H4CK3RS

ÍNDICE

TECNICISMOS

- **Software:** es el conjunto de programas informáticos que permiten el funcionamiento del ordenador o que realizan tareas, como el sistema operativo, los juegos, los navegadores web, aplicaciones como Word…
- **Hardware:** es la parte física del ordenador, es decir, sus componentes electrónicos, eléctricos, mecánicos. Por ejemplo: el teclado, el ratón, la pantalla, las tarjetas…
- **Malware:** es todo aquel programa o software que se introduce en un ordenador sin el conocimiento del usuario y cuyo objetivo es dañar su funcionamiento o modificarlo para obtener información de él. Ejemplo: virus, gusanos…
- **URL:** es una secuencia de caracteres que permite localizar un recurso (documento, imagen, página web…) dentro de Internet y visualizarlo.
- **Wifi:** es un conjunto de protocolos que permite a los dispositivos electrónicos conectarse a Internet de forma inalámbrica.
- **HTML:** es un lenguaje informático que define el contenido de una página web.
- **Iframe:** es un elemento HTML que permite insertar un documento dentro de otro.
- **Firewall:** parte de un sistema o red que protege a un ordenador de posibles intrusiones de una red externa. Controla el tráfico de datos entre el ordenador e Internet.
- **VPN:** *Virtual Private Network* o Red Privada Virtual es una tecnología que permite una extensión segura de la red de área local sobre una red pública.
- **Dirección IP:** es un número único que identifica a cada equipo informático en la red.

¿QUÉ ES UN HACKER?

En la actualidad se conoce como **hacker** a una persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un software o dispositivo. Esto dista mucho del significado que tenía en los años setenta y ochenta, cuando con este término se referían a programadores brillantes y en ocasiones traviesos como **Linus Torvalds**, fundador de **Linux**; **Steve Wozniak**, de **Apple**, y **Bill Gates**, de **Microsoft,** entre otros.

AL PRINCIPIO FUERON LOS AUTÉNTICOS PROGRAMADORES

No era así como se llamaban a sí mismos. Tampoco **"hackers"** ni nada parecido; el sobrenombre "Auténtico Programador" **(Real Programmer)** no sería usado hasta el año 1980, en que uno de ellos lo hizo de forma retrospectiva.

Desde 1945, las tecnologías de la computación habían atraído a muchos de los cerebros más brillantes y creativos del mundo. Desde el primer ordenador ENIAC de Eckert y Mauchly, existió una cultura técnica de cierta continuidad, consciente de sí misma, compuesta por programadores entusiastas; personas que creaban y manipulaban software por pura diversión.

Los Auténticos Programadores provenían habitualmente de disciplinas como la ingeniería o la física y con frecuencia se trataba de radioaficionados que programaban en código máquina, ensamblador, FORTRAN y en media docena más de arcaicos lenguajes ya olvidados.

Los Auténticos Programadores constituyeron la cultura técnica dominante en el ámbito de la computación. Algunos vestigios venerados del folklore hacker datan de esta época, entre ellos varias listas de las Leyes de Murphy y el póster **"Blinkenlights"** que aún adorna muchas salas de ordenadores.

LOS PRIMEROS HACKERS

Los comienzos de la cultura hacker, tal y como la conocemos actualmente, se pueden fechar con seguridad en 1961, año en que el **MIT (*Massachusetts Institute of Technology*)** adquirió una computadora **PDP-1**, lo que atrajo la curiosidad de un grupo de estudiantes que formaban parte del **TMRC (*Tech Model Railroad Club*)** que convirtieron esta máquina en su pasatiempos favorito, inventando para ella herramientas de programación, una jerga propia y una cultura circundante que aún se reconoce a día de hoy.

La cultura en torno a las computadoras del MIT parece haber sido la primera en adoptar el término "hacker". Los hackers del **Tech Model Railroad Club** se convirtieron en el núcleo del Laboratorio de Inteligencia Artificial del MIT, el centro más destacado de investigación sobre Inteligencia Artificial de todo el mundo a principios de los 80. Su influencia se extendió por todas partes a partir de 1969, año de creación de la primera red intercontinental de alta velocidad llamada ARPANET que luego fue una de las bases de lo que hoy conocemos como Internet.

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.

TIPOS DE HACKERS

BLACK HATS

Un ***black hat*** o **hacker de sombrero negro** es un hacker que viola la seguridad informática por razones más allá de la malicia o para beneficio personal. Los ***black hats*** concuerdan con la idea que actualmente tiene la sociedad de los hackers como criminales informáticos. Los ***black hats*** entran a redes seguras para destruir los datos o hacerlas inutilizables para aquellos que tengan acceso autorizado. La forma en que eligen las redes a las que van a entrar es un proceso que puede ser dividido en tres partes:

1. **Elección de un objetivo:** El hacker determina que red irrumpir durante esta fase. El objetivo puede ser de especial interés para el hacker, ya sea política o personalmente, o puede ser elegido al azar. Luego, el hacker revisará los

puertos de una red para determinar si es vulnerable a ataques, lo cual simplemente es probar todos los puertos de una máquina anfitrión en busca de una respuesta. Un puerto se define como un medio de comunicación por el que la computadora recibe datos a través de la red. Los puertos abiertos —aquellos que respondan— le permitirían a un hacker tener acceso al sistema.

2. **Recopilación de información e investigación**: Es en esta etapa que el hacker visita o hace contacto con el objetivo de alguna manera con la esperanza de descubrir información vital que le ayudará a acceder al sistema.
   La principal forma en que los hackers obtienen los resultados deseados durante esta etapa es la de la ingeniería social. La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Los hackers utilizan esta técnica para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.
   Además de la ingeniería social, los hackers también pueden utilizar una técnica llamada recolección urbana, que es cuando un hacker, literalmente, bucea en un contenedor de basura con la esperanza de encontrar los documentos que los usuarios han tirado, lo cual le ayudará a obtener acceso a una red.
3. **Finalización del ataque**: Esta es la etapa en la que el hacker invadirá al objetivo preliminar que había planeado atacar o robar. En este punto, muchos hackers pueden ser atraídos o atrapados por sistemas conocidos como *honeypot* —trampa colocada por el personal de seguridad informática—.
   El término hacker de sombrero negro proviene de las películas del western donde los buenos llevaban sombreros blancos y los malos sombreros negros.
   Los *black hats* pueden ir desde adolescentes que esparcen virus informáticos hasta redes de criminales que roban números de la tarjeta de crédito y otra información financiera.
   Las actividades de hacker de sombrero negro incluyen plantación de programas de control de teclado para robar datos y lanzar ataques para deshabilitar el acceso a sitios web.

WHITE HATS

Un *White Hat* o hacker de sombrero blanco es un especialista en seguridad informática que entra en sistemas protegidos y redes para probar y evaluar su seguridad.

Los hackers de sombrero blanco utilizan sus habilidades para mejorar la seguridad al exponer las vulnerabilidades antes de que los hackers maliciosos (conocidos como hackers) puedan detectarlos y explotarlos. Aunque los métodos utilizados son similares, si no idénticos, a los empleados por los hackers maliciosos, los hackers de sombrero blanco tienen permiso para contratarlos contra la organización que los ha contratado.

El término sombrero blanco en la jerga de Internet se refiere a un hacker ético. Esta clasificación también incluye a personas que llevan a cabo

pruebas de penetración y evaluaciones de vulnerabilidad dentro de un acuerdo contractual.

El Consejo Internacional de Consultores de Comercio Electrónico, también conocido como *EC-Council*, ha desarrollado certificaciones, cursos, clases y capacitaciones en línea cubriendo toda la esfera del hacker ético. Además existen certificaciones como CPEH (*Certified Professional Ethical Hacker*) y CPTE (*Certified Penetration Testing Engineer*) de Mile2, que cuentan con acreditaciones de la Agencia Nacional de Seguridad de los Estados Unidos (NSA) y de la Iniciativa Nacional para los Estudios y Carreras en Ciberseguridad de los Estados Unidos (NICCS).

Pueden ser reformados black hats negro o simplemente pueden ser bien versados en los métodos y técnicas utilizadas por los hackers. Una organización puede contratar a estos consultores para hacer pruebas e implementar las mejores prácticas que los hacen menos vulnerables a los intentos de hacking malicioso en el futuro.

GREY HATS

Un *Grey hat* o hacker de sombrero gris, en la comunidad hacker, hace referencia a un hacker talentoso que a veces actúa ilegalmente, pero con buenas intenciones. Son un híbrido entre los hackers de sombrero blanco y de sombrero negro. Usualmente no atacan por intereses personales o con malas intenciones, pero están preparados para cometer delitos durante el curso de sus hazañas tecnológicas con el fin de lograr una mayor seguridad.

Mientras que los hacker sombrero blanco suelen comunicar a las empresas sobre brechas de seguridad en forma silenciosa, los hackers sombrero gris son más propensos a avisar a la comunidad hacker, además de las compañías, y simplemente observar las consecuencias. Los *grey hats* también pueden encontrar vulnerabilidades en las redes y pedir dinero a las compañías para arreglarlos.

El término sombrero gris fue acuñado por un grupo de hackers llamado L0pht en 1998. El grupo hace las referencias en una entrevista con el *New York Times* en 1999 donde describe su comportamiento de "sombrero gris". El primer uso conocido del término sombrero gris, en el contexto de la literatura de seguridad informática, se remonta a 2001.

La frase fue utilizada para describir a los hackers que apoyan la denuncia ética de vulnerabilidades directamente al proveedor de software. Esto en contraste con las prácticas de completa divulgación que prevalecían en la comunidad de sombrero blanco en el momento; y de los principios de los sombreros negros según la cual nadie debe estar al tanto de los agujeros de seguridad.

Algunos ejemplos de *grey hats* son el de abril de 2000, los hackers conocidos como "{}" y "*Hardbeat*" obtuvieron acceso no autorizado a apache.org. Ellos eligieron alertar a la gente de Apache de los problemas en lugar de tratar de dañar los servidores.

En junio de 2010, un grupo de expertos en computación conocido como *Goatse Security* revelaron una falla en la seguridad de AT&T que permitía revelar las direcciones de correo electrónico de los usuarios de iPad. El grupo reveló la falla de seguridad a los medios de comunicación después de

que AT&T había sido notificado. Desde entonces, el FBI ha abierto una investigación sobre el incidente y registraron la casa de weev, el miembro más prominente del grupo.

En abril de 2011, un grupo de expertos descubrió que el iPhone y el iPad 3G estaban "registrando" lo que el usuario visita. Apple ha publicado una declaración diciendo que el iPad y el iPhone registraban sólo las torres donde el teléfono podía tener acceso. Ha habido numerosos artículos sobre el tema y que ha sido visto como un problema de seguridad menor. Esta instancia podría ser clasificada como "sombrero gris", porque aunque los expertos podrían haber utilizado este con fines malévolos, el tema se informó.

PHREAKERS

Un *phreaker* es una persona que investiga los sistemas telefónicos, mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas.

El término *Phreak*, *Phreaker* o phreak telefónico es un término acuñado en la subcultura informática para denominar a todas aquellas personas que realizan *Phreaking*. *Phreak* es una conjunción de las palabras *phone* (teléfono en inglés) y *freak*, algo así como “pirado por los teléfonos”, y surgió en Estados Unidos en los años 1960. También se refiere al uso de varias frecuencias de audio para manipular un sistema telefónico, ya que la palabra phreak se pronuncia de forma similar a *frequency* (frecuencia). A menudo es considerado y categorizado como hacking informático. También se le denomina la cultura H/P (H de *Hacking* y P de *Phreaking*).

Entre los *phreakers* más conocidos destacan: Capitán Crunch (John Draper), empleó un silbato que regalaban con una caja de cereales de desayuno para lograr su objetivo. Dicho silbato tenía la particularidad de emitir un pitido a una frecuencia de 2.600 Hz, justamente la empleada en los sistemas de establecimiento de llamada de la compañía telefónica Bell. Siendo este el primer paso para manipular el sistema, siendo incluso posible realizar llamadas gratuitas; *The Whistler* (Joe Egressia) era un joven *phreaker* ciego que tenía oído absoluto y ya a los 9 años descubrió que silbando podía hacer cosas en el teléfono. También tenía el sobrenombre de la caja azul humana porque podía conmutar las líneas telefónicas a su antojo con simples silbidos; Steve Wozniak, uno de los creadores de Apple también tuvo un pasado *phreaker*, se dedicaba a vender cajas azules para poder financiar algunos de sus proyectos.

Durante muchos años los *phreakers* usaron las llamadas boxes, artefactos que provocaban diversas anomalías en la línea telefónica, estos dispositivos se conocen por un color identificativo.

En la actualidad, los *phreakers* tienen también como blanco a la telefonía móvil, a las tecnologías inalámbricas y el VoIP.

LAMMERS

Lamer es un anglicismo propio de la jerga de Internet que hace alusión a una persona falta de habilidades técnicas, sociabilidad o madurez considerada un incompetente en una materia, actividad específica o dentro de una

comunidad, a pesar de llevar suficiente tiempo para aprender sobre la materia, actividad o adaptarse a la comunidad que le considera un *lamer*. Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender.

Este término proviene del argot informático, relacionado con el antiguo Commodore 64 en los mediados de los años 80. Se popularizó entre los crackers y creadores de virus para Amiga gracias al más famoso y temido virus que existió jamás para los Amiga: el *Lamer Exterminator*. Este virus marcaba como sectores defectuosos los *floppy disks* que no tenían activada la protección contra escritura, y donde al mirar dichos sectores se podían leer incontables repeticiones de la cadena "LAMER!".

La divulgación posterior de este término le hizo el elegido para referirse a aquellas personas que eran consideradas sin habilidades técnicas o intelectuales en una determinada área, pero pretendían aparentar lo contrario. Luego, con la llegada de los boletines electrónicos se empezó a extender el uso de esta expresión para denominar a los incompetentes en el uso, manejo y respeto a las reglas de chats, foros y grupos de noticias; y posteriormente también usado para indicar a la persona que tiene un mal manejo de los programas y opciones del ordenador, y los que presentan pocas habilidades para jugar a los videojuegos. Igualmente, dependiendo el contexto, aparecerían también términos opuestos a *lamer*, como: *elite* o *leet*, *gosu*, etc.

De este modo, *lamer* acabó siendo el nombre estándar para aquellos considerados incompetentes frente a otras personas que sí presentarían realmente más habilidades o conocimientos sobre un tema en específico, referente a una materia, actividad, o sobre un grupo o comunidad; y/o para indicar a aquellas personas que dicen tener más habilidades o conocimientos que los que tendrían realmente. Esto a pesar de que este tipo de persona, a diferencia del *newbie*, llevaría un tiempo más que prudente para llegar a comprender el tema y/o integrarse debidamente al grupo o comunidad.

Se considera *lamer* a un usuario amateur que se jacta de poseer grandes conocimientos que realmente no posee y que no tiene intención de aprender. Es aquel que ha visitado varias páginas web sobre hacking, ha descargado algunos programas referentes al tema y creer que puede utilizarlos, con éxito o no, en su propio beneficio. Muchas veces el término se aplica a personas que desearían poder ser llamados hackers pero no han tenido un acercamiento en profundidad a la informática ni han recibido la formación necesaria. Pecan de una actitud exigente para con los creadores de software y en muchos casos irrespetuosa con usuarios expertos de comunidades de intercambio de conocimiento informático, que acaban por ignorarlos.

En foros y chats de internet, se usa para describir a usuarios novatos que se comportan siempre de forma incompetente, o por un tiempo prolongado. Se les apela en la jerga popular como "*noobs*" o "*newbies"* por otros usuarios más experimentados, aunque el segundo término se utiliza para usuarios novatos con ganas de aprender, en contraposición al primero, que tiene un tono más despectivo.

NOVATOS o NEWBIE

Newbie, *newb* o *noob* es un término de argot para un principiante o recién llegado, o alguien inexperto en cualquier profesión o actividad. El uso contemporáneo puede referirse en particular a un principiante o un nuevo usuario de ordenadores, a menudo con respecto a la actividad en Internet, como juegos en línea o uso de Linux. Puede tener connotaciones despectivas, pero también se utiliza a menudo sólo con fines descriptivos, sin un juicio de valor.

El origen del término es incierto. Los primeros usos probablemente datan de la jerga de las Fuerzas Armadas de los Estados Unidos a finales del siglo XX, aunque los posibles términos precursores son mucho más antiguos. Las formas variantes del sustantivo incluyen *newby* y *newbee*, mientras que el término relacionado *noob* (a menudo deletreado n00b) se usa a menudo en juegos en línea.

Su etimología es incierta. Puede derivar de "*newie*", que es acogido en fuentes de los EEUU y de Australia de los 1850 y significa un neófito en un lugar o una situación; Alternativamente, puede derivar de la jerga de la escuela pública británica "nuevo chico" o "sangre nueva", que se atribuye a la misma época y se aplicó a un colegial en su primer término.

En los años 1960-1970 el término "novato" tuvo un uso limitado entre las tropas estadounidenses en la Guerra de Vietnam como un término de argot para un nuevo hombre en una unidad. Su uso conocido más temprano en el Internet pudo haber estado en el grupo de noticias de Usenet: *talk.bizarre*. Se cree que el término entró en uso en línea en 1981.

SCRIPT KIDDIES

Script Kiddie es un anglicismo propio de la jerga de Internet que hace alusión a una persona falta de habilidades técnicas, sociabilidad o madurez.

Considerada un incompetente en una materia actividad específica o dentro de una comunidad.

A pesar de llevar suficiente tiempo para aprender sobre la materia, actividad o adaptarse a la comunidad que le considera un *Script Kiddie*.

Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender.

Es un término despectivo utilizado para describir a aquellos que utilizan programas y scripts desarrollados por otros para atacar sistemas de computadoras y redes. Es habitual asumir que los *script kiddies* son personas sin habilidad para programar sus propios *exploits*, y que su objetivo es intentar impresionar a sus amigos o ganar reputación en comunidades de entusiastas de la informática sin tener alguna base firme de conocimiento informático. Suelen tener intenciones maliciosas al igual que los *lamers*.

A diferencia de los *lamers*, los *script kiddies* usan siempre programas ajenos o *scripts* y los *lamers* pretenden ser expertos y se comportan como tales aunque no tienen esos conocimientos y no tienen intención de aprenderlos.

TIPOS DE HACKING

PHISHING O SUPLANTACIÓN DE IDENTIDAD

Esta técnica recibe su nombre de la palabra inglesa *fishing*, que significa pescar, ya que se basa en utilizar “cebos” para obtener información.

Consiste en contactar con una persona a través de un canal de comunicación, normalmente un correo electrónico, haciéndose pasar por una empresa conocida en un intento de engañar a dicha persona. Su objetivo es conseguir que esta revele información personal y así poder suplantarla.

Lo más común es que contengan un enlace que envíe a la persona a una página web falsa parecida a la de la empresa por la que se hacen pasar. Allí les pedirán introducir contraseñas, números de cuentas bancarias… y otros tipos de información que la empresa ya tiene, con alguna excusa como renovar las bases de datos o para ingresar algún tipo de premio que han recibido por ser clientes.

Una vez que la persona ha introducido sus datos, la página web los guardará y el timador podrá verlos y robarlos. El phishing es una de las formas más comunes de hacking, ya que es mucho más fácil que una persona caiga en este engaño por su cuenta que intentar romper las defensas de su ordenador.

Algunos tipos de phishing son fáciles de detectar, ya que se ve claramente que son falsas y que no pertenecen a una empresa real. Sin embargo, algunos están muy bien hechos y contienen el logo e información de la empresa a la que suplantan, incluso usando diferentes tipos de técnicas para que su URL sea parecido o igual al de la empresa real.

Ejemplo de phishing: En 2003 se produjo un caso de phishing a gran escala, en el que un gran número de personas recibió un correo de un timador que se hacía pasar por eBay comunicándoles que su cuenta iba a ser suspendida si no actualizaban los datos de su tarjeta de crédito en el

enlace que se les mostraba. Como se ha dicho antes, se puede crear una página web que tenga un gran parecido a la real, por lo que este timo afectó a muchas personas.

Cómo defenderse: Los métodos de defensa son muy parecidos a los de ingeniería social: no pinches en enlaces desconocidos, busca la supuesta empresa que te está contactando por tu cuenta, borra correos de spam, etc.

INGENIERÍA SOCIAL

Aunque la ingeniería social no se usa exclusivamente en ataques informáticos, es una de las técnicas de hacking más exitosas. Consiste en manipular al usuario de un ordenador para que revele información confidencial. Aunque el tipo de información que se pretende descubrir varía, lo más común es que se pidan contraseñas o cuentas bancarias, o incluso se recurra a engañar a las personas para acceder a su ordenador y robar información desde allí. La ingeniería social se utiliza a menudo ya que es más sencillo que les des la información que buscan por la confianza que generan en ti que buscar las debilidades de tu ordenador para hackearlo.

Tipos de ataques a través de la ingeniería social:

Correo electrónico de un amigo: si se consigue la contraseña de una persona (ya sea por ingeniería social o por otro tipo de hacking) se consigue también acceso a la lista de contactos de esa persona, y probablemente a otros tipos de redes sociales ya que la mayoría de las personas usan la misma contraseña para varias cuentas. Una vez que se tiene la cuenta de correo electrónico bajo control, se envían correos a todos los contactos de esa persona o se publican mensajes en las páginas de sus amigos. Estos mensajes pueden:

- Contener un enlace que produce curiosidad: normalmente tendrán un título o comentario que te hará pinchar en ellos, y estarán infectados con algún virus que permitirá al hacker acceder a tu ordenador y volver a repetir el ciclo.
- Contener una descarga: pueden ser imágenes, vídeos, música, películas… que tienen un virus que infectará tu ordenador si descargas el archivo enviado (algo probable ya que al ser un amigo no te produce desconfianza).

Estos mensajes suelen tener un pretexto o historia que los hace más creíbles en caso de que el usuario desconfíe, por ejemplo:

- El amigo que te ha enviado el enlace está de viaje y debido a diferentes causas (robo, pérdida de la cartera, poca planificación…) necesita que le envíes dinero al lugar del enlace.
- Tu amigo te pide que ayudes a una causa benéfica de la que forma parte, siguiendo las instrucciones del enlace.

Solución a un problema del que no has informado: El hacker puede hacerse pasar por el trabajador de una empresa a la que perteneces, ofreciéndote ayuda para solucionar el "problema que tenías". Aunque no les hayas contactado antes por un problema, probablemente tengas alguno, así que aprovechas la oportunidad para solucionarlo. El "representante de la empresa" te pedirá que te identifiques dándole tus datos, que le des acceso a tu ordenador para que pueda solucionarlo o que introduzcas algún

comando o programa necesario, pero que en realidad le dará acceso a tu sistema.

Crear desconfianza: Empieza normalmente ganando acceso a una cuenta de comunicación de alguien que pertenezca a un chat público, foro o red social. El hacker entonces podrá alterar mensajes o información privada, ya sean imágenes, vídeos… a través de técnicas de edición básicas para que sean ofensivas y creen odio en las personas que las reciben. La información alterada será enviada a los sitios públicos a los que pertenece el verdadero usuario, haciendo parecer que se envió accidentalmente o como amenaza de algún tipo. Esto perjudicará la imagen de la persona que supuestamente la ha enviado, y probablemente servirá de chantaje para que el hacker consiga dinero o información a cambio de borrarla.

Cómo defenderse:

1. Lee los correos con detenimiento: el atacante pretende asustarte y darte una sensación de urgencia para que no te pares a pensar sobre la seguridad.
2. Investiga el correo: si te han mandado un mensaje supuestamente de tu compañía, no contactes por correo. Busca el teléfono de su compañía por tu cuenta y llámales desde allí.
3. Borra las peticiones de información financiera o personal: una verdadera compañía no te pedirá que mandes un mensaje por correo electrónico con contraseñas.
4. Rechaza ofertas de ayuda de compañías: las empresas reales no te contactarán personalmente para asistirte sin que les hayas notificado antes. Tampoco respondas a las peticiones de ayuda de organizaciones benéficas que no conoces, si quieres donar busca una organización conocida y manda el dinero a través de su página oficial.
5. No pinches en los enlaces para que te lleven a una página: si quieres ir a la página de la que te hablan, búscala por Google u otro motor de búsqueda.
6. No confíes en correos sospechosos incluso si te los ha mandado alguien que conoces: actualmente el robo de una cuenta de correo electrónico es relativamente común, por lo que si recibes un mensaje con un enlace desconocido pregúntale a la persona que supuestamente te lo ha mandado antes.
7. Ten cuidado con las descargas: si no conoces a la persona que te la ha enviado o no estás esperando un archivo suyo no lo descargues.
8. Pon tus filtros de spam altos.
9. Protege tus aparatos electrónicos: instala antivirus, *firewalls*, filtros de correo electrónico…

PHREAKING

Se denomina *phreaking* al hacking de sistemas telefónicos, con el objetivo de manipular los teléfonos para hacer llamadas gratis o para escuchar las conversaciones de un móvil. Se realiza mediante unos aparatos electrónicos llamados “cajas”, que interfieren en el funcionamiento normal de las líneas telefónicas ya sea emitiendo tonos audibles que generan funciones de cambio o manipulando componentes eléctricos de la línea. Algunos ejemplos son:

- La caja azul: Era un generador de tonos que simulaba el sonido de marcación de número de las operadoras de telefonía. Replicaba los tonos usados para cambiar llamadas a larga distancia, lo que permitía hacer llamadas gratis. Hoy en día no funciona en la mayoría de países, ya que el tono ahora se transmite de forma digital y a través de un canal al que el usuario no puede acceder. Se llama así porque el primer aparato de este tipo que se confiscó era de ese color.

- La caja negra: Al ser conectada a un teléfono fijo permitía que la llamada fuera gratis. Esto es posible porque la empresa de telefonía empezaba a cobrar cuando detectaba un descenso de voltaje en la línea. La caja negra colocaba un resistor en serie con la línea, por lo que el voltaje antes de recibir la llamada era lo suficientemente bajo como para descolgar el teléfono, pero no lo suficiente como para que la compañía empezara a cobrar.

- La caja roja: Se utilizaba para hacer llamadas gratis en cabinas telefónicas. Genera el sonido de monedas al ser insertadas, engañando al sistema haciéndole creer que se había pagado. El sonido que hacían debía variar según el país, ya que no todas las monedas tenían la misma frecuencia.

- La caja dorada: Servía para crear una conexión entre dos líneas telefónicas. Se coloca la caja en la línea con la que quieres conectarte y después llamas a esa línea, siendo “contestado” por la caja. Entonces se crea una unión entre ambas. Cuando esto sucede se puede situar la llamada en la línea afectada aunque no haya sido hecha desde allí. Esto es utilizado cuando se quiere hacer llamadas gratis o de broma.

  En la actualidad la mayoría de estos aparatos ya no funcionan, pues la tecnología de los sistemas telefónicos ha cambiado. Sin embargo, aún se producen ataques de phreakers a través de softwares y virus que afectan al teléfono y que son más peligrosos que los métodos antiguos.

  ### WATERHOLE

  El objetivo de estos ataques es infectar a un grupo de personas introduciendo virus u otro tipo de malware en páginas web que suelen ser visitadas por algún miembro del grupo. Normalmente van dirigidos a miembros de grandes empresas, como Apple o Microsoft, ya que cuando un usuario es infectado el hacker tiene acceso a su ordenador. Su nombre está inspirado por los depredadores (hackers) que acechan cerca de zonas de agua (páginas web) esperando una oportunidad para atacar a su presa (usuario).

  Cómo defenderse: lo principal es informar a los miembros de tu empresa o grupo de estos tipos de ataques, sobre todo a aquellos que tienen acceso a información privilegiada. Pídeles que se instalen algún tipo de antivirus o programa similar que evite gran parte del malware posible de estas páginas. También se pueden monitorizar las cien páginas más visitadas por lo empleados y examinarlas en busca de virus o código maligno. Si se detecta alguno, bloquea el tráfico a esta página web y alerta a los usuarios. Si el problema continúa, contacta con el creador de la página e infórmales de él.

  Ejemplo de un ataque waterhole: Unos hackers subieron unas cuantas docenas de herramientas de administración a páginas web populares, que fueron descargadas y usadas por cientos de miles de usuarios que administraban páginas web. Una de las más descargadas fue una consola de administración de páginas web, otra muy popular fue un contador de visitantes. Las dos tenían una URL simple que cargaba un logo junto con la aplicación.

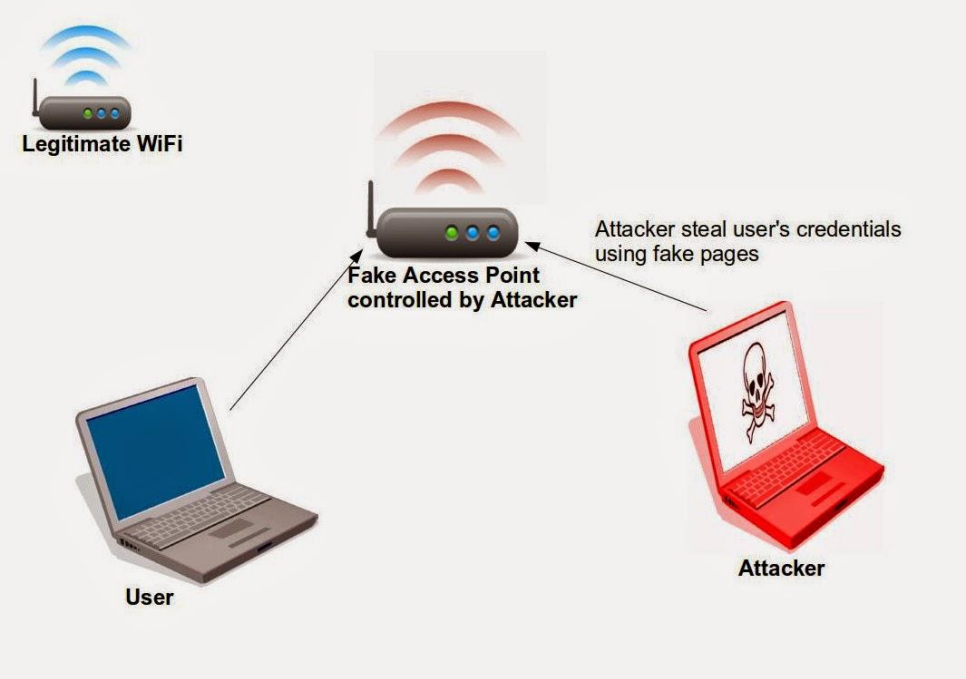
  El contrato del autor decía que cualquiera podía modificar la aplicación si lo necesitaba, mientras que la URL no se cambiara de ninguna forma. Después de varios meses los hackers redirigieron el sitio web al que llevaba la URL del logo a un link de JavaScript que engañaba a los usuarios para que instalaran malware. Así, todas las personas que instalaron estas aplicaciones fueron infectadas.

PUNTO DE ACCESO INALÁMBRICO (WAP) FALSO

Este tipo de hacking es relativamente sencillo, pues solo requiere una pieza de software y una tarjeta de red inalámbrica. Esta técnica se realiza en sitios públicos con wifi, donde el hacker creará una conexión wifi pública propia. Esta conexión tendrá un nombre parecido a la real, de forma que las personas la confundirán pensando que es la original y se conectarán a ella.

Cuando esto suceda, la wifi falsa te pedirá que introduzcas un nombre de usuario y una contraseña. La persona que creó la red falsa usará estos datos y los introducirá en redes sociales y otros sitios web famosos asumiendo que utilizas la misma contraseña y usuario en diferentes lugares.

Aunque a primera vista no parezca muy peligroso, mucha gente usa los mismos datos siempre, por lo que el hacker podría acceder a correos electrónicos que contengan información más privilegiada.



Cómo defenderse:

- La mejor defensa es verificar siempre la wifi real con algún empleado del local o lugar en el que estás, preguntando cuál es el nombre de su red.
- Suponiendo que no puedas hacerlo por cualquier motivo usa una contraseña y usuario diferentes a las que suelas usar. Además, desactiva la opción de conectarse automáticamente a una red.
- Ten cuidado si de repente te desconectas de la wifi a la que estabas conectado, especialmente si no has sido el único al que le ha ocurrido. Algunas aplicaciones son capaces de desconectarte de tu red actual, y el atacante la usará esperando que te reconectes a su wifi falsa.
- Si una red está interfiriendo con tu red privada virtual (VPN) y forzándola a cerrarse, no te conectes a ella. La VPN es una gran defensa contra este tipo de ataques ya que encripta todos los datos que envíes a esa red, por lo que aunque introduzcas tus datos el atacante no podrá verlos.

ATAQUES DE DÍA CERO (0day exploits)

Estos tipos de ataques se aprovechan de un punto débil en la seguridad de un programa que todavía no ha podido ser solucionado, llamado vulnerabilidad día cero (*0day*). Recibe este nombre porque no pasan días desde que se descubre el error y sucede el primer ataque informático.

Normalmente cuando alguien descubre un fallo en el software notificará a la compañía de él. Así, la compañía puede arreglar el código del programa y crear un parche o actualización para los ordenadores de los usuarios. Sin embargo, se corre el riesgo de que alguien con malas intenciones lo descubra o se entere de él antes de que se pueda solucionar. Si esto sucede, es probable que esa persona cree algún virus que afecte a ese fallo y produzca consecuencias mayores como un bloqueo del ordenador.

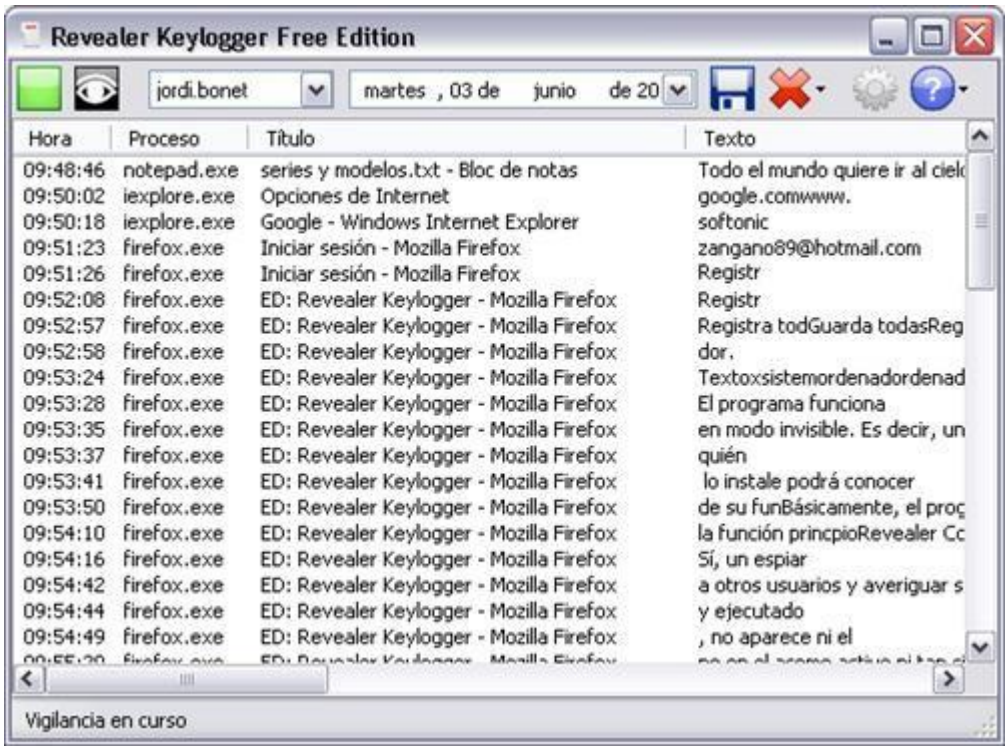
En ocasiones, estas vulnerabilidades “se venden” en el mercado negro, donde hackers pagan para que sea revelada. Es uno de los tipos de hacking más peligrosos ya que no se puede usar ningún tipo de protección para el malware que el hacker haya creado aprovechándose del fallo en el código hasta que el creador sea capaz de arreglarlo, incluso si se está al corriente de él.

Ejemplos de ataques de día cero: El más famoso ocurrió conjuntamente con ataques Stuxnet, un gusano informático que tenía el objetivo de sabotear el programa de armas nucleares de Irán. En este caso, el gusano que se aprovechaba de cuatro vulnerabilidades día cero que afectaban a varias versiones de Windows fue enviado a una instalación nuclear israelí dentro de varios USB. Se cree que estos fallos se vendieron por unos tres millones de dólares en el mercado negro.

KEYLOGGERS

Son un tipo de software o dispositivos hardware que se encargan de registrar las teclas pulsadas en el teclado y guardarlas en un fichero o enviarlas por Internet. Aunque la mayoría de las veces que se usa es con fines ilegales, también es usada por autoridades y empresas como herramienta de vigilancia o por padres que quieren estar al tanto de las actividades en Internet de sus hijos ya que adquiere la información del usuario sin que este lo note. Hay muchas variantes de *keyloggers*, pero los dos tipos principales son:

- De software: es parte de otros tipos de malware como virus o troyanos. Es el tipo más fácil de instalar en un ordenador porque no es necesario estar en contacto con él, sino que se puede instalar remotamente. Su función aparte de guardar las teclas pulsadas es escanear los ficheros con estos datos buscando tipos específicos de texto, como números, y descargarlos a un servidor. Esto facilita la búsqueda de, por ejemplo, números de cuentas bancarias. Muchas veces los *keyloggers* se combinan con otros tipos de software con funciones similares, como programas que guardan capturas de pantalla.



- De hardware: no son tan utilizados como los de software, ya que son más difíciles de instalar (el hacker debe haber estado en contacto con el ordenador) y son fácilmente detectables. Se tratan de dispositivos USB o falsos conectores que se encuentran entre el cable del teclado y el ordenador.

Cómo defenderse:

- Usa un firewall: la mayoría de las veces un *keylogger* tiene que transmitir la información obtenida a una tercera persona, por lo que debe usar Internet. Aunque un examen del uso de tu red puede revelar un *keylogger*, no se puede contar como una manera de evitarlos. El ancho de banda que usan estos programas es prácticamente indetectable, por lo que la única manera fiable de detectar el envío de datos es con un *firewall*. Estos programas monitorizan la actividad del ordenador y al detectar un programa intentando

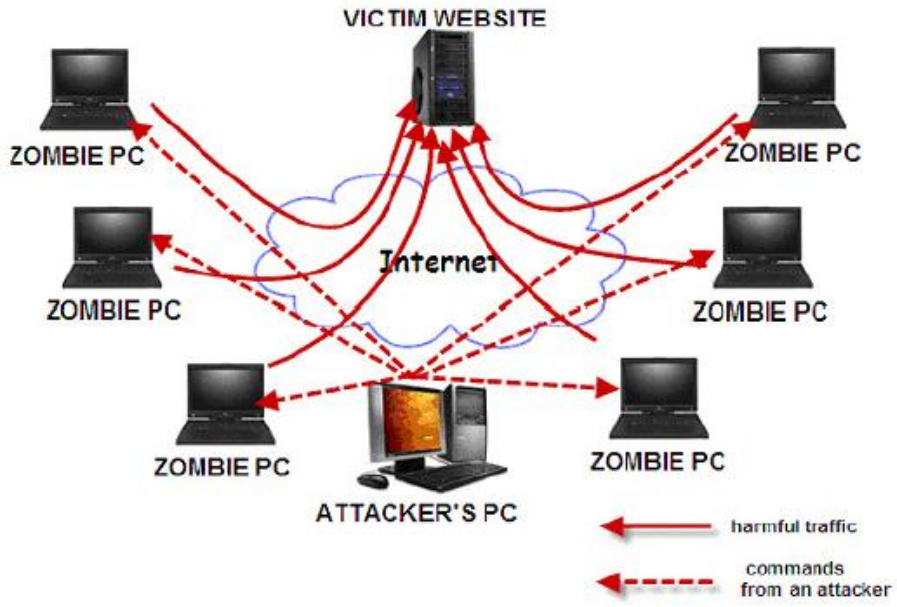
enviar datos te pedirá validación o mandará una advertencia. Algunos *firewalls* tienen la opción de bloquear la entrada y salida de datos completamente.

- Instala un administrador de contraseñas: los *keyloggers* sólo registran lo que has escrito, por lo que al tener una opción de auto rellenado no serán capaces de registrar tu contraseña. Muchas veces al poner una contraseña en una página web te preguntará si quieres guardarla. Si dices que sí, la próxima vez que entres se auto rellenará.
- Mantén tu software actualizado: los *keyloggers* se aprovechan de alguna vulnerabilidad de tu ordenador para instalarse. Las compañías de Internet están continuamente actualizando sus programas para resolver estos fallos, así que actualizar tu software a menudo podría evitar que seas atacado en un futuro.

DDOS (Distributed Denial of Service) y redes zombis

Este ataque, en español llamado ataque distribuido de denegación de servicios, consiste en usar gran cantidad de ordenadores para acceder a una página web al mismo tiempo y sobrecargar los servidores, provocando que deje de funcionar durante un período de tiempo. Cuando un ordenador quiere acceder a un servidor le envía un "paquete", que es respondido con otro de parte del servidor. Sin embargo la cantidad que puede recibir es limitada, y si se supera este límite el servidor se ralentizará o parará.

La persona que pretenda realizar este ataque debe controlar cientos de miles de ordenadores, algo que consigue mediante las redes zombis (redes de ordenadores infectadas por un troyano y que el hacker puede controlar remotamente).

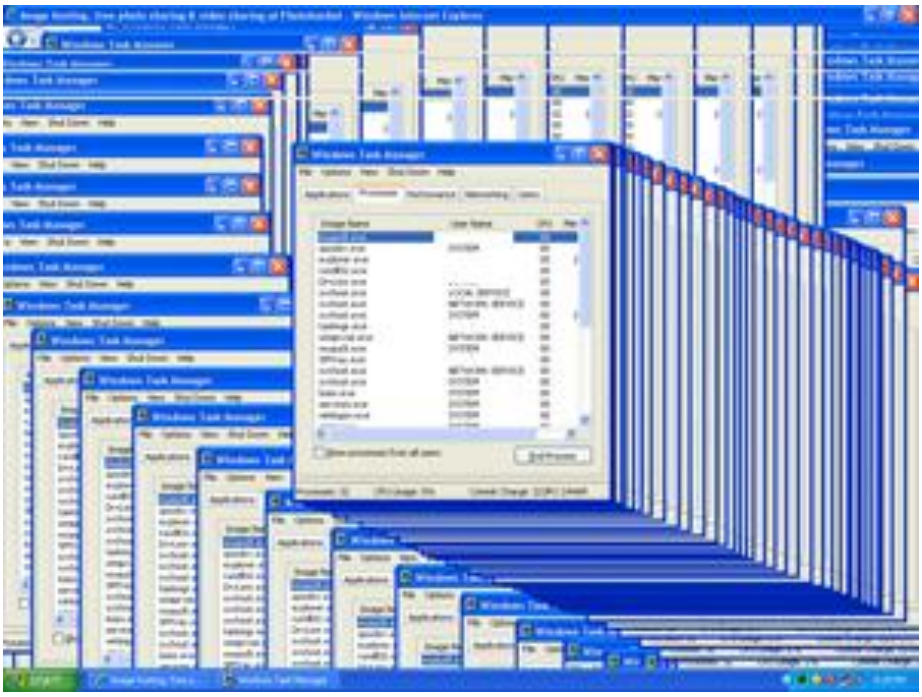


De esta forma los usuarios de los ordenadores no saben que están participando en el ataque, haciendo prácticamente imposible encontrar al verdadero culpable. El objetivo de estos ataques suelen ser páginas comerciales como Amazon, ya que si sus servidores dejan de funcionar pierden grandes cantidades de dinero. En menos ocasiones se atacan páginas informativas de algunas instituciones como medio de protesta.

VIRUS, TROYANOS y GUSANOS

Todos estos términos se refieren a tipos de malware, normalmente usados en conjunto con otras técnicas de hacking:

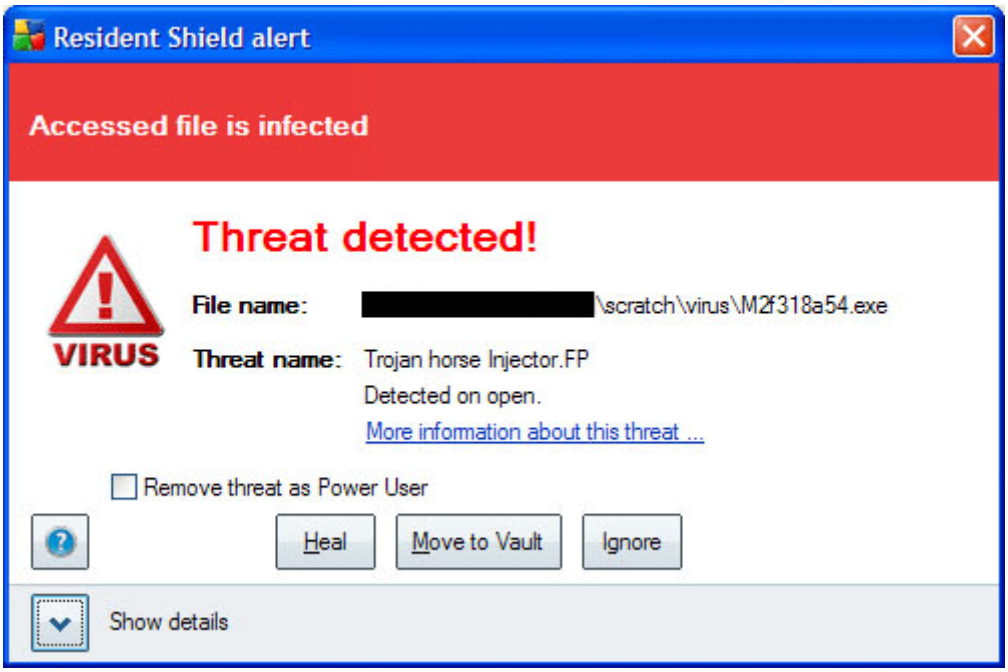
- **Virus:** Estos programas tienen la función principal de infectar tantos ordenadores como les sea posible. Para ello infectan archivos que se encuentran en dispositivos USB, discos duros, CD-ROM o cualquier otro medio de almacenamiento disponible los cuales transmitirán esos virus a cualquier otro equipo que entre en contacto con ellos.



Los virus pueden tener consecuencias muy variadas, tanto en el software como en el hardware:

  - Software: puede alterar el funcionamiento de programas y archivos, ralentizar el sistema, robar datos personales, saturar las redes…
  - Hardware: puede dañar el disco duro, sobrecalentar el microprocesador, dejar inservible el chip BIOS…

- **Troyano:** Los troyanos son un tipo de malware cuyo principal propósito es dar acceso remoto a un sistema. Igual que el mítico caballo que usaron los griegos para introducirse en Troya sin levantar sospechas, estos programas tratan de pasar lo más desapercibidos que puedan, abriendo una puerta trasera para que un atacante remoto se introduzca en el ordenador. Mediante otros tipos de hacking como la ingeniería social el atacante te engaña para que te instales el troyano, haciéndolo pasar por un software inofensivo.



Hay varios tipos:

- **De puerta trasera:** Permite al atacante acceder a tu ordenador, dándole total control sobre él. Puede borrar y crear archivos, instalar programas, cambiar el código interno del ordenador…
- **Rootkits**: Su objetivo es encubrir actividades o programas del ordenador, normalmente las del propio troyano, para evitar ser descubiertos.
- **Botnets**: Crean redes de ordenadores zombis y los utilizan para enviar spam o hacer ataques DDOS.
- **Ransom**: Modifica los datos de tu ordenador para impedir que accedas a ciertos programas o archivos. El atacante suele pedir algún tipo de recompensa a cambio de "liberar" al ordenador del troyano.

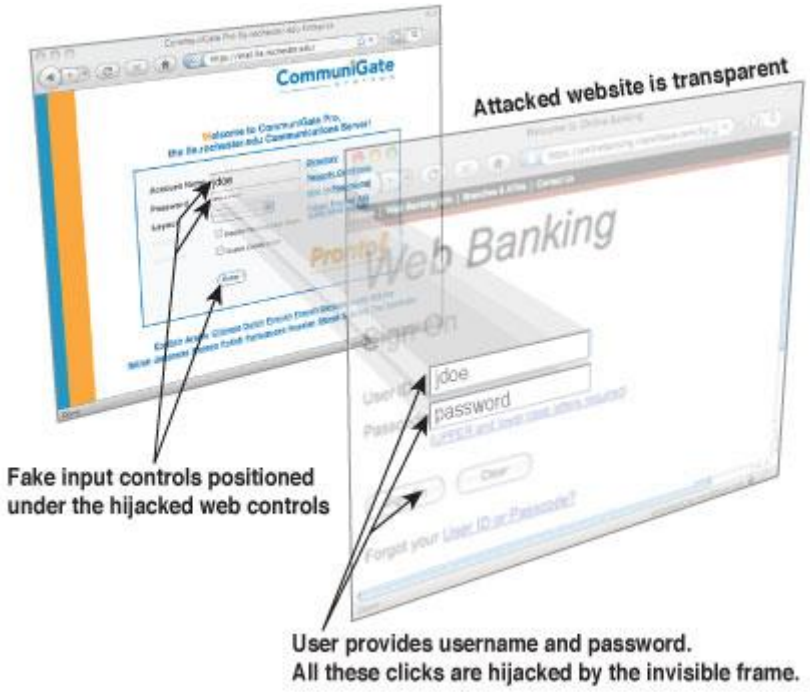
- **Gusano:** Es un programa que se copia a sí mismo a través de la red. Es similar a un virus, a excepción de que el gusano puede funcionar por sí mismo sin necesidad de un programa host que lo contenga.

Es una de las formas de malware más peligrosas, ya que a diferencia de otros softwares maliciosos los gusanos pueden acceder a tu ordenador sin que tú hagas nada. Por ejemplo un virus necesitará que pinches un enlace o te descargues un ejecutable para poder infectarte, mientras que el gusano buscará vulnerabilidades en tu ordenador para poder acceder a él y volver a replicarse mandándose a IP aleatorias hasta que encuentre otra con algún fallo que le permita infectarla.

CLICKJACKING

Consiste en engañar al usuario que visita una página web haciéndole creer que está pinchando en una enlace, anuncio… cuando en realidad está pinchando en una página web cargada dentro de un iframe invisible puesto encima.

Por ejemplo, cargando una página con un virus encima de un anuncio de viajes en una página web cualquiera, cuando el usuario quiera pinchar en el anuncio en realidad estará haciendo click en el iframe invisible que le llevará a la página maliciosa con el virus. Este tipo de ataque es muy común y se encuentra a menudo en Internet, sobretodo en páginas web para ver series y películas online.



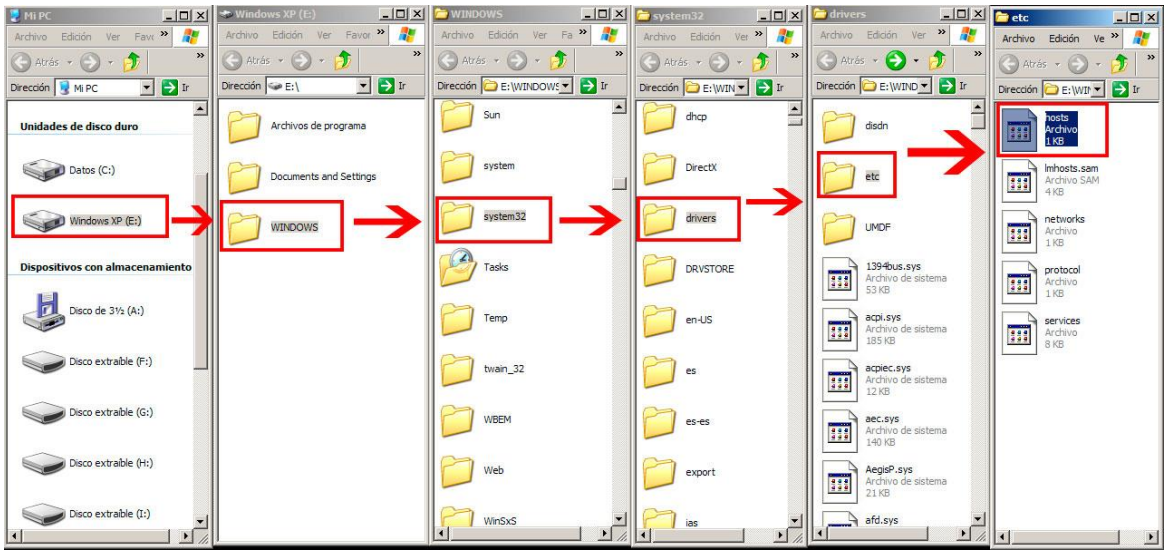
Cómo defenderse: si eres el usuario, puedes descargarte programas como *Ad-Block* o *NoScript*, que eliminarán estos iframes y evitarán que pinches en ellos. Si eres el creador de la página web en los que estos iframes han sido introducidos puedes usar la función X-FRAME, que no permitirá que haya ningún tipo de páginas cargadas dentro de iframes.

MANIPULACIÓN DEL ARCHIVO HOSTS

Es un archivo de texto sin extensión que se encuentra en una carpeta del sistema operativo.

Aunque no parezca muy importante, es imprescindible para poder conectarse a Internet, ya que Windows necesita este archivo para ver la dirección IP del ordenador y de esta forma establecer la conexión de red. Esto es necesario cada vez que visitamos una página web o pinchamos en un enlace, lo que convierte este archivo en objetivo de hackers.

El archivo hosts se encuentra en **C:\Windows\System32\drivers\etc** o en **C:\Windows\System32\Drivers\etc**, dependiendo de la versión que tengas.



Este archivo puede ser modificado por malware que haya podido entrar a tu ordenador, lo que puede causar el re-direccionamiento de la navegación a páginas web seleccionadas.

Cuando esto sucede y el usuario se da cuenta, intentará solucionarlo accediendo a Internet para instalar un antivirus o buscar soluciones en foros de ayuda, sin embargo esto le será imposible debido a que la manipulación de su archivo Hosts le impedirá efectuar una conexión.

Cómo defenderse: tener instalado un antivirus evitará que adquieras malware que pueda afectar a tu archivo Hosts. En caso de que haya sido modificado, se deben seguir estos pasos:

- Accede a la carpeta con el archivo hosts y elimínalo.
- Entra en el Bloc de notas y haz un nuevo documento de texto, a continuación copia dentro: 127.0.0.1 localhost
- Cierra el documento, guarda los cambios y nómbralo hosts. Asegúrate de que no tenga ninguna extensión de archivo.
- Haz clic derecho en el archivo creado y en Propiedades marca la casilla de solo lectura, después dale a aceptar.

También existen aplicaciones que sustituyen el archivo Hosts existente por uno nuevo parecido al predeterminado, usarlas también solucionará el problema.

TRUCOS CON FICHEROS

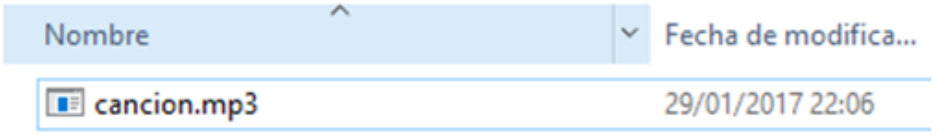
Muchos hackers utilizan diferentes trucos relacionados con ficheros de los sistemas operativos para engañar a los usuarios y hacerles creer que programas maliciosos son ficheros inocentes, para lograr de esta manera que los usuarios los ejecuten y así poder introducir virus u otros malwares en sus ordenadores.

Ejemplos de trucos con ficheros:

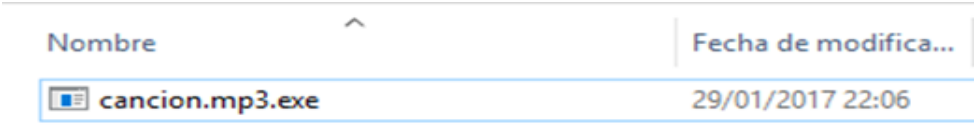
Aprovecharse de la configuración por defecto de las aplicaciones del sistema:

Por defecto el explorador de Windows viene configurado para ocultar las extensiones de los ficheros. De esta manera es posible enviarle un fichero ejecutable cuyo nombre esté especialmente formado para engañar al usuario, por ejemplo **canción.mp3.exe** o **foto.jpg.exe.** Si el usuario tiene el ordenador configurado por defecto verá el fichero como **canción.mp3** o **foto.jpg** lo que podría hacer que lo ejecutara sin percatarse del peligro que corre.

Así se ve el fichero en un explorador configurado por defecto



Así se ve el fichero en un explorador bien configurado



Aprovecharse del orden de ejecución de los ficheros ejecutables:

El sistema operativo Windows lleva incorporado una serie de reglas a la hora de ejecutar aplicaciones que datan de la época de los primeros sistemas operativos de Microsoft por temas de compatibilidad. Si dos aplicaciones tienen el mismo nombre pero las extensiones son **.COM** y **.EXE** Windows le da prioridad a la extensión **.COM .**

Un atacante puede utilizar esta peculiaridad para hacer que un usuario ejecute primero el malware creyendo que está ejecutando un programa legal.

El sistema operativo Windows cuenta con diferentes extensiones ejecutables. Para conocer su orden de ejecución basta con ejecutar el comando **echo %PATHEXT%** en una consola de comandos.

```
C:\Users\carla>echo %PATHEXT%
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
```

Manipular nombres y extensiones de ficheros utilizando caracteres Unicode:

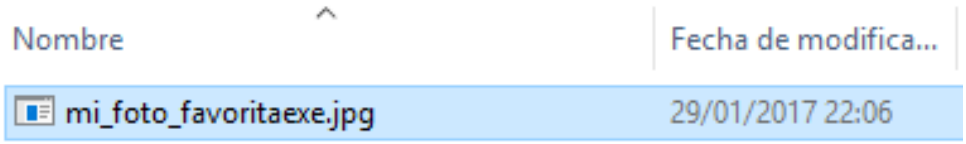
Unicode es un estándar de codificación de caracteres diseñado para facilitar el intercambio de información entre múltiples lenguajes, para lograrlo existen caracteres Unicode especiales que realizan diferentes acciones que los atacantes pueden utilizar.

Uno de estos caracteres es el "Reemplazar Derecha a Izquierda" **(Código Unicode U+202E)** cuya función es cambiar la dirección del texto de derecha a izquierda para soportar lenguajes con una orientación diferente como el árabe. Esto significa que si en un texto insertamos este caracter los siguientes caracteres se escribirán de manera invertida. Por ejemplo si nombramos nuestro fichero de esta manera:

mi_foto_favorita[U+202E]gpj.exe

En el explorador aparecerá como

mi_foto_favoritaexe.jpg



Engañando de esta manera al usuario, haciéndole creer que está ante un fichero inofensivo. Hay que notar que en las últimas versiones del Sistema Operativo Windows el antivirus que trae incorporado impide la utilización de este truco.

GOOGLE DORKS

Consiste en realizar diferentes combinaciones de búsquedas en Google para encontrar información que las personas han publicado inconscientemente, normalmente fotos, vídeos, DNI, documentos con contraseñas, etc.

Esta información se hace pública porque Google es capaz de indexar una gran cantidad de tipos diferentes de archivos que estén en un directorio Web que pueda ser listado, y una vez que esto suceda cualquier persona puede acceder a esta información utilizando ciertas palabras claves y operadores de google en el buscador.

Por ejemplo utilizando esta búsqueda (inurl:/mjpg/video.mjpg) podemos encontrar diferentes cámaras web que están emitiendo de forma pública ya sea de manera consciente o simplemente por un error de configuración.

