hackers hasta perder el pulso de la pluma, sin embargo creo que eso sería oportuno para otra ocasión. En esta introducción me conformo con definir por encima lo que es un Hacker y especular superficialmente sobre ellos. Defenderlos o acusarlos sería caer en un grave error. Según por donde se mire sé actuaría de una u otra forma. Criticar los hechos podría ser nefasto y entraríamos en denuncias continuas que no son precisamente la ideología de este libro. Defenderlos hasta la muerte podría ser también otro error, ya que podríamos pecar de egocentrismo. De modo que solo queda exponer los hechos, o mejor dicho de otra manera, solo queda opinar y exponer mis criterios. Sentar las bases de lo que es el Hacking y explicar o mostrar los conocimientos adquiridos en un terreno complejo y difícil como es el mundo de las nuevas tecnologías, tecnología que agrupa la informática, las comunicaciones y los sistemas de pago por televisión.

Si, ha leído bien, los sistemas de pago por televisión también son el objetivo de la mayoría de los Hackers, de sobras es sabido de la existencia de Software para descodificar canales de pago. La criptografía también está presente en esta área de las nuevas tecnologías y los nuevos Hackers se especializan, cada vez mas, en el tratamiento de algoritmos y sistemas de cifrado, que tan empleados están siendo en la televisión y en la informática.

Este es, en definitiva, el mensaje que quiero haceros llegar. Ahora solo me queda decirles, que espero que disfruten con esta obra, y que aprendan tanto como yo aprendí al escribirla.

Claudio Hernández

Aguilas Noviembre 2000 - Junio de 2001

Capítulo 1

La historia de la Tecnología de hoy

Cada vez que escribo sobre la existencia de los Hackers, siempre surge la misma pregunta del millón. ¿Quién fue primero?, o al menos, cuando se inició la era del Hacker. Siempre empiezo explicando que el termino Hacker se acuñó cuando un técnico de telefonía asestaba un golpe seco al aparato de teléfono para arreglarlo, algo que habitualmente funcionaba.

Esto significa, que de ser cierto, que lo es, el termino Hacker nació en un momento en el que las computadoras eran grandes armatostes como las habitaciones de una casa victoriana. En su interior, cientos de cables se caldeaban al lado de las válvulas de vacío, lámparas mágicas se apresuraban a decir los técnicos.

Eran tiempos del Eniac, de la TX-0 o del MIT. Pero si esto es cierto, los Hackers surgieron en esa época. O quizás surgieron cuando un conocido escritor de novelas de ciencia-ficción los reflejaba en una de sus obras y ya sabéis de quien hablo. En nuestro país, el termino Hacker nació, cuando este que escribe, se decidió a coger la pluma y plasmarlos en unas amarillentas paginas.

Entonces corría el año 1990 y la televisión de pago había sido Crackeada, Internet ya existía para unos cuantos y en el kiosco apenas podías encontrar una o dos revistas de informática. ¿O eso fue después?. En cualquier caso, el principio fue eso, solo el principio de una larga historia.

1.2. Los primeros Hackers

Quien dice primero, puede estar mintiendo, pero también es cierto que parece que todos apuntan a que fueron los chicos de MIT, los primeros en acuñarse la denominación Hacker. Estos eran un grupo de alumnos del prestigioso y conocido

Massachusetts Institute of Technology (MIT), en su mayoría miembros del Tech Model Railroad Club (TMRC, Club de Modelos de Trenes) que en 1959 se apuntaron al primer curso de programación que la institución ofreció a sus alumnos, y que se enamoraron de los ordenadores y de lo que se podía hacer con ellos. Esta bella historia de amor “ tecnológica “ precipitó que los chicos pensarán de otra manera con respecto a la forma de funcionar con los ordenadores de aquellos días.

Estos ordenadores eran unos aparatos demasiado carísimos y más que descomunales que, con un poco de suerte, ocupaban salas enteras que rápidamente impregnaban con un olor a chamuscado el ambiente de la sala. Para contrarrestar esto, los enormes ordenadores necesitaban complejos sistemas de aire acondicionado que los ventilaran continuamente.

