¿QUÉ ES (Y QUÉ NO) UN *HACKER*?

El *hacking* está íntimamente ligado al nacimiento de Internet y a las oportunidades económicas, técnicas y sociales que supuso desde sus inicios en la década de los 60 y 70. Desde su origen militar (como fue DARPA[1]), hasta su proliferación masiva a partir del año 2000 y su implantación global hoy en multitud de dispositivos electrónicos (desde ordenadores a servidores, móviles, tabletas…), Internet ha servido como vehículo de popularización, difusión e intercambio para este movimiento.

Aunque poco tiene que ver con su origen – en un principio se utilizaba "hack" como verbo para expresar "perder el tiempo" – el significado del término ha cambiado a lo largo de décadas desde que empezó a utilizarse en un contexto informático.

Actualmente, el término *hacker* puede tener connotaciones positivas y negativas en función del concepto que se maneje. Así, la palabra se utiliza tanto para definir a un desarrollador de *software* apasionado por la informática que depura y arregla errores en los sistemas, como para referirse a aquel que se infiltra en un sistema informático con el fin de eludir o desactivar las medidas de seguridad.

I La cultura *hacker* y sus motivaciones

Definir a una persona como un verdadero *hacker* puede ser difícil. Pocos acostumbran a autodefinirse como tales. Nadie nace *hacker* aunque sí puede poseer la curiosidad, paciencia y creatividad necesarias. Un verdadero *hacker* es aquel que posee una gran motivación e impulso natural por investigar y realizar todo aquello que se proponga por la búsqueda del simple conocimiento. El objetivo es el control total del sistema que tiene entre manos, la sensación de poder afirmar que ese programa, red, dispositivo, mecanismo… que acaba de *hackear* le pertenece, ya que lo domina a su antojo.

No es una definición totalmente técnica asociada al mundo informático o a las nuevas tecnologías. De hecho, actualmente es un concepto abierto y más global, distanciado de la ética *hacker* inicial: puede ser considerado como *hacker* tanto un mecánico, un ingeniero industrial, un artista como cualquier persona que no ceje en su empeño por investigar y dominar su técnica hasta perfeccionarla. En esta vertiente tenemos ejemplos como *Hackerschool*[2], orientado al perfeccionamiento de los programadores y la creación de software libre, y no a la intrusión de sistemas o modificación de programas (como pudiera parecer para un neófito). Se debe incidir por tanto en la idea de que el *hacking* es experiencia y excelencia en las técnicas propias del sujeto por puro conocimiento.

[1] Defense Advanced Research Projects Agency (Agencia de Investigación de Proyectos Avanzados de Defensa).

[2] Iniciativa Hackerschool: http://www.hackerschool.com/

Aunque un tanto romántica, la definición anterior es válida para las personas que practican esta filosofía día a día. Sin embargo, esta idea está muy alejada de lo que se da a conocer en noticias o medios de comunicación ajenos a esta filosofía. A menudo, esos *hackers* de los que se habla no son tales, y la propia cultura *hacker* tiene asignados sus propios roles para ellos, de los que se hablará más adelante.

Así pues, el verdadero *hacker* es aquella persona curiosa, paciente, creativa, que investiga y no se detiene hasta controlar un sistema o perfeccionar u optimizar su técnica. Su motivación es el puro conocimiento. Por ello, si sus objetivos son otros (económicos o no) se debería encasillar en subtipos dentro de la cultura *hacker*.

Especial mención merece la importancia de la filosofía *hacking* en el mundo de la programación, ya que fue en sus inicios con los sistemas UNIX donde una gran generación de usuarios y programadores explotaron sus conocimientos para el diseño de nuevos sistemas operativos, *software* e incluso *hardware* que han sentado las bases de lo que hoy se utiliza de forma masiva. El *software* libre ha bebido mucho de la filosofía *hacking* y claro ejemplo es el proyecto GNU[3], con Richard Stallman como uno de sus mayores exponentes. Esta es una de las bases sobre las que se asienta el popular sistema operativo libre GNU/Linux.

Esta es (o era) la definición original de la ética del *hacking*, y de ella se han derivado las bases filosóficas que se consideran ligadas a esta cultura:[4]

- Apoyar procesos de apropiación social o comunitaria de las tecnologías.
- Poner a disposición del dominio público el manejo técnico y destrezas alcanzadas personal o grupalmente.
- Crear nuevos sistemas, herramientas y aplicaciones técnicas y tecnológicas para ponerlas a disposición del dominio público.
- Realizar acciones de *hacktivismo* tecnológico con el fin de liberar espacios y defender el conocimiento común, o mancomunal.

