Universidad Nacional
Federico Villarreal

FACULTAD DE INGENIERÍA
ELECTRÓNICA E INFORMÁTICA

INGENIERIA DE SISTEMAS DE INFORMACIÓN

Docente: Ing. Alejandro Rea

Lima Perú Junio 2025

Sesión 11

¿Qué es la ciberseguridad y para qué sirve?

En la actualidad, la mayoría de las organizaciones emplean sistemas informáticos para realizar sus operaciones y almacenar datos sensibles.

Aunque esta tendencia ofrece grandes facilidades, es también una vía de acceso para los delitos virtuales.

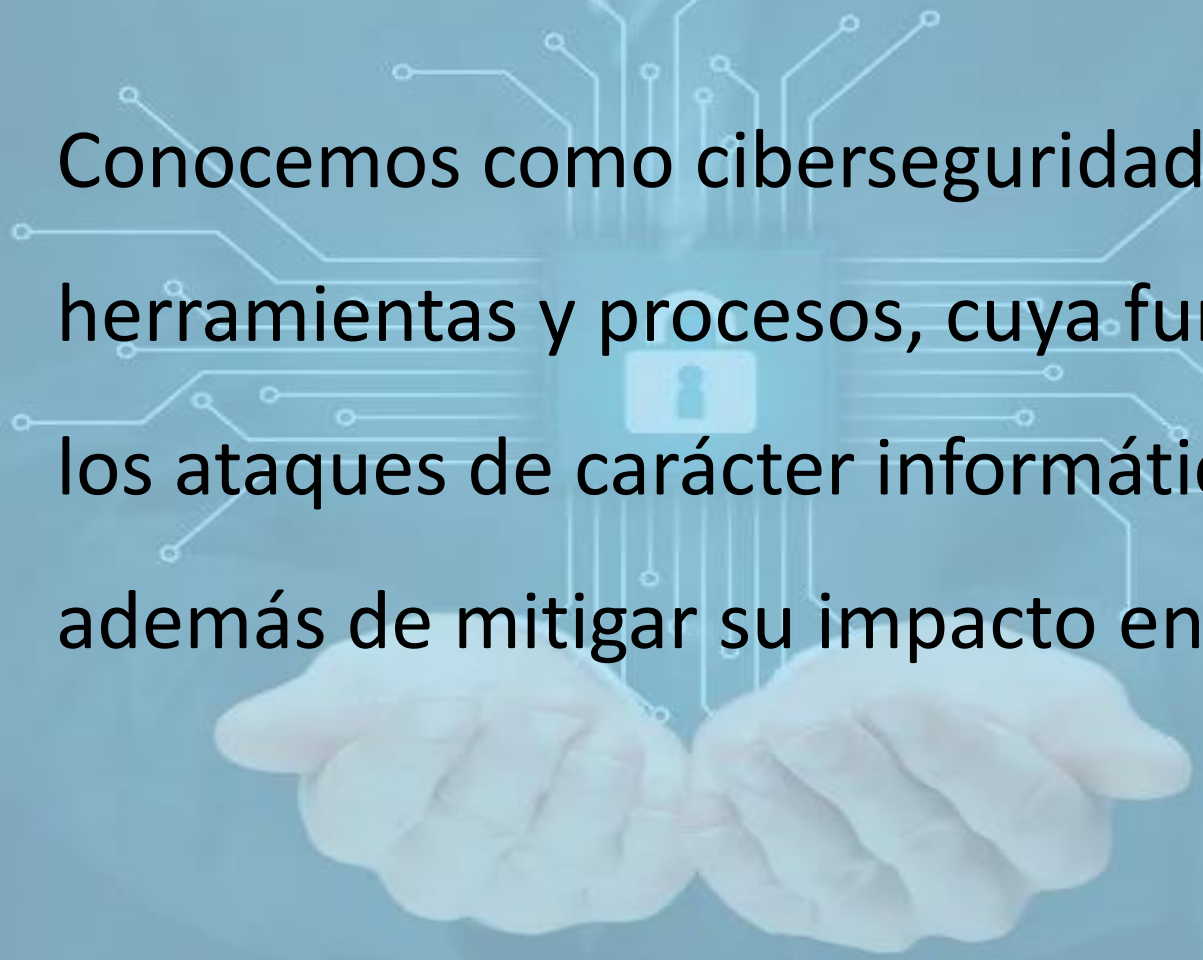
Para evitar ser víctima de estas prácticas, es necesario conocer qué es la ciberseguridad y cómo funciona.

Te invito a repasar conmigo la ciberseguridad desde cero, haciendo hincapié en su importancia y las amenazas que enfrenta.

Debido a la creciente demanda en los sectores público y privado, la especialización en ciberseguridad es una opción cada vez más solicitada entre los profesionales de ingeniería, sistemas e informática.


¿QUÉ ES LA
CIBERSEGURIDAD?

Ciberseguridad: ¿qué es?



Conocemos como ciberseguridad a un amplio conjunto de herramientas y procesos, cuya función principal es la de prevenir los ataques de carácter informático en todas sus modalidades, además de mitigar su impacto en las organizaciones y personas.

Ciberseguridad: ¿qué es?

La ciberseguridad se aplica en diferentes contextos, desde la elección de una contraseña segura hasta el uso de sistemas de protección sofisticados. Estudiar ciberseguridad implica conocer todas las medidas existentes para la protección de sistemas informáticos, redes, software y bases de datos ante posibles amenazas digitales.

¿Por qué es importante la ciberseguridad en tu empresa?

