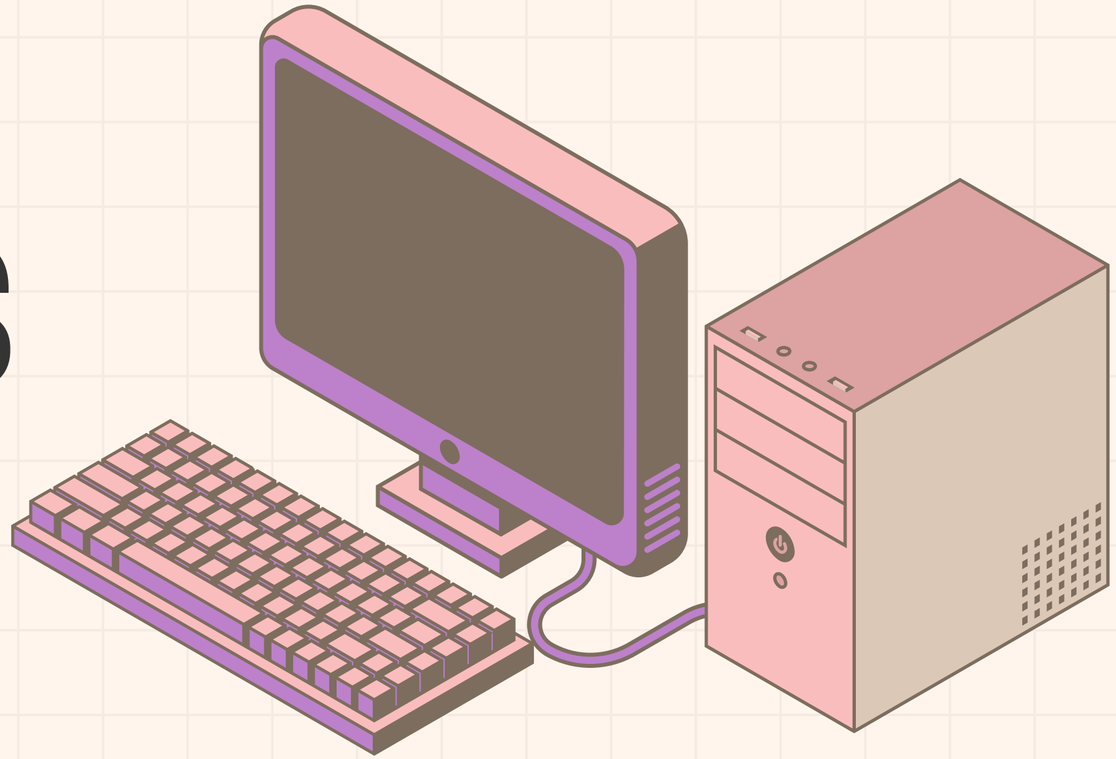
AMENAZAS INFORMATICAS



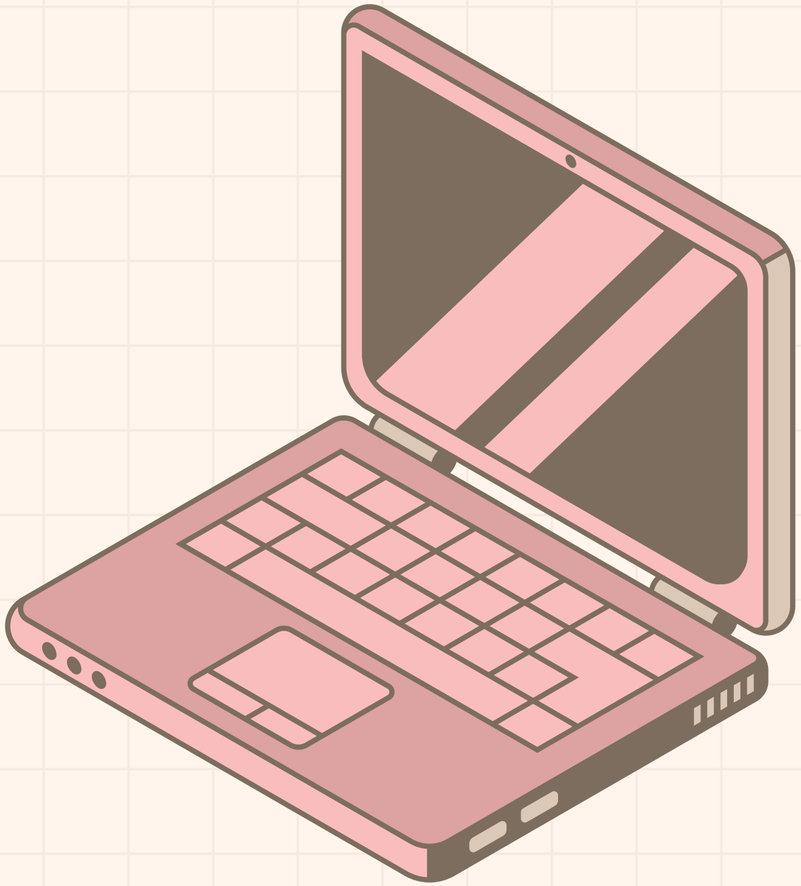
INTEGRANTES:

Carabajal Lourdes
Barin Zoe
Moral Luz
Beron Julieta

DOCENTE: ANDREA GOMEZ
CURSO/AÑO: 3ºA

AMENAZAS

- Backdoors – Barin Zoe
- Ransomware – Berón Julieta
- Troyano –Moral Luz
- Sniffing –Carabajal Lourdes



BACKDOORS

DEFINICIÓN

Un backdoor es una puerta trasera oculta en un sistema informático que permite a los atacantes acceder y controlar un equipo sin ser detectados. Esto les permite ejecutar archivos, robar información y realizar otras acciones dañinas de forma remota y resultando complicado que puedan ser detectados a tiempo

CARASTERISTICAS

- Un rendimiento lento del sistema puede ser un indicio de que se están ejecutando procesos ocultos en el mismo.
- . Es habitual que aparezcan programas desconocidos que han sido instalados sin autorización.
- También pueden darse cambios en archivos y directorios.
- Es posible detectar conexiones de red sospechosas a direcciones IP no conocidas.
- Además, es habitual que surjan pop-ups y mensajes extraños en pantalla.

COMO ES OCASIONADO

El malware con backdoors se distribuye comúnmente a través de correos electrónicos de phishing, descargas mal intencionadas y vulnerabilidades en el software.

Una vez instalado, el backdoor puede persistir utilizando técnicas como la modificación de archivos del sistema o la instalación de servicios ocultos para garantizar que el atacante mantenga el acceso el máximo tiempo posible.

COMO ES POSIBLE EVITARLO

- Mantener el software de protección actualizado a su última versión.
- Usar contraseñas fuertes y autenticación de dos factores.
- Usar herramientas de monitoreo para detectar actividad inusual.
- Configurar correctamente los firewalls para limitar las conexiones no autorizada

https://www.godaddy.com/resources/latam/seguridad/ataque-backdoor-que-es-como-proteger-sistema

RANSOMWARE

DEFINICIÓN

Es un tipo de software malintencionado (malware) que amenaza con bloquear el acceso a un sistema o a datos informáticos, normalmente mediante el cifrado, hasta que la víctima paga una suma al atacante. En muchos casos, la exigencia del rescate viene con una fecha límite.

CARASTERISTICAS

El ransomware , aunque también es malware, es diferente: cifra los datos de la víctima y un hacker exige el pago de un rescate

Solo una vez pagado el rescate, el hacker envía una clave de descifrado para restaurar el acceso a los datos de la víctima.

COMO ES OCASIONADO

puede infectarse con ransomware incluyen: visitar sitios web inseