# Glosario de términos de ciberseguridad

Este glosario contiene términos seleccionados asociados con la ciberseguridad.

## A

**Amenaza de persona con información privilegiada**: Una amenaza para una organización que proviene de personas dentro de la organización, por ejemplo, empleados, contratistas o socios empresariales que tienen "información privilegiada" sobre las prácticas de seguridad, los datos y los sistemas de la organización.

**Amenaza persistente avanzada (APT)**: Un ataque de red a largo plazo y en varias fases donde usuarios no autorizados obtienen acceso y recopilan datos valiosos de la empresa.

**Ataque de fuerza bruta**: La técnica que utiliza un hacker para infiltrarse en unsistema, por ejemplo, intentar "adivinar" su contraseña.

**Autenticación**: Un servicio de seguridad que demuestra que un usuario de un sistema es verdaderamente quien dice ser.

**Autenticación de dos factores**: El uso de dos componentes diferentes para verificar la identidad reclamada de un usuario.

## B

**Botnet**: Un grupo de ordenadores, potencialmente ubicados en cualquier lugar del mundo, que están infectados por un software malicioso. El software permite al hacker conectar en red los sistemas infectados. De esta forma, el hacker tiene el control completo de todos los bots de la red y puede realizar tareas maliciosas.

## C

**Centro de control y mandato**: Una aplicación que controla todos los bots de un botnet. Un hacker envía un mandato a través de una aplicación, que a su vez retransmite el mandato a todos los sistemas afectados de la red.

**Ciberataque**: Intentos maliciosos de dañar, interrumpir u obtener acceso no autorizado a ordenadores, redes o dispositivos utilizando cibermétodos.

**Ciberseguridad**: La conservación de la confidencialidad, la integridad y la disponibilidad de la información en el ciberespacio.

**Cifrado**: Una técnica algorítmica que cambia el contenido de un archivo por datos ilegibles para las personas externas a la cadena de comunicación.

**Cloud**: Una colección de sistemas con grandes prestaciones de almacenamiento que atienden remotamente las solicitudes de archivos del cliente; la tecnología permite el acceso a los archivos a través de Internet, desde cualquier punto del mundo.

**Contraseña única**: Una contraseña que se genera para su uso en una sesión de inicio de sesión. A veces, se comunica entre el cliente y el servidor a través de un canal seguro.

**Copia de seguridad**: Forma de garantizar que todos los datos importantes se almacenen en una ubicación fuera de línea segura para que no se pierdan si se hackea un sistema.

**Cortafuegos**: Una tecnología defensiva basada en hardware o software dedicada a impedir el acceso no autorizado. Se crea un *"muro"* o filtro que juzga cada interacción intentada con el sistema del usuario y la conexión a Internet para determinar *"*si esta entrada debe permitirse o no*"*.

## D

**Día cero (ataque)**: Un tipo específico de exploit de software, normalmente un malware. Lo que hace que un exploit de día cero sea exclusivo es que es desconocido para el público o el proveedor de software. Es decir, como son pocas personas las que conocen la vulnerabilidad, tienen *"*cero días*"* para protegerse de su uso.

## E

**Exploit**: Una aplicación o un script maliciosos que puede utilizarse para aprovechar la vulnerabilidad de un sistema.

## F

**Firma digital**: Información que se cifra con una clave privada y se adjunta a un mensaje u objeto para garantizar al destinatario la autenticidad y la integridad del mensaje u objeto.

## G

**Gusano**: Un malware que puede replicarse para propagar una infección a otros sistemas conectados. El malware busca activamente sistemas débiles en una red para explotarlos y propagarse.

## H

**Hacker de Sombrero blanco**: Una persona que utiliza sus habilidades de hackeo para fines éticos. Por otro lado, un hacker de "Sombrero negro" normalmente tiene un objetivo malicioso. Las empresas a menudo contratan hackers de Sombrero blanco para probar sus prestaciones de ciberseguridad.

## I

**Infracción**: El momento en el que un usuario no autorizado o un intruso (hacker) explota con éxito una vulnerabilidad en un sistema o dispositivo y obtiene acceso a los archivos y la carpeta.