Así como tu negocio físico necesita de sistemas de seguridad, tus propiedades digitales también

¿Por qué es importante la ciberseguridad y para qué sirve?

Según reportes, la ciberdelincuencia podría acarrear a la economía mundial un gasto de 10.5 billones de dólares al año 2025. Este y otros indicadores nos dan una idea de la importancia que tiene la ciberseguridad en Perú y el resto de los países.

¿Por qué es importante la ciberseguridad y para qué sirve?

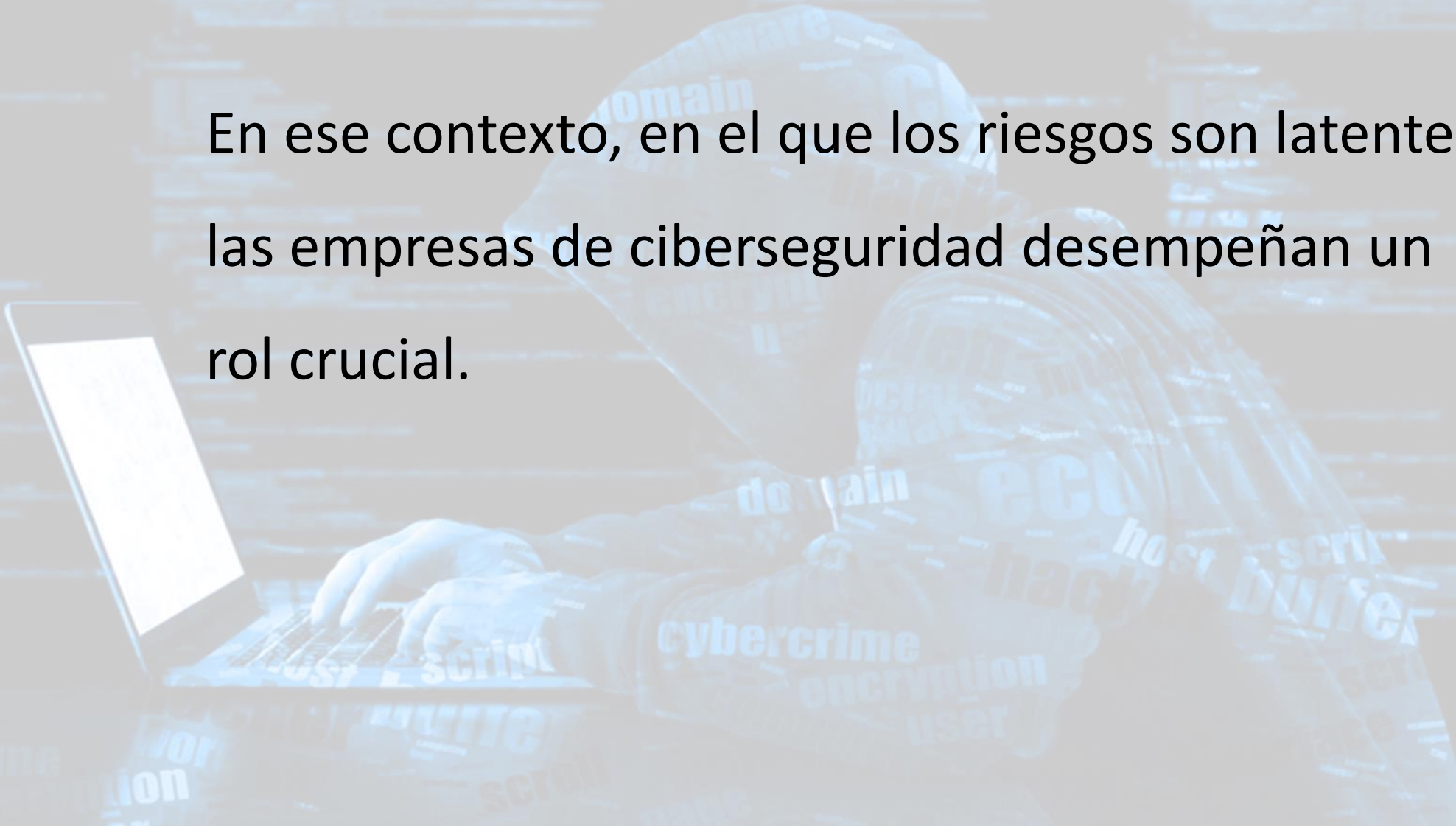
En el caso de las organizaciones, los delitos y ataques cibernéticos pueden llegar a generar cuantiosas pérdidas económicas, además de la pérdida de datos y fallas operativas. A nivel individual, las víctimas de estas prácticas podrían sufrir robos o ver su identidad suplantada.

¿Por qué es importante la ciberseguridad y para qué sirve?

Para hacerte una idea de la magnitud de las amenazas digitales, solo hace falta ver qué es una guerra cibernética, un tipo de conflicto en el que los propios Estados vulneran los sistemas informáticos de otros países, a fin de generarles un perjuicio.

¿Por qué es importante la ciberseguridad y para qué sirve?

En ese contexto, en el que los riesgos son latentes, las empresas de ciberseguridad desempeñan un rol crucial.



TIPOS DE AMENAZAS

INTENCIONADAS

ACCIDENTALES

INTENCIONADAS

ACCIDENTALES

Tipos de amenazas y ataques a la ciberseguridad

Luego de una breve introducción a la ciberseguridad, veamos cuáles son los tipos de ataques virtuales más comunes.