Ejemplo de búsqueda

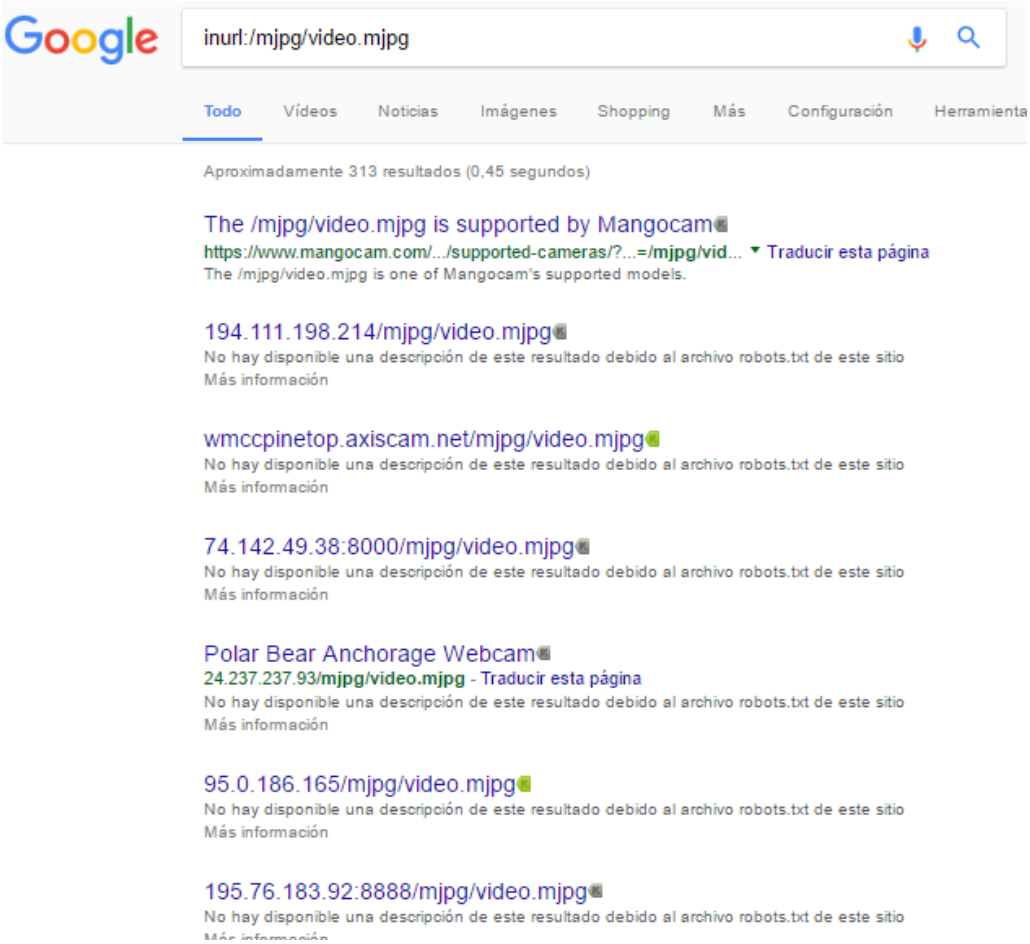
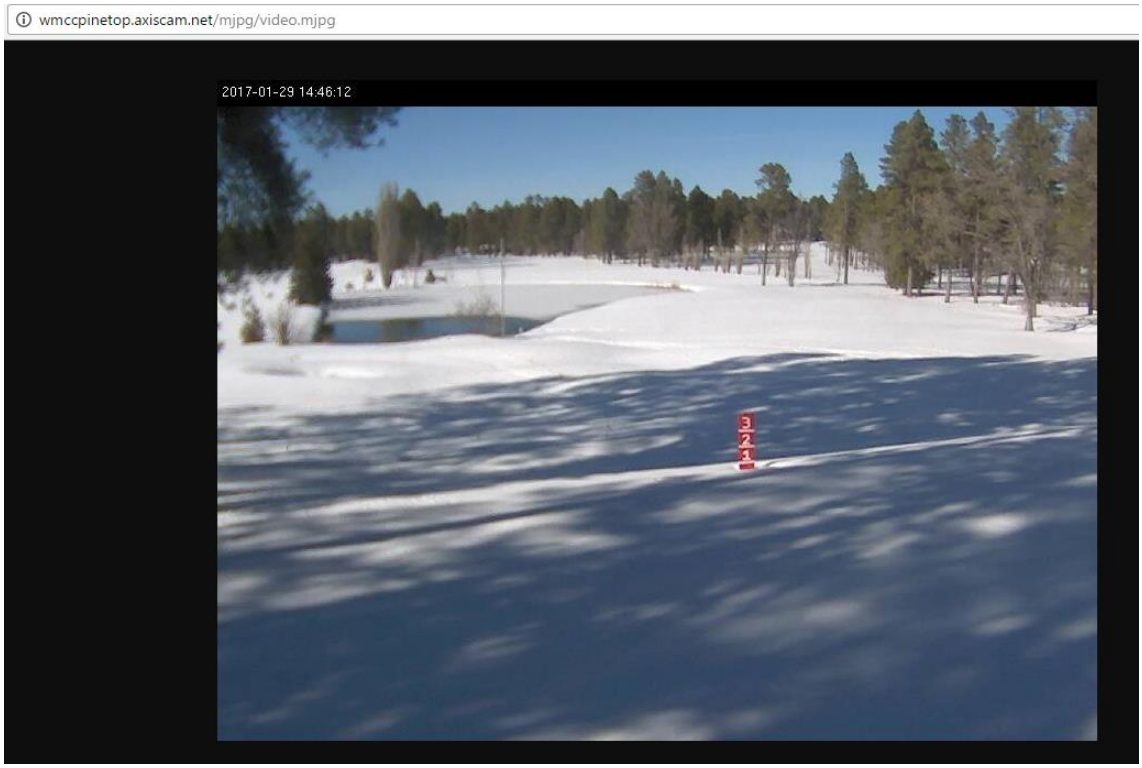


Imagen de una de las cámaras encontradas:



No solo es posible encontrar dispositivos que no se encuentren correctamente configurados, sino que con esta técnica los atacantes pueden encontrar información confidencial como fotos privadas, datos personales (teléfono, dirección, contraseñas, número de DNI) entre otros.

EXTRACCIÓN DE DATOS EXIF DE IMÁGENES

EXIF es la abreviatura de ***Ex**changeable **I**mage file **F**ormat*. Es un estándar creado para almacenar metadatos en las fotos hechas con cámaras digitales. Esto significa que las fotos pueden incorporar información relativa a la propia imagen (Tamaño, Tipo, Colores, etc.) o a como ha sido tomada (Tipo de cámara, Apertura del diafragma, Tiempo de obturación, Coordenadas GPS, etc.)

Ejemplo de algunos de los metadatos que pueden ser incorporados a una imagen

Properties - EXIF		
File		
Comment		Comentarios editables con programas
Camera		
Make	Canon	Fabricante
Model	Canon EOS 400D DIGITAL	Modelo cámara
Orientation	Upper Left	Orientación
Image		
Image description		Descripcion de la imagen (editable)
Artist		Artista (editable)
Copyright		Información del copyright (editable)
Exposure time	1/1600 s	Tiempo de obturación
F-number	f/5	Apertura de diafragma
Exposure program	Aperture priority	Modo de disparo (Av)
ISO speed ratings	100	Sensibilidad
Date/time original	07/04/2007 14:42:17	Fecha y hora del disparo
Exposure bias value	0.00 EV	Nivel de exposición
Metering mode	Pattern	Método de medición de luz (matricial)
Flash	Flash did not fire, compulsory flash mode	Flash
Focal length	50 mm	Distancia focal
User comment		
Colorspace	sRGB	Espacio de color
Pixel X dimension	3888	Ancho de la imagen
Pixel Y dimension	2592	Alto de la imagen
White balance	Manual white balance	Ajuste de blancos
Scene capture type	Standard	Modo del disparo (estandar)
Miscellaneous		
Exif version	2.21	
FlashPix version	1.0	
Canon Maker Notes		
Firmware version	Firmware 1.0.4	Versión de firmware
Owner name	Jesus Rodriguez Martin	Propietario
Camera serial number	7C59-0275B	Número de serie del cuerpo

Lo que en principio parecía una buena idea, ha sido utilizado por hackers y atacantes para localizar a sus víctimas, gracias a que la mayoría de los teléfonos móviles traen activado por defecto la geolocalización de las fotos tomadas con las cámaras del dispositivo.

Así cuando una persona envía una foto tomada desde un dispositivo con la geolocalización activada, está enviando las coordenadas GPS exactas del lugar donde fue tomada dicha foto.

Pero no solo los hackers utilizan está técnica. El FBI capturó a un hacker gracias a que siempre dejaba una foto de los pechos de su novia en los sitios que atacaba. En esta foto iban incrustadas las coordenadas de su domicilio, lo que facilitó a las fuerzas del orden su captura.

PRINCIPALES HACKERS

Los hackers suelen tener mucha repercusión mediática y algunos que realizan hallazgos o proezas importantes se vuelven famosos, estos son algunos de estos hackers:

JONATHAN JAMES

Jonathan James fue un hacker estadounidense, famoso como el primer joven enviado a prisión por delito cibernético en Estados Unidos. Se suicidó en 2008 de un disparo.

Entre el 23 de agosto de 1999 y el 27 de octubre de 1999, James cometió una serie de intrusiones en varios sistemas, incluyendo los de BellSouth y el sistema escolar de Miami-Dade.

Sin embargo, lo que lo llevó a la atención de las autoridades federales fue su intrusión en las computadoras de la *Defense Threat Reduction Agency*, una división del Departamento de Defensa de los Estados Unidos, cuya función principal es analizar amenazas potenciales a los Estados Unidos de América, tanto en el país como en el extranjero.

James más tarde admitió a las autoridades que había instalado una puerta trasera no autorizada en un servidor de computadora en Dulles, Virginia, que utilizó para instalar un *sniffer* que le permitió interceptar más de tres mil mensajes que pasaron a los empleados de DTRA, junto con numerosos nombres de usuario y contraseñas, incluyendo al menos 10 en computadoras militares oficiales.

Más tarde se reveló que el software preciso obtenido era el código fuente de la Estación Espacial Internacional que controlaba elementos críticos de mantenimiento de la vida. Según la NASA, "el software apoyaba el entorno físico de la Estación Espacial Internacional, incluyendo el control de la temperatura y la humedad dentro del espacio vital". Esta intrusión, cuando se detectó, hizo que la NASA cerrara sus computadoras durante tres semanas, con un costo de $ 41,000 para verificar y arreglar sus sistemas.

James fue condenado a seis meses de arresto domiciliario y libertad condicional hasta la edad de dieciocho años, y se le pidió que escribiera

cartas de disculpa a la NASA y al Departamento de Defensa. También se le prohibió el uso de computadoras para fines recreativos. James más tarde violó esa libertad condicional cuando probó positivo para el uso de drogas y luego fue puesto bajo custodia por el Servicio de Alguaciles de Estados Unidos y voló a un centro correccional federal de Alabama, donde finalmente sirvió seis meses.

El 17 de enero de 2007, la cadena departamental TJX fue víctima de una invasión masiva de sistemas informáticos que comprometió la información personal y crediticia de millones de clientes. El mismo anillo de hackers también cometió intrusiones en el *BJ's Wholesale Club*, el *Boston Market*, *Barnes & Noble*, *Sports Authority, Forever 21*, DSW, *OfficeMax* y *Dave & Buster*, y supuestamente hizo un millonario fuera del grupo Albert González. Aunque negó haber hecho algo, James -que era amigo de algunos de los hackers involucrados- fue investigado por el Servicio Secreto, que allanó las casas de James, su hermano y de su novia.

El 18 de mayo de 2008, Jonathan James fue encontrado muerto en su ducha con una herida de bala autoinflingida en la cabeza. Su suicidio aparentemente estaba motivado por la creencia de que sería procesado por crímenes que no había cometido. "De verdad, no tenía nada que ver con TJX", escribió James en su nota de suicidio, "No tengo fe en el sistema de justicia. Tal vez mis acciones de hoy y esta carta enviarán un mensaje más fuerte al público. De cualquier manera, he perdido el control sobre esta situación, y esta es mi única forma de recuperar el control".

KEVIN MITNICK

Kevin David Mitnick (nacido el 6 de agosto de 1963) es un consultor estadounidense de seguridad informática, autor y hacker, más conocido por su detención de alto perfil en 1995 y más tarde cinco años en prisión por varios delitos informáticos y relacionados con las comunicaciones.

La persecución, el arresto, el juicio y la sentencia de Mitnick junto con el periodismo, los libros y las películas asociados eran polémicos.

Ahora dirige la empresa de seguridad *Mitnick Security Consulting*, LLC, que ayuda a probar las fortalezas de seguridad de las empresas, sus debilidades y posibles lagunas. También es Director de Hacking de KnowBe4, así como miembro activo de la junta asesora de Zimperium.

A los 13 años, Mitnick utilizó la ingeniería social y el buceo de basura para evitar el sistema de tarjetas perforadas utilizado en el sistema de autobuses de Los Ángeles. Después de convencer a un conductor del autobús de que le dijera dónde podía comprar su propio boleto para "un proyecto escolar", pudo montar en cualquier autobús en el área de LA usando boletos de

transferencia no utilizados que encontró en un basurero junto a la compañía de autobuses garaje. La ingeniería social se convirtió posteriormente en su principal método de obtener información, incluyendo nombres de usuario y contraseñas y números de teléfono de módem.

Mitnick primero obtuvo el acceso no autorizado a una red de computadoras en 1979, a los 16 años, cuando un amigo le dio el número de teléfono para el *Ark*, el sistema informático *Digital Equipment Corporation* (DEC) utilizado para desarrollar su software de sistema operativo RSTS / E. Ingresó a la red informática de DEC y copió su software, un crimen del que fue acusado y condenado en 1988. Fue condenado a 12 meses de prisión seguido de tres años de libertad supervisada. Cerca del final de su liberación supervisada, Mitnick invadió las computadoras del correo de voz de *Pacific Bell*. Después de que se emitiera una orden de arresto, Mitnick huyó, convirtiéndose en fugitivo durante dos años y medio.

Según el Departamento de Justicia de los Estados Unidos, Mitnick obtuvo acceso no autorizado a docenas de redes informáticas mientras era un fugitivo. Utilizó teléfonos celulares clonados para ocultar su ubicación y, entre otras cosas, copió el valioso software propietario de algunas de las compañías de telefonía celular e informática más grandes del país. Mitnick también interceptó y robó contraseñas de computadoras, alteró las redes de computadoras y rompió y leyó mensajes de correo electrónico privados.

Después de una búsqueda bien publicitada, el FBI arrestó a Mitnick el 15 de febrero de 1995, en su departamento de Raleigh, Carolina del Norte, por delitos federales relacionados con un período de 2 años y medio de piratería informática que incluía computadoras y telefonía. Lo encontraron con teléfonos celulares clonados, más de 100 códigos de teléfono celular clonados y múltiples piezas de identificación falsa.

Mitnick fue acusado de fraude telefónico (14 cargos), posesión de dispositivos de acceso no autorizados (8 cargos), interceptación de cables o comunicaciones electrónicas, acceso no autorizado a una computadora federal y daño a una computadora.

Desde el año 2000, Mitnick ha sido consultor de seguridad pagado, orador público y autor. Realiza consultoría de seguridad para las empresas *Fortune 500* y el FBI, realiza servicios de pruebas de penetración para las compañías más grandes del mundo y enseña clases de ingeniería social a decenas de compañías y agencias gubernamentales.

ROBERT MORRIS

Robert Tappan Morris (nacido el 8 de noviembre de 1965) es un informático y empresario estadounidense. Él es el más conocido para crear el gusano de Morris en 1988, considerado el primer gusano de ordenador en Internet.

Morris fue procesado por liberar el gusano, y se convirtió en la primera persona condenada bajo la entonces nueva Ley de Fraude y Abuso de Computadoras. A continuación, co-fundó la tienda online *Viaweb*, una de las primeras aplicaciones basadas en la web, y más tarde la firma de financiación *YCombinator*, ambas con Paul Graham.

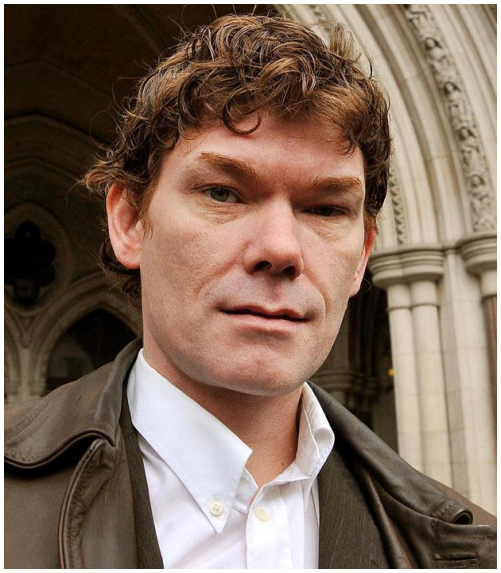
Más tarde se unió a la facultad en el departamento de Ingeniería Eléctrica y Ciencias de la Computación en el Instituto de Tecnología de Massachusetts, donde recibió la tenencia en 2006.

El gusano de Morris fue desarrollado en 1988, mientras que era un estudiante graduado en la universidad de Cornell. Dijo que fue diseñado para medir el tamaño de Internet. Soltó el gusano desde el MIT.

El gusano estaba programado para verificar cada computadora que encontrara para determinar si la infección ya estaba presente. Sin embargo, Morris creyó que algunos administradores podrían tratar de derrotar a su gusano instruyendo a la computadora a reportar un falso positivo. Para compensar esta posibilidad, Morris ordenó al gusano que se copiara de todos modos, el 14% del tiempo, sin importar la respuesta a la interrogación sobre el estado de la infección.

Este nivel de persistencia fue un defecto de diseño: creó cargas del sistema que no sólo lo trajeron a la atención de los administradores del sistema, sino que también interrumpieron los equipos de destino. Durante el ensayo que siguió, se estimó que el costo en "pérdida potencial de productividad" causada por el gusano y los esfuerzos para eliminarlo de diferentes sistemas oscilaban entre $ 200 y $ 53,000.

GARY MCKINNON



Gary McKinnon (nacido el 10 de febrero de 1966) es un administrador de sistemas escocés y un hacker que fue acusado en 2002 de perpetrar el "mayor hack de ordenadores militares de todos los tiempos", aunque el propio McKinnon afirma que estaba simplemente buscando pruebas de supresión de energía libre y un Encubrimiento de la actividad OVNI y otras tecnologías potencialmente útiles para el público. El 16 de octubre de 2012, después de una serie de procedimientos judiciales en Gran Bretaña, la Secretaria del Interior, Theresa May, retiró su orden de extradición a los Estados Unidos.

McKinnon fue acusado de hackear 97 computadoras militares y NASA de Estados Unidos durante un período de 13 meses entre febrero de 2001 y marzo de 2002, en la casa de la tía de su novia en Londres, usando el nombre 'Solo'.

Las autoridades estadounidenses declararon que eliminó los archivos críticos de los sistemas operativos, que cerraron la red del Distrito Militar del Ejército de los Estados Unidos de Washington de 2.000 computadoras durante 24 horas. McKinnon también publicó un aviso en el sitio web del ejército: "Su seguridad es una mierda". Después de los atentados del 11 de septiembre de 2001, eliminó los registros de armas en la Estación Naval de Armas de Earle, haciendo que su red de 300 ordenadores inoperables y municiones paralizantes suministraran entregas para la Flota Atlántica de la Marina de los Estados Unidos. McKinnon también fue acusado de copiar datos, archivos de cuenta y contraseñas en su propia computadora. Las autoridades estadounidenses afirmaron que el costo de seguir y corregir los problemas que causó fue de más de $ 700,000.

Las autoridades estadounidenses afirmaron que McKinnon estaba tratando de minimizar sus propias acciones. Un alto oficial militar del Pentágono dijo al *Sunday Telegraph*: "La política de Estados Unidos es combatir estos ataques con la mayor fuerza posible, como resultado de las acciones del Sr. McKinnon, sufrimos graves daños. Los daños deliberados a las computadoras militares y de la NASA y dejó mensajes tontos y anti-América.Toda la evidencia era que alguien estaba realizando un ataque muy serio contra los sistemas informáticos estadounidenses".

ANONYMOUS

Anonymous (anónimo o anónimos en español) es un seudónimo utilizado mundialmente por diferentes grupos e individuos para realizar en su nombre

—Poniéndose de acuerdo con otros— acciones o publicaciones individuales o concertadas. Surgidos del *imageboard* de 4chan y de Foro Hackers en un comienzo como un movimiento por diversión, desde 2008 *Anonymous* se manifiesta en acciones de protesta a favor de la libertad de expresión, de la independencia de Internet y en contra de diversas organizaciones, entre ellas, *Daesh*, *Scientology*, servicios públicos, consorcios con presencia global y sociedades de derechos de autor. En sus inicios, los participantes actuaban solamente en Internet, pero entretanto desarrollan sus actividades también fuera de la red.

Puesto que no existe una jerarquía, resulta en general difícil confirmar la autenticidad de las noticias o informaciones referentes a *Anonymous*. Asimismo, debido al anonimato, sucede que un único individuo puede producir noticias falsas e introducirlas como supuestamente auténticas del colectivo *Anonymous*.

CONCLUSIONES

En la actualidad los sistemas de comunicación están presentes en todos los ámbitos de nuestra vida, ya sean los correos electrónicos personales o las conferencias laborales. Es decir, es una parte esencial de nuestra sociedad y del desarrollo de la tecnología en general.

Aunque los avances en la tecnología sean imprescindibles para el desarrollo de nuestra sociedad, debemos tener cuidado e informarnos bien de los peligros que podemos correr. Cada día se descubre una nueva forma de protección pero también una de ataque, por lo que prevenirnos de ellas será una ventaja a la hora de defender nuestra información privada y de evitar problemas.

También es necesario señalar que los hackers, aunque algunos puedan usar sus conocimientos para perjudicar a otros usuarios, son en su mayoría personas sin las que no podríamos contar con extraordinarios avances en el campo de la informática, y que la concepción negativa que se tiene de ellos no es correcta. Por ejemplo, el sistema operativo Linux fue creado por un hacker y hoy en día es uno de los más utilizados. Este es solo uno de los muchos ejemplos de avances hechos realidad por hackers, que al fin y al cabo sólo son entusiastas de los ordenadores y quieren contribuir a la sociedad. Por ello, la visión que se tiene de ladrones o criminales de ellos debe desaparecer.