Además, estos gigantes de la informática necesitaban de una gran carga de suministro eléctrico para funcionar y subsistir, por lo que el acceso a éstos estaba realmente restringido para los estudiantes, lo que desembocaba en que en pocas ocasiones era el usuario final el que manejaba el ordenador directamente, sino que habitualmente se veía obligado a dar sus programas a los operadores, que a su vez se encargaban de introducirlos en el ordenador y de devolverle los resultados después.

Evidentemente, esto a los chicos del TMRC esto no les bastaba, y aparte de ingeniárselas para que en ocasiones les dejaran introducir directamente programas a ellos mismos y para tener tanto contacto como les fuera posible con el ordenador, no les suponía ningún problema el usarlo desde una sala de terminales a la que en realidad no tenían acceso de modo oficial colándose en ella por las noches. Lo que realmente les importaba a estos chicos, era poder usar el ordenador, sin preocuparse de las menudencias administrativas que dictaban una forma “oficial” de acceder a él.

Poco tiempo después de aquel curso llegó al MIT el TX-0, un ordenador revolucionario para la época, y el grupo de pirados de la informática del MIT tuvo la suerte de que Jack Dennis, un antiguo miembro del TMRC y ahora profesor del MIT, les diera acceso prácticamente ilimitado a esa máquina. Para ellos, una de las principales ventajas que tenía ésta era que en lugar de interactuar con los usuarios mediante tarjetas perforadas, tenía un teclado gracias al cual era posible trabajar directamente con él, lo que les permitía ver directamente el resultado de su trabajo, con lo que cada vez empezaron a pasar más y más tiempo con el ordenador y pronto eran capaces de hacer cosas con él que ni sus diseñadores hubieran creído posibles. Fue en

éste entorno y en ese momento cuando el término hacker se empezó a aplicar a aquellos pirados de la informática capaces de hacer maravillas con un ordenador.

En cualquier caso, la contribución más importante de este grupo de hackers a la historia de la informática no fue la de adoptar ese término sino la de ser los primeros en pensar diferente acerca de cómo se usaban los ordenadores y de lo que se podía hacer con ellos, y, sobre todo, la creación de una ética que regía su comportamiento que aún sigue vigente hoy en día y que todos los hackers siguen (o dicen seguir) en mayor o menor medida, sobre todo en la parte que mantiene que la información debe ser libre.

Esta historia, ha sido repetida una y otra vez, en la mayoría de los reportajes que se han escrito sobre Hackers, ya que de alguna manera se describe con certeza a los primeros Hackers o al menos, cuando se acuñó este termino. Por mi parte creo que podría ser un gran acierto, pero es evidente que no toda la historia del Hacktivismo se ha escrito todavía aun a día de hoy. Por esta misma razón decidí que este era el texto que se iba a publicar, cuando “ Bicho “ me paso un borrador de un artículo sobre Hackers, empujado por Álvaro, un gran amigo mío, que me pidió que interviniera en el proceso del reportaje.

La descripción de las hazañas de los “ locos por los ordenadores “ del MIT estaba bien narrada y además aporta un dato importante a la historia del Hacktivismo, sin embargo hay quien opina que el Hacktivismo comenzó después, ya que el Hacktivismo parece tener una relación directa con el Phreaking, en un momento en el que reinaba la Bell Telephone.

Este comienzo está bien descrito en el libro The Hacker Crackdown de Bruce Sterling, al que llama la Caza de Hackers. Entre 1960 y 1969 tuvieron algunos de los hechos más destacados en el mundo del teléfono. Dos de los artífices de estos hechos son Dennis Ritchie y Ken Thompson que curiosamente no aparecen en el libro de Sterling. Ambos, denominados dmr y Ken, crearon sus fuerzas con el legendario laboratorio de Bell. Eran unos técnicos muy cualificados, lo que en 1969 les llevo a crear importantes aplicaciones para UNIX, un elegante sistema operativo para mini computadoras, ya que así se les llamaba a los ordenadores.