Malware

Se conoce como “malware” a los programas o archivos maliciosos que se instalan en un sistema con el objetivo de dañarlo o deshabilitarlo. En esta categoría encontramos a los virus informáticos, troyanos, spyware, ransomware, adware, etc.

En años recientes, también han proliferado los mineros en ciberseguridad, un tipo de malware que utiliza los recursos de un ordenador para minar criptomonedas, sin autorización de su propietario.

Perú enfrenta más de 177 mil ataques de malware por día

Los sectores más atacados son el gobierno, energía y servicios públicos, y agricultura.

El Panorama de Amenazas de Kaspersky 2024 reveló que la empresa global de ciberseguridad bloqueó más de 64 millones de ataques de malware (software malicioso diseñado para infiltrarse en tu dispositivo sin tu conocimiento) en Perú entre junio de 2023 y julio de 2024, lo que equivale a 177.400 por día y alrededor de 123 ataques por minuto.

Entre los sectores más atacados por **malware** en Perú se encuentran el **gobierno (41.74%)**, energía y servicios públicos (8.77%), y la agricultura/forestal (7,16%).

Este enfoque de los cibercriminales hacia el sector gubernamental se debe a que el gobierno contiene los datos de los ciudadanos, convirtiéndolo en una posibilidad infinita de fraudes, estafas y **ataques**. Otra razón para que el sector gubernamental se ubique en el top, está relacionada a temas ideológicos, los cuales se intensifican en las temporadas electorales.

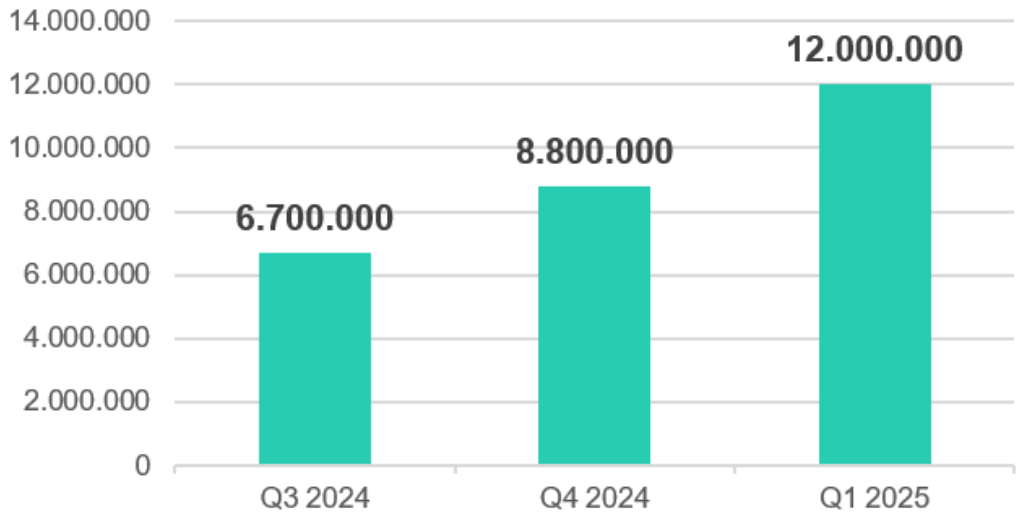
Más de 12 millones de smartphones fueron blanco de ataques con malware a inicios de 2025: revela Kaspersky

9 de junio de 2025

kaspersky

La compañía advirtió en un informe reciente que este tipo de amenazas sigue en aumento. Entre enero y marzo de este año, se registró un crecimiento del 27% en archivos maliciosos detectados, en comparación con el cierre de 2024.

Según el informe de Kaspersky *Evolución de las amenazas informáticas en el primer trimestre de 2025: estadísticas móviles,* los ataques a smartphones siguen en aumento. Solo en los primeros tres meses del año se detectaron 180,000 archivos maliciosos, un 27% más que a finales de 2024. Además, más de 12 millones de personas fueron afectadas por estas amenazas, lo que representa un incremento del 36% respecto al trimestre anterior. Esta tendencia al alza no es nueva, ya que los ataques vienen creciendo desde mediados del año pasado.




WORMS
ROOTKITS
SPYWARE
TROJANS
CRIMEWARE
MALWARE
VIRUSES
ADWARE

Ransomware

Es un software o código malicioso que cifra los datos más importantes dentro de un sistema, a fin de pedir un rescate para descifrarlos.

Funciona como un “secuestro virtual”, en el que los hackers buscan obtener un beneficio económico. Para prevenirlo, es recomendable hacer copias de respaldo de la información más valiosa.

Hackers se atribuyen ataque a web gob.pe, pero Gobierno niega afectación a plataforma del Estado: “Los datos están a salvo”

El secretario de Gobierno y Transformación Digital de la PCM precisó, en diálogo con Infobae Perú, que en las últimas semanas no se ha registrado ningún ciberataque que haya vulnerado la plataforma del Estado

Por **Valeria Mendoza Talledo** 02 May. 2025 09:24 a.m. PE

Hackers atacan página oficial del Gobierno peruano y piden 54 bitcoins como rescate. Foto: Composición Infobae Perú

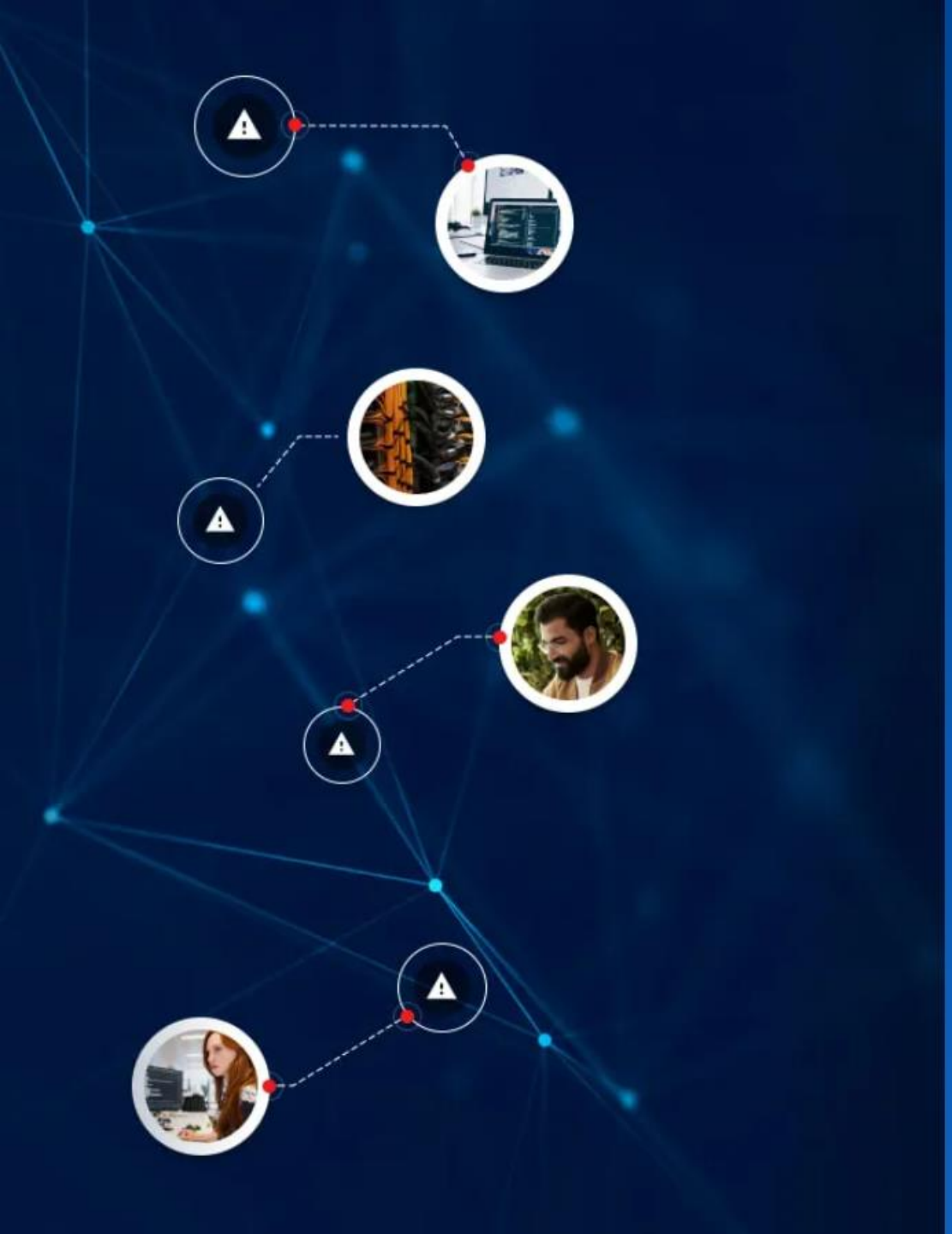
La **página gob.pe, relacionada al Gobierno del Perú,** habría sufrido un presunto *ataque cibernético* por parte de hackers, lo que ocasionó que el sitio web se cayera temporalmente. A pesar de la interrupción, el portal fue restablecido después de unos minutos de inactividad.

El *ataque* estaría a manos de **Rhysida Ransomware**, un tipo de malware que forma parte de un grupo de ciberdelincuentes que utilizan la táctica de “ransomware” para extorsionar a sus víctimas. Según el reporte publicado por **DarkWeb Informer**, los ciberdelincuentes habrían solicitado un rescate de 5 bitcoins, lo que equivale a aproximadamente **1,779,568.25 soles.**


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Ataque de intermediario

A través de esta modalidad, también conocida como man-in-the-middle, el atacante intercepta la comunicación entre dos partes para obtener información, robar credenciales o alterar datos. En muchos casos, se utilizan redes de Wifi sin contraseña como “gancho” para ver el tráfico web de los dispositivos conectados.