## J

**Jailbreak**: Omisión de las restricciones de software en un dispositivo, por ejemplo, cuando un usuario puede entrar en acceso raíz del sistema operativo o el kernel. Este método se utiliza a menudo en el contexto de la seguri dad de teléfonos móviles.

## M

**Malware**: Un término paraguas que describe todas las formas de software malicioso diseñadas para provocar el caos en un sistema. Los formas típicas de malware incluyen virus, troyanos, gusanos y ransomware.

**Man-in-the-Middle (MitM)**: Una intrusión donde el atacante intercepta los mensajes entre un usuario y un sitio web para observar y registrar transacciones. Los ataques MitM son variaciones avanzadas de los ataques de tipo phishing y pharming. En un ataque MitM, un usuario que ha iniciado una sesión en un sitio web no es consciente de que toda la información intercambiada entre ellos y el sitio web pasa a través de un sitio web intermedio. Un delincuente puede utilizar el sitio web intermedio para ver la informaciónprivada y alterar las transacciones.

## P

**Parche**: Un nuevo software publicado como un “arreglo”. La mayoría del software requiere miles de líneas de lenguaje de programación para crearse, por lo que es difícil para el desarrollador garantizar que se han cubierto todas las vulnerabilidades. Cuando los hackers o un desarrollador descubren puntos de entrada, los proveedores de software normalmente publicarán un nuevo software como un arreglo.

**Phishing (ataque)**: Una técnica utilizada por los hackers para obtener información confidencial como, por ejemplo, contraseñas, cuentas bancarias o datos de tarjetas de crédito. A menudo, un usuario recibe inesperadamente un correo electrónico camuflado como si fuera de una fuente legítima. En mucho casos, el hacker intentará engañar al destinatario para que responda con la información de interés, por ejemplo, datos bancarios, o inducirlo para que pulse un enlace malicioso o ejecute un archivo adjunto.

## R

**Ransomware**: Una forma de malware que impide deliberadamente el acceso a archivos de un ordenador. Si un sistema está infectado con malware diseñado con estos fines, normalmente se cifrarán los archivos y se solicitará el pago de un “rescate” para poder descifrarlos.

**Red privada virtual (VPN)**: Una herramienta que permite a un usuario permanecer anónimo mientras utiliza Internet. Una VPN ofrece anonimato al enmascarar la ubicación y cifrar el tráfico mientras viaja entre el sistema del usuario y el sitio web que está visitando.

## S

**Señal**: Un elemento que autoriza el acceso a un servicio de red. En general, una señal de autenticación o una señal de seguridad de hardware hace referencia a dispositivos de hardware

pequeños como, por ejemplo, llaveros o tarjetas inteligentes que los usuarios tienen en su posesión para autorizar el acceso a un servicio de red.

**Señuelo:** Una técnica de ciberseguridad de defensa. Esta técnica implica el uso de un sistema (servidor) diseñado para parecer un destino legítimo de gran valor en una red. El objetivo es atraer a los hackers para que ataquen al sistema no a los datos o sistemas de gran valor real. La técnica del señuelo permite a los administradores observar a los hackers "en acción" y aprender a protegerse de sus métodos de ataque.

## T

**Troyano**: Un malware que permite a un hacker obtener acceso remoto a un sistema. Un sistema infectado con un troyano crea un punto de entrada para que el infractor pueda descargar archivos o ver las pulsaciones de un usuario.

## V

**Virus**: Un tipo de malware de sistemas personales. Los virus aparecieron por primera vez con el uso de los disquetes. Los virus normalmente buscan dañar, borrar o modificar información en un sistema antes de propagarse a otros, y algunos también pueden provocar daños físicos.

## W

**Watering Hole (ataque)**: Un ataque destinado a un grupo de interés especial que coloca código malicioso en un sitio web frecuentado por un determinado público. Ejemplo: en 2013, los visitantes de varios sitios web de empresas de energía y suministros se vieron expuestos a código malicioso que podía infectar sus sistemas.

**Wi-Fi abierta**: Una red pública con restricciones limitadas o sin restricciones que puede exponer los dispositivos y la actividad (tráfico) de los usuarios conectados a los demás usuarios de esa red.