Sus hazañas con los teléfonos de Bell nunca fueron publicadas, por lo que al igual que Bill Gates, se les recuerda como unos jóvenes Hackers que hicieron algo interesante para la tecnología. De igual forma, años mas tarde, gente como Bill Gates o Paul Allen hicieron algo interesante con sus conocimientos.

Sin embargo estas hazañas nunca fueron consideradas como el inicio del Hacktivismo. Según Bruce Sterling, el inicio fue cuando el 15 de enero de 1990, la centralita de larga distancia AT&T se vino abajo, dejando fuera de servicio a miles de abonados. Esto denota cierto interés por las catástrofes creadas por algunos Hackers, mas que por sus conocimientos. Sea por sus hazañas o por su afán de protagonismo, lo cierto es que ya hay un árbol genealógico de los Hackers más famosos, que de alguna manera han marcado la historia.

1.3. El árbol genealógico de los Hackers

Es difícil establecer un orden en este sentido, pero lo voy a intentar. Es obvio que Hackers, los ha habido, y muchos, mas de los que se mencionan en los diversos libros que se escriben sobre Hackers. Pero en algo se coincide en todos ellos. En que se barajan los nombres de los más importantes, o al menos, los que se han dado a conocer por sus hazañas.

En un árbol genealógico, bastante sencillo, tratare de encadenar cada uno de estos personajes. Estos hombres podrán ser considerados buenos o malos. Aquí no voy a hacer distinciones. Solo me argumentare en catalogarlos por un orden cronológico, no por sus proezas o ataques. En esto no voy a culpar a nadie.

1.4. Richard Stallman

Stallman brilla por su gran capacidad para programar. Todavía a día de hoy utiliza para trabajar, una maquina bastante antigua. Se trata de una DEC PDP-10. Stallman se integro en el laboratorio de Inteligencia Artificial del MIT en 1971, lo que le valió para crear sus propias aplicaciones de Inteligencia Artificial. Stallman, por sus trabajos, fue recompensado con el premio McArthur Genius. En la actualidad Stallman se dedica a crear miles de utilidades gratuitas para entornos UNIX. Evidentemente, no los escribe el solo, para ello creo recientemente la Fundación Free Software en la que intervienen muchísimos programadores.

1.5. Dennis Ritchie, Ken Thompson y Brian Kernighan

Estos tres mosqueteros del chip son buenos programadores y trabajan para Bell Labs. Es como si esta empresa sólo gestara buenos Hackers. Los tres están especializados en el entorno UNIX y en el lenguaje C. Estos hombres han tenido que ver, y mucho, con el nacimiento de Internet y su progreso. De no haber estado ellos en este proyecto, Internet quizás no existiría ahora, o de hacerlo, sería muchísimo más lenta.

En la actualidad Ritchie esta trabajando en el Plan 9 de Bells Labs, un sistema operativo de ultima generación que vendrá a sustituir a UNIX. Thompson y Kernighan todavía siguen trabajando como Hackers, algo que siempre les motivo a seguir viviendo con cierta ilusión.

1.6. John draper

Conocido como el capitán Crunch, este hombre fue quien descubrió que con un silbato de los cereales Crunch se podía hacer Phreaking. Este silbato curiosamente generaba un silbido a 2.600 Hertzios. Esta frecuencia es la que se empleaba para cortar los contadores de los teléfonos de Bell. Este descubrimiento llevó a John a crear la primera " Blue Box " una caja electrónica mágica para los teléfonos.

1.7. Paul Baran

Hay quien lo cataloga como el mejor Hacker de todos. Esto es solo una objeción de otro Hacker bastante conocido, Anonymous. No obstante hay que reconocer que Baran estuvo enredado con Internet incluso antes de que esta existiese como tal, por lo que los principios de Internet se deben asignar a Baran.