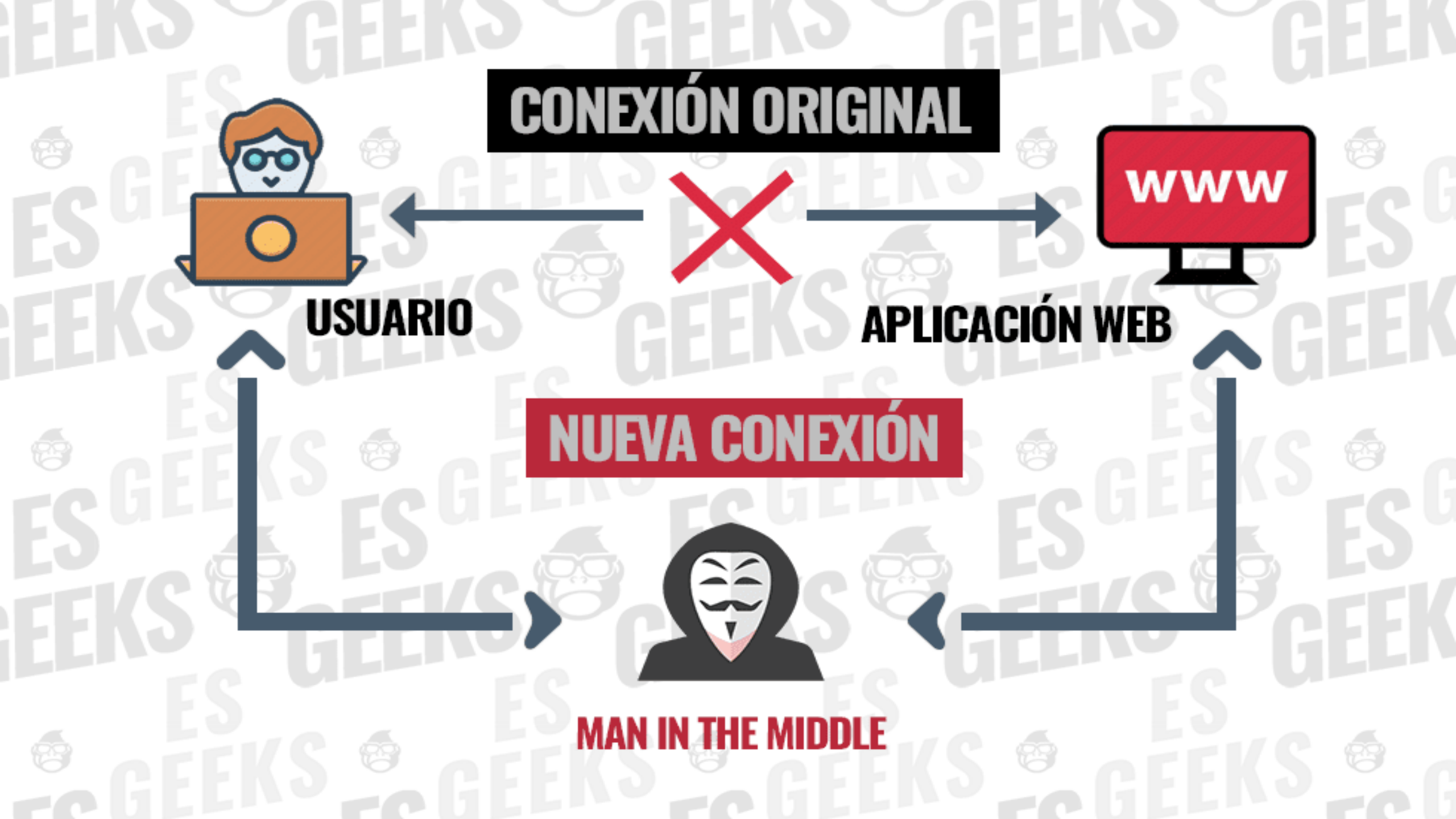
¿Qué es un ataque de intermediario?

Los ataques de intermediario o MITM, por sus siglas en inglés, consisten en un **ataque cibernético** donde el cibercriminal intercepta los datos enviados entre dos empresas o particulares. El objetivo es robar, espiar o modificar los datos con un fin malicioso, como la extorsión.

¿Cómo funciona un ataque de intermediario?

Estos ataques dependen de la manipulación de redes existentes o la creación de redes maliciosas que los cibercriminales controlan. Estos interceptan el tráfico y lo dejan pasar, recopilando información transaccional, o lo redirigen a otro lugar.

En esencia, los cibercriminales actúan como un "intermediario" entre la persona que envía la información y la que la recibe, de ahí su nombre. Estos ataques son sorprendentemente comunes, sobre todo en **redes Wi-Fi públicas**. Como las redes wifi públicas son a menudo poco seguras, no se puede saber quién supervisa o intercepta el tráfico web, ya que cualquier persona puede iniciar sesión.


CONEXIÓN ORIGINAL
www
USUARIO
APLICACIÓN WEB
NUEVA CONEXIÓN
MAN IN THE MIDDLE

Tipos de ataques de intermediario

Hay varios tipos de ataques de intermediario, lo que los convierte en las amenazas cibernéticas más versátiles que se encuentran hoy en día.

Red wifi pública

Uno de los métodos de ataque de intermediario más comunes se produce en redes wifi públicas. Las redes wifi públicas no suelen ser seguras, por lo que los cibercriminales pueden ver el tráfico web de cualquiera de los dispositivos conectados a la red y recopilar la información que necesiten.

Punto de acceso no autorizado

Se trata de un punto de acceso no autorizado e inalámbrico instalado en una red legítima. Esto le permite al cibercriminal interceptar o supervisar el tráfico entrante, que generalmente lo redirige a una red totalmente diferente para propiciar las descargas de malware o extorsionar al usuario. El malware es un tipo de software malicioso que se instala en el dispositivo de la víctima para espiar y robar datos.

Suplantación de la dirección IP

La suplantación de la dirección IP consiste en modificar la dirección IP para redirigir el tráfico al sitio web del atacante. Este "falsea" la dirección alterando las cabeceras de los paquetes para hacerse pasar por una aplicación o un sitio web legítimos.

Suplantación del ARP

Este ataque vincula la dirección MAC del atacante con la dirección IP de la víctima en una red de área local usando mensajes del ARP falsos. Cualquier dato que la víctima envíe a la red de área local se redirige en su lugar a la dirección MAC del cibercriminal, lo que le permite interceptar y manipular los datos a su antojo.

Suplantación de DNS

El cibercriminal accede al servidor DNS de un sitio web y modifica el registro de la dirección web del sitio. El registro del DNS alterado redirige el tráfico entrante al sitio web del cibercriminal.