[3] Proyecto GNU Anuncio inicial: http://www.gnu.org/gnu/initial-announcement.html

[4] http://es.wikipedia.org/wiki/Hacking

II Una posible clasificación de los distintos tipos de *hackers*

Igual que para estudiar cualquier disciplina técnica o artística es necesario familiarizarse con determinados conceptos y vocabulario propio, el mundo del *hacking* no es diferente. Debido a la densidad de conceptos y la delgada línea que separa algunos de otros, muchos términos y definiciones son erróneamente aceptados o simplemente confundidos, estereotipando conceptos equivocados. Es por ello necesario conocer de manera introductoria la jerga común entre la cultura del *hacking* para identificar tanto a aquellos que pertenecen a ella, como a los que no.

Podemos definir tres categorías principalmente:

- ***Whitehackers*, *whitehats* o *hackers* éticos.** Son profesionales dedicados a la búsqueda y solución de vulnerabilidades en sistemas empresariales, gubernamentales y particulares. Estas personas suelen trabajar para las empresas de informática. Dentro de este grupo podemos englobar a los llamados:

    - ***Bluehat hackers*** ("sombreros azules"). Generalmente son consultores o profesionales externos de seguridad dedicados a *betatesting* o comprobación de un *software* o *hardware* antes de su lanzamiento oficial y salida al mercado, para intentar exponer las vulnerabilidades existentes, paralelamente al trabajo realizado por el propio grupo interno de la empresa. Son como una tercera opinión y su término se generalizó a través de su presencia en los certámenes organizados por Microsoft[5].

    - ***Red Hat hackers*** ("sombreros rojos"). Se refiere a un *hacker* trabajando dentro de la compañía "*Red Hat*", responsable de la creación y mantenimiento de las distribuciones del sistema operativo GNU/Linux & Fedora. Este tipo de *hacker* se caracteriza principalmente por utilizar, promover y mejorar el *software* libre.

- ***Blackhackers, blackhats* o *crackers.*** Son personas dedicadas a utilizar (de forma profesional o amateur) sus conocimientos para actividades delictivas y sacar un provecho económico: En muchos casos están relacionados con la delincuencia organizada.

- Finalmente, podríamos identificar un grupo intermedio: ***los Greyhat hackers*** ("sombreros grises"). Un cajón de sastre donde encajan aquellas personas que trabajan indistintamente tanto para firmas de seguridad como para organizaciones criminales. Puede que la información obtenida durante el desarrollo de un perfil,

[5] Certamen de Bluehackers de Microsoft: http://technet.microsoft.com/es-es/security/cc261637.aspx

alimente el otro, o que se produzca un proceso donde finalmente el individuo se posicione finalmente.

Ilustración 1: Tipos de *hackers*

***Fuente:** INTECO*

III ¿Qué no es un *hacker*?

El término *hacker* es positivo, y para enfatizarlo resumimos aquellos términos o personajes que no deben identificarse con el verdadero *hacking*:

- ***Crackers*.** Un *cracker* puede haberse o no formado en la cultura y conocimientos propios del movimiento, pero el hecho de utilizarlos en su propio beneficio dañando a los demás, supone por sí solo un hecho diferenciador que lo aleja del verdadero *hacking*. Aunque se trata un subtipo de *hacking*, no es considerado como un verdadero *hacker* por las connotaciones peyorativas que posee, y por alejarse de filosofía *hacker*. Se consideran en esta clasificación tanto los atacantes, como los *hackers* dedicados a crear *cracks* (pequeños programas que permiten eludir la licencia de *software* de pago).

- ***Lammers* (incompetentes)**. Persona generalmente con pocos conocimientos técnicos que los utiliza para vanagloriarse y hacerse pasar por un verdadero *hacker*.

- ***Scriptkiddies***. Aprendices que tampoco llegan a mejorar en sus conocimientos y se dedican a ejecutar guías paso a paso o utilizar pequeños conjuntos de herramientas realizadas por terceros. Su objetivo es conseguir algún tipo de reconocimiento dentro del movimiento o simplemente realizar *dafacements*[6]

[6] Listado de *defacements* online: http://www.zone-h.org/archive

(cambiar o eliminar el contenido de una web) o denegaciones de servicio impidiendo el acceso a las mismas.

- **Activistas Anonymous.** En su origen fue un movimiento de protesta en Internet asociado a determinados foros y canales de IRC y que ha tenido una gran difusión gracias a las redes sociales y al eco mediático de sus ataques a empresas y organismos gubernamentales. Cualquiera puede pertenecer a Anonymous[7] y por tanto no puede definirse como un grupo por sí mismo de *hackers* o *crackers* (aunque siempre se les asocia a los *greyhats*). Básicamente es un grupo anárquico de usuarios a priori sin connotaciones políticas.