Baran comenzó a edificar lo que es hoy día, un Navegador. Baran tuvo un gran acierto con crear esta herramienta que a día de hoy, esta siendo utilizada por millones de internautas de todo el planeta.

1.8. Eugene Spafford

Este profesor de Informática de la universidad de Purdue, ha descubierto e impulsado a varios estudiantes realmente brillantes, entre los que destaca Dan Farmer. Spaffor es el

creador de COPS “ Computer Oracle Password and Security System “, un sistema de seguridad para Redes.

1.9. Dan Farmer

Dan Farmer participo en la creación de COPS iniciado por el profesor Stafford, dado que Farmer era el alumno de Stafford mas destacado. Finalmente COPS vio la luz en 1991 y Farmer estaba trabajando para la CERT “ Computer Emergency Response Team “ de la Universidad Carnegie Mellon.

Farmer gano la fama al desarrollar SATAN “ System Administrator Tool for Analyzing Networks “, una herramienta realmente potente que sirve para analizar los defectos y los puntos débiles de una red remota.

1.10. Mark Abene

Con el alias Phiber Optik, este Hacker es uno de los miembros fundadores del grupo " Master of deception " un grupo dedicado exclusivamente al conocimiento profundo de los teléfonos. Su primer acercamiento a la tecnología fue con un Conmodore 64 y un sistema de Radio Shack TRS-80.

1.11. Johan Helsingius

Alias Julf, es el más popular creador de correo anónimo, es decir, él fue quien creó este tipo de correo seguro a través de una cuenta llamada penet.fi. Julf se inició con un 486 con 200 megas de disco duro.

1.12. Wietse Venema

En la actualidad, este hombre trabaja en la Universidad de Tecnología de Eindhoven. Es un programador prolífico que ha recibido multitud de reconocimientos por todo su trabajo. Venema es coautor con Dan Farmer de la herramienta SATAN. Pero fue el programa TCP Wrapper, el que le lanzó a la fama. Esta herramienta de seguridad es una

de las más utilizadas en el mundo. Este programa controla y registra los paquetes que entran en una Red. Evidentemente, esto le mereció un premio a su trabajo.

1.13. Kevin Mitnick

Mitnick es la leyenda viva. Se le conoce como el cóndor. Este apodo surge por la habilidad de este, de ser el más escurridizo del FBI. Es el Cracker más famoso del mundo. Kevin comenzó sus andanzas con tan solo 10 años. Con esta edad, Mitnick fue capaz de violar el sistema de seguridad del sistema de defensa de los EE.UU. Sus principios se basan en el Phreaking, desde entonces ha violado todos los sistemas de seguridad imaginables, incluyendo los militares, empresariales o las grandes firmas.

Su obsesión por recuperar un software de OKI, le llevo a invadir los ordenadores Tsutomu Shimomura en una noche de navidad. Shimomura era también otro Hacker. Esto le llevo a la ratonera más grande jamás creada. En la actualidad Mitnick a cumplido condena y se encuentra libre, eso sí, le esta prohibido acercarse a un ordenador. Sin embargo se sabe que Mitnick actuó como asesor de seguridad contra el famoso Virus I Love You.

1.14. Kevin Poulsen

Este hombre siguió los mismos pasos que Mitnick. A Poulsen se le conoce por su gran habilidad para controlar el sistema telefónico de Pacific Bell. Una buena prueba de ello, es que Poulsen utilizo su talento para ganar un Porsche en un concurso radiofónico. Para ello intervino las líneas telefónicas, dándose prioridad asimismo. Poulsen ha violado prácticamente todos los sistemas de seguridad, pero parece que tienes mas interés en conocer los sistemas de la defensa militar. Esta filosofía le ha llevado a pasar por la cárcel, donde cumplió una condena de cinco años. En 1996 fue soltado y parece que hasta la fecha, Poulsen no ha hecho ninguna de las suyas, al menos que se conozca.

1.15. Justin Tanner Peterson

Justin Tanner es también conocido como el Agente Steal. Su habilidad haciendo cracking le llevó a conocer perfectamente las tarjetas de crédito. Pero no empleo sus

conocimientos sólo para fines educativos, ya que lo que verdaderamente le motivaba, era ganar dinero de una forma rápida y fácil. Esta falta de ética del Hacker verdadero, le llevo a una sucia jugada con el FBI para trabajar con ellos en la clandestinidad. Su colaboración con ellos, le llevo a denunciar entre otros Hackers, a Poulsen, pero al final fue incapaz de protegerse el mismo.

1.16. Vladimir Levin

Vladimir Levin, un matemático ruso de 24 años, penetra vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citibank en Wall Street. Una vez dentro, este Hacker logró transferir a diferentes cuentas de EE.UU, Rusia, Alemania, Israel y Suiza fondos por valor de 10 millones de dolares. Pero finalmente el Hacker fue detenido en 1995. En Internet es fácil encontrar un documento titulado “ Como robe 10 millones de dólares “.

1.17. Los escritores del Ciberpunk

También los escritores del Underground han tenido un antes y un después, y por supuesto un inicio. A ellos también se extiende este estudio. Un árbol genealógico nunca estaría completo sin los escritores que se encargan de resumir las actuaciones de los Hackers. Dentro de este grupo, podemos encontrar a los visionarios y los narradores de historias. De este estudio se extraen dos escritores. Se trata de William Gibson y Bruce Sterling, evidentemente no son los únicos, pero si los que han marcado un inicio.

William Gibson es el primer escritor que acuñó el término CiberPunk y que de hecho ha escrito sobre él. Su primera novela, Neuromante, esta considerada como el principio del movimiento CiberPunk. Nacido en 1948 en Myrtle Beach, South Carolina,, Gibson imagino como serian los rebeldes del futuro. Todas las visiones que Gibson ha tenido, parecen cumplirse a rajatabla. Los Hackers de hoy, son quizás, una clara imagen viva de las premoniciones de Gibson.

Pero esto era pura ficción, así que Bruce Sterling toma la pluma e introduce un nuevo concepto de literatura. Sterling escribe La caza de Hackers y describe en su obra toda una persecución de Phreakers y Hackers. Dicha obra, para tomar mas relevancia, es

publicada gratuitamente en Internet. Esta decisión, es la que ha llevado a Sterling a ser reconocido uno de los escritores mas acertados del Underground.

También el cine se ha hecho eco de la nueva sociedad CiberPunk, por un lado adaptando algunos libros de Gibson y por otro, creando todo un clásico del cine, Hackers, es el título de la película que cuenta las aventuras de un puñado de jóvenes Hackers que deben enfrentarse al FBI y al mas temido Hacker que esta del lado de la seguridad de los EE.UU. La historia esta bien lucida y ya es un clásico entre los seguidores del movimiento CiberPunk.

1.18. El cine también habla de Hackers

No podía haber dos sin tres. Primero se ha hecho un retrato del árbol genealógico de los Hackers, de una manera básica y lo más cercana posible. Después se han mencionado a dos de los escritores del ciberpunk, más conocidos. Ahora cabe recordar aquí, en unas pocas palabras, que el cine también ha dejado un hueco para estos genios de la informática.

Después de recordar que la película más popular entre la comunidad Hacker, es precisamente Hacker, cabe recordar que también existen otras películas que abordan el tema del Hacking. En este sentido cabe recordar The Net “ La Red “de Sandra Bullock, una experta en Virus informáticos que es perseguida por otros Hackers.

Pero las películas que más extrañan son sin duda WarGame “ Juegos de Guerra “ y Sneakers “ Fisgones “ las cuales dan una clara idea de lo que es un Hacker y de lo que es capaz de hacer. Finalmente cabe destacar The Matrix, una película donde se muestran los Hackers del futuro, de ser esto último cierto, ¿Es posible que el mundo este dominado algún día por los Hackers?