Suplantación de HTTPS

Cuando el usuario se conecta a un sitio seguro con el prefijo https://, el cibercriminal envía un certificado de seguridad falso al navegador. Esto "engaña" al navegador para que piense que la conexión es segura cuando, en realidad, el cibercriminal está interceptando y posiblemente redirigiendo los datos.

Secuestro de sesiones

Los cibercriminales secuestran las sesiones para tomar su control en un sitio web o una aplicación. El secuestro expulsa al usuario legítimo de la sesión y bloquea al cibercriminal en la aplicación o el sitio web hasta que obtiene la información que quiere.

Inyección de paquetes

Los cibercriminales crean paquetes que parecen normales y los inyectan en una red establecida para acceder y supervisar el tráfico o iniciar ataques DDoS. Un ataque de denegación de servicio distribuido (DDoS) consiste en interrumpir el tráfico normal de un servidor saturándolo con una avalancha de tráfico de internet.

SSL Stripping

El cibercriminal intercepta la señal TLS de una aplicación o un sitio web y la modifica para que el sitio cargue en una conexión no segura como HTTP en lugar de HTTPS. Esto hace que la sesión del usuario esté visible para el cibercriminal y exponga información confidencial.

Suplantación de SSL

Este método implica suplantar la dirección de un sitio seguro para que la víctima acceda a él. El cibercriminal intercepta la comunicación entre la víctima y el servidor web del sitio al que quiere acceder, disfrazando el sitio malicioso como la URL del sitio legítimo.

SSL BEAST

El cibercriminal infecta la computadora de un usuario con JavaScript malicioso. Después, el malware intercepta las cookies del sitio web y los tokens de autenticación para descifrarlos, lo que expone la sesión completa de la víctima al cibercriminal.

Robo de las cookies del navegador de SSL

Las cookies son bits útiles de la información de sitio web que el sitio al que accede almacena en su dispositivo. Sirven para recordar la actividad web y los inicios de sesión, pero los cibercriminales pueden robarlas para obtener información y utilizarlas con fines maliciosos.

Rastreo

Los ataques de rastreo supervisan el tráfico para robar información. El rastreo se realiza con una aplicación o hardware y expone el tráfico web de la víctima al cibercriminal.

Ataque de intermediario

Ejemplos de ataques de intermediario

Equifax

En 2017, la agencia de información crediticia Equifax fue víctima de un ataque man-in-middle debido a una vulnerabilidad no parcheada en su marco de aplicaciones web. El ataque expuso la información financiera de casi 150 millones de personas.

Al mismo tiempo, Equifax descubrió brechas de seguridad en sus aplicaciones móviles que podrían dejar a los clientes vulnerables ante nuevos ataques MITM. Equifax eliminó las aplicaciones de la App Store y Google Play.

DigiNotar

Gracias a sitios web falsos para recopilar contraseñas, los piratas informáticos lanzaron un exitoso ataque MITM contra la autoridad holandesa de seguridad digital DigiNotar en 2011.

La vulneración fue importante porque provocó que DigiNotar emitiera más de 500 certificados de seguridad comprometidos a importantes sitios web, como Google, Yahoo! y Microsoft. Finalmente, DigiNotar fue eliminado como proveedor de certificados de seguridad y se declaró en quiebra.

Tesla

En 2024, los investigadores de seguridad informaron de que una vulnerabilidad permite a los hackers lanzar un ataque MITM para desbloquear y robar vehículos Tesla. Al utilizar un punto de acceso wifi falsificado en una estación de carga de Tesla, un atacante podría recopilar las credenciales de la cuenta de un propietario de Tesla. El atacante podría entonces añadir una nueva “llave de teléfono” que desbloquee y arranque el vehículo sin el conocimiento del propietario, según los investigadores.

Phishing

Es un tipo de ciberataque bastante común y variado, en el que el delincuente se hace pasar por una entidad legítima a través de e-mails, mensajes o sitios web falsos, ya sea para obtener información confidencial de la víctima, robarle dinero o causarle algún otro perjuicio.

Día de "pesca"

A través del ***phishing*** se lanza un ataque con fines fraudulentos a millones de usuarios, principalmente por medio del **correo electrónico**. De todos ellos alguno "pescará el anzuelo" y proporcionará información personal o de tipo financiera.

Algunos datos

ISTR
Internet Security Threat Report
Symantec 2017
reporta que el principal señuelo para el *phishing* son los correos que aparentemente contienen **facturas**.

78%
de las personas
es consciente de los riesgos de los enlaces desconocidos en los mensajes de correo.
Sin embargo, les dan clic.

Acciones preventivas

Instituciones confiables
Toma en cuenta que nunca solicitan datos mediante un email.

Enlace sospechoso
No lo abras. Escribe en la barra de direcciones el nombre del sitio.

Verifica autenticidad
Si sospechas del origen o contenido del correo.

Correo electrónico dudoso
Nunca des clic en los enlaces que contenga.

Sistema operativo
Actualízalo para eliminar algunas debilidades de los programas instalados.

Verifica tus cuentas
Hazlo constantemente para poder evitar un *phishing* bancario.

Diferentes tipos de ataques phishing o de suplantación de identidad

1. Suplantación de identidad dirigida

La suplantación de identidad o ataques de phishing espada implica dirigirse a una persona específica en una organización para intentar robar sus credenciales de inicio de sesión. El atacante a menudo primero recopila información sobre la persona antes de comenzar el ataque, como su nombre, puesto y detalles de contacto.

Ejemplo de suplantación de identidad dirigida

Un atacante intentó atacar a un empleado de NTL World , que es parte de la compañía Virgin Media, usando suplantación de identidad de lanza. El atacante afirmó que la víctima necesitaba firmar un nuevo manual del empleado. Esto fue diseñado para atraerlos a hacer clic en un enlace donde se les habría pedido que enviaran información privada.

Diferentes tipos de ataques phishing o de suplantación de identidad

2. Vishing

Vishing, que es la abreviatura de "suplantación de identidad de voz" (voice phishing), es cuando alguien usa el teléfono para intentar robar información. El atacante puede fingir ser un amigo o familiar de confianza o representarlo.

Ejemplo de vishing

En 2019, hubo una campaña de vishing dirigida a los miembros del parlamento del Reino Unido y a sus empleados. El ataque fue parte de un ataque que involucró al menos 21 millones de correos electrónicos no deseados dirigidos a legisladores del Reino Unido.

Diferentes tipos de ataques phishing o de suplantación de identidad

3. Suplantación de identidad de identidad por correo electrónico

En una estafa de **suplantación de identidad por correo electrónico**, el atacante envía un correo electrónico que parece legítimo, diseñado para engañar al destinatario para que ingrese información en respuesta o en un sitio que el pirata informático puede usar para robar o vender sus datos.

Ejemplo de suplantación de identidad por correo electrónico

Los piratas informáticos utilizaron LinkedIn para obtener información de contacto de los empleados de Sony y los atacaron con una campaña de suplantación de identidad por correo electrónico basándose en ingeniería social. Se escaparon con **más de 100 terabytes de datos.**

Diferentes tipos de ataques phishing o de suplantación de identidad

4. Suplantación de identidad HTTPS

Un ataque de suplantación de identidad HTTPS se lleva a cabo al enviar a la víctima un correo electrónico con un enlace a un sitio web falso. El sitio puede utilizarse para engañar a la víctima para que ingrese su información privada.

Ejemplo de suplantación de identidad HTTPS

El grupo de piratas informáticos **Scarlet Widow** busca los correos electrónicos de los empleados de las empresas y luego los dirige con suplantación de identidad HTTPS. Cuando el usuario recibe un correo electrónico principalmente vacío, hace clic en el pequeño enlace que está allí, dando el primer paso a la web de Scarlet Widow.

Diferentes tipos de ataques phishing o de suplantación de identidad

5. Farmacéutica

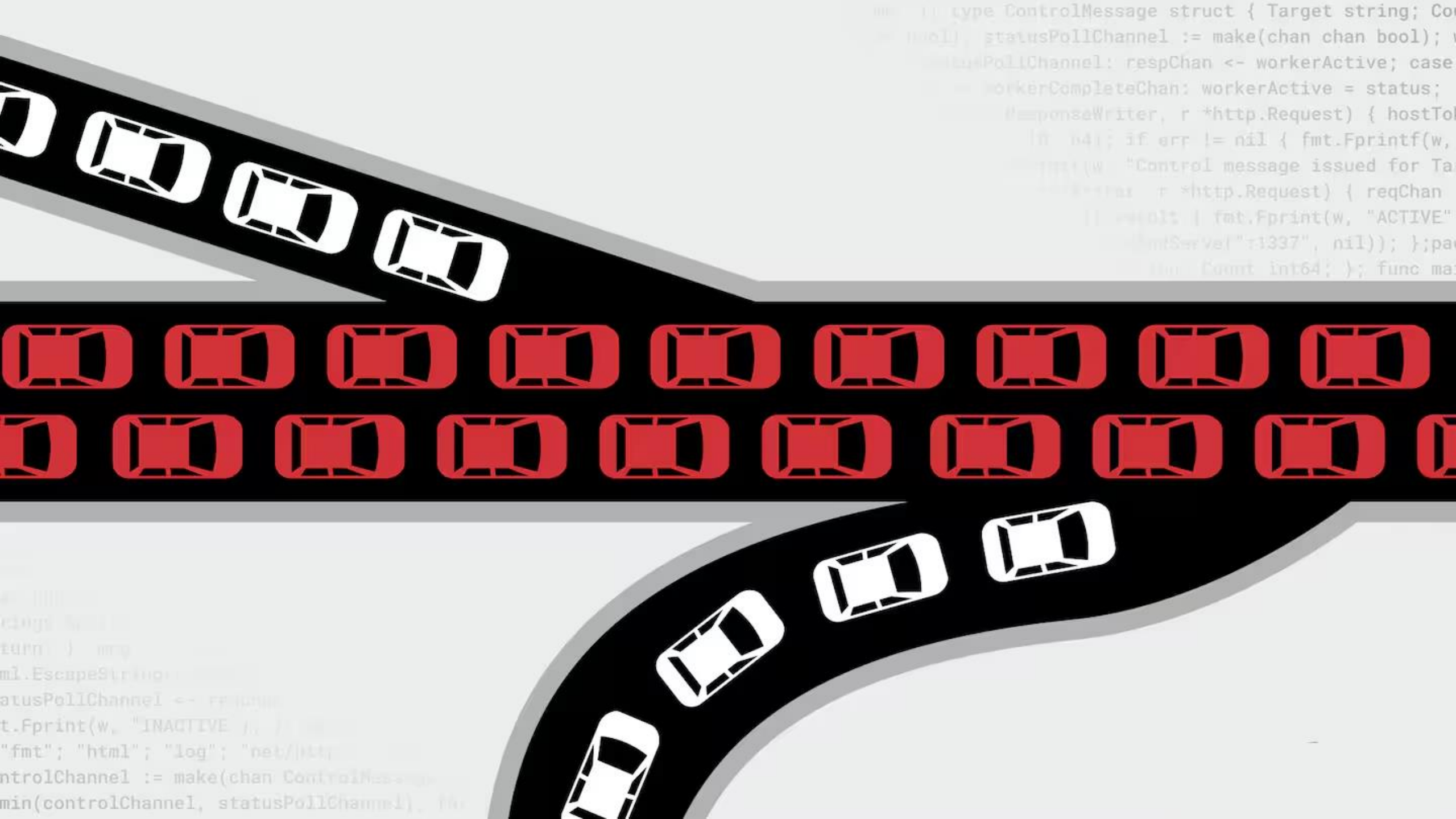
En un ataque **farmacológico**, la víctima recibe un código malicioso instalado en su computadora. Este código envía a la víctima a un sitio web falso diseñado para recopilar sus credenciales de inicio de sesión.