  Una escisión, que provocó molestias a las fuerzas de orden público, sobre todo al FBI, la CIA, y a grandes empresas como Sony, fue *Lulzsec* (@LulzSec)[8] que actualmente se encuentra inactivo. Como ejemplo de la filosofía que mueve a Anonymous, cualquiera puede pertenecer al movimiento y tan rápido como se generan unos grupos, desaparecen.

- **Vandalismo**. Impedir el acceso a páginas web, realizar ataques denegación de servicio (DoS), alterar el contenido de las webs (*deface*), entre otras, son técnicas que cualquiera con un mínimo de conocimientos puede realizar pero que, en rigor, no puede considerarse *hacking*.

- **Piratería** (*Warez*). No está relacionada con el *hacktivismo*. Se define como la acción de distribuir contenido digital protegido por derechos de propiedad intelectual (*copyright*) con el objetivo de conseguir una remuneración económica, bien por la distribución y/o venta, o bien por ingresos a través de publicidad.

- ***Malware***. La creación de *malware* tampoco es propia del hacking. Podría incluirse como herramienta propia o medio del *cracking* que busca la infiltración en el mayor número de equipos o el mayor daño posible.

- ***Hacktivismo*.** Mención especial merece éste término que hace referencia a las actuaciones de determinados *hackers* para defender, dar a conocer o tomar conciencia sobre hechos, conflictos o abusos políticos. Aunque pueda parecer íntimamente relacionado con el movimiento Anonymous no lo están. Estos sí pueden ser grupos de *hackers*, profesionales u expertos que protestan de una determinada manera en el mundo digital para demostrar su punto de vista (político

[7] Ejemplo de activista: http://twitter.com/Anon_Central

[8] LulzSec: http://twitter.com/lulzsec

o social)[9]. Dependiendo de las formas usadas para conseguir su objetivo, podrían llegar a entrar dentro de uno u otro grupo de los anteriormente descritos.

Ilustración 2: *Hackivismo*: ¿*hacking* o *cracking*?

Fuente: INTECO

IV La profesionalización: el *hacking* ético

Como en cualquier otra actividad, puede llegar un momento en el que se generan necesidades tecnológicas en el mercado y éstas deben ser atendidas. Es por ello que el mundo del *hacking* ha evolucionado, profesionalizándose en todas sus facetas y en todos los ámbitos tanto legales como al margen de la sociedad.

El *hacking* ético engloba todos aquellos servicios prestados para la seguridad de las empresas tanto por *hackers* como por consultores y expertos en seguridad. Principalmente, estos servicios están orientados a la simulación de intrusiones reales en los sistemas corporativos para poder hacer un análisis y evaluación de las vulnerabilidades. Posteriormente la empresa las solucionará para evitar una posible intrusión en sus sistemas.

Los *Ethical Hackers* son expertos que realizan una serie de medidas para determinar la vulnerabilidad de un sistema. A esta práctica normalmente se le conoce como *Pen-test* (*penetration test*) o test de intrusión. Dichas pruebas de intrusión permiten:

a) Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.

b) Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.

c) Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable.

Para ello, se sigue una serie de pautas, usadas también por los atacantes (recopilación de información, descripción de la red, exploración de los sistemas, extracción de

[9] Hackea por tus derechos: http://comunes.org/es/hack-for-your-rights/

información, acceso no autorizado a información sensible o crítica, auditoría de las aplicaciones web...), pero con la diferencia de haber sido consensuadas previamente con los responsables del sistema objetivo.

Otra división dentro del *hacking* ético sería la búsqueda de vulnerabilidades en el *software*, que llevan a cabo los profesionales encargados de detectar activa o pasivamente fallos en el *software*. Dependiendo de si el fallo descubierto se comunica de forma responsable a los fabricantes se hablará de "*full disclosure*" o "*responsible disclosure*".

En el primer caso, se hacen públicos todos los datos técnicos del error, sin avisar previamente al fabricante. Esto puede llegar a considerarse una irresponsabilidad y ser calificado de "vandalismo". En el segundo, se coordina con los responsables del programa una solución para así hacer público el fallo cuando ya existe un parche que permita proteger a sus clientes.

Otra modalidad es la venta de los fallos a terceros, que se encargan de negociar con el fabricante la solución. Ejemplos de empresas dedicadas a la compra de vulnerabilidades son *ZDI o iDefense Labs.*

V La otra cara de la profesionalización: el mercado negro y la ciberdelincuencia organizada

Cuando el mercado no puede absorber en empresas lícitas el conocimiento de las personas con talento *hacker*, pueden aparecer otras organizaciones que intenten rentabilizar sus habilidades en otras áreas orientadas a la criminalidad. Se trata de *crackers*, *spammers, scammers, phishers* organizados que, como las mafias, se dedican al lucro propio de forma profesional. Existen tantos tipos como actividades delictivas en el mundo digital:

- ***Phreakers*.** Equivalente en sistemas telefónicos al *cracker*, se le supone amplios conocimientos sobre las tecnologías y mecanismos que intervienen en las comunicaciones digitales y analógicas, siendo capaces de interceptarlas y tomar control del sistema para su propio beneficio. Fueron muy conocidos en los años 70 y 80 con la creación y distribución de la *bluebox* y posterior *blackbox*. Se trataba de pequeños dispositivos analógicos-digitales que permitían realizar llamadas gratuitas desde los antiguos sistemas de telefonía.

- ***Phishers*.** Dedicados al fraude bancario, diseñan, habilitan y gestionan sitios falsos de webs bancarias o sistemas de pago, principalmente para intentar engañar a los usuarios y conseguir sus credenciales de sus cuentas o de las tarjetas de crédito. Trabajan conjuntamente con los *spammers.*

- ***Scammers*.** Dedicados a todo tipo de estafas en la red, ya sea vendiendo productos fraudulentos, simulando la prestación de servicios ficticios, etc. Una estafa particularmente persistente tiene su origen en Nigeria y hace referencia a todo ese compendio de correos electrónicos ofreciendo herencias o depósitos millonarios, que necesitan ser retirados del país rápidamente por encontrarse en una situación límite. Piden ayuda a la víctima para custodiar esa gran suma de dinero a cambio de un porcentaje. El objetivo es obtener información de las víctimas (para robar sus ahorros) o pedir un pequeño adelanto en concepto de gastos de gestión, que la víctima perderá.

- ***Spammers*.** Quienes generan y distribuyen correo basura. El *spam* supone gran parte de tráfico de correos electrónicos a nivel mundial y una de las mayores molestias para los usuarios. Aunque a simple vista inofensivo, en realidad se trata de una herramienta esencial para *phishers* y *scammers* que la utilizan como vehículo para conducir a sus víctimas a sitios fraudulentos o infecciosos.

- ***Skimmers* y *carders***. Son aquellos sujetos y mafias encargados de la clonación de tarjetas bancarias. Sus objetivos suelen ser clientes en tiendas o restaurantes en colaboración con algún trabajador del local que obtenga acceso a la tarjeta en el momento del paso por el terminal TPV o cualquier usuario de un cajero que haya sido modificado para copiar las bandas magnéticas. Todos ellos se dedicarían al *skimming* (manipulación de los dispositivos que leen las tarjetas para poder extraer sus datos y clonarlas), siendo la función del *carding* comprobar que esos datos siguen siendo válidos para su distribución y uso. Usarán Internet para sacar provecho de esas tarjetas robadas, ya sea comprando bienes y servicios o directamente vendiendo la información a terceros.

Una de las actividades más lucrativas y que más repercusión está teniendo es la **creación y venta de *botnets*** o granjas de usuarios/sistemas infectados por todo el mundo. Al ser tan elevado el número de sistemas zombi que poseen estas *botnets*, se pueden realizar desde ataques colectivos de denegación de servicio e intrusión a gran escala hasta grandes fraudes económicos con pérdidas que rondan o superan los centenares de miles de euros.[10]

Como ejemplo tomemos a Koobface, *botnet* de origen ruso[11], que lleva activa desde 2009 y se la conoce por utilizar Facebook como medio de difusión de su propio virus-gusano. Una vez infectados los equipos, son utilizados para recabar datos y credenciales de los usuarios para defraudar. Aunque las autoridades tienen identificados a los autores de

[10] Botnet Economics: Uncertainty Matters: http://www.falleneth.com/cmuj/papers/botnets_econ.pdf

[11] Symantec: Koobface http://www.symantec.com/security_response/writeup.jsp?docid=2008-080315-0217-99&tabid=2

esta *botnet*, es difícil incriminarles[12] debido a sus técnicas tan meticulosas a la hora de realizar este tipo de actividades.

Existen además determinados foros donde es posible encontrar sus servicios a baja o gran escala, desde intrusiones a sistemas de particulares hasta venta de denegaciones de servicio a webs. Cualquier servicio relacionado que permita ser llevado a cabo con una de estas redes, está a la venta a un precio.