Ejemplo de farmacia

En 2007, se produjo un complejo ataque farmacológico tras al **menos 50 instituciones** financieras en todo el mundo. Los usuarios fueron dirigidos a sitios web falsos y se les indicó que ingresaran información confidencial.

DDoS

Un ataque de “denegación de servicio distribuido” o DDoS consiste en hacer colapsar un servidor de forma intencional utilizando redes de bots u otras técnicas. De ese modo, la organización bajo ataque no puede ofrecer sus servicios con normalidad.



Ejemplos de ataques DDoS: ¿Cuáles son los diferentes tipos de ataques?

1. Ataques en el nivel de aplicaciones

Estos ataques, a veces llamados ataques de capa 7 (porque apuntan a la séptima capa (de aplicación) del modelo OSI), agotan los recursos del servidor de destino utilizando sitios web DDoS. La séptima capa es donde un servidor genera páginas web en respuesta a una solicitud HTTP. Los atacantes ejecutan numerosas solicitudes HTTP, saturando el servidor de destino mientras responde cargando numerosos archivos y ejecutando las consultas de base de datos necesarias para crear una página web.

Diferentes tipos de ataques phishing o de suplantación de identidad

2. Inundación HTTP

Piense en estos ataques DDoS como si actualizaran un navegador web numerosas veces en muchas computadoras. Esto crea una “inundación” de solicitudes HTTP, lo que obliga a una denegación de servicio. La implementación de estos ataques puede ser simple (utilizando una URL con un rango estrecho de direcciones IP) o compleja (utilizando una matriz de direcciones IP y URL aleatorias).

Diferentes tipos de ataques phishing o de suplantación de identidad

3. Ataques de protocolo

Estos ataques DDoS, a menudo llamados ataques de agotamiento del estado explotan vulnerabilidades en las capas 3 y 4 del modelo OSI (las capas de red y transporte). Estos ataques crean una denegación de servicio al saturar los recursos del servidor o los recursos del equipo de red, como los firewalls.

Existen varios tipos de ataques de protocolo, incluidas las inundaciones SYN. Estos explotan el protocolo de enlace TCP (Protocolo de control de transmisión), que permite que dos personas establezcan una conexión de red y envíen una cantidad inmanejable de “solicitudes de conexión inicial” TCP desde direcciones IP falsas.

Diferentes tipos de ataques phishing o de suplantación de identidad

4. Ataques volumétricos

Estos ejemplos de ataques DDoS crean una denegación de servicio al utilizar todo el ancho de banda disponible en un servidor de destino y enviar enormes cantidades de datos para crear un aumento repentino del tráfico en el servidor.

Diferentes tipos de ataques phishing o de suplantación de identidad

5. Amplificación de DNS

Se trata de un ataque basado en la reflexión en el que se envía una solicitud a un servidor DNS desde una dirección IP falsificada (la del servidor de destino), lo que provoca que el servidor DNS "llame" al destino nuevamente para verificar la solicitud.

Esta acción se amplifica mediante el uso de una botnet, que sobrecarga rápidamente los recursos del servidor objetivo.

Amenaza interna

Como su nombre lo indica, es un ataque que se origina dentro de una organización. Los atacantes suelen ser empleados con acceso a información privilegiada, que usan su posición para extraer datos o hacer modificaciones críticas en los sistemas.

¿Cómo funciona la ciberseguridad?

Los sistemas de ciberseguridad funcionan de formas muy variadas. Desde el lado preventivo, se encargan de implementar actualizaciones de software o capas de protección para detectar cualquier actividad inusual y bloquearla.

¿Cómo funciona la ciberseguridad?

En la ciberseguridad también se emplea el hacking ético, una práctica que consiste en detectar los puntos vulnerables de un sistema de forma supervisada, a fin de corregirlos.


ETHICAL HACKING
ETHICAL HACKING
ETHICAL HACKING
ETHICAL
HACKING
ETHICAL HACKING
ETHICAL HACKING
ETHICAL HACKING

Hacker ético

Funciones

- Ejecutar periódicamente pentesting o pruebas de penetración
- Monitorear redes para evitar la inyección de código malicioso
- Manejo de sistemas y recuperación de información

Formación

- Grado en Computación, Ingeniería de Sistemas o afines
- Certificaciones y formación en Hacking Ético (CEH EC-C)

Habilidades

- Criptografía
- Análisis de vulnerabilidades
- Monitoreo de redes
- Penetración de redes
- Herramientas de hacking ético (Nmap, Burp Suite, Netsparker)

Salario

Junior:	38.000 $
Medio:	54.000 $
Senior:	80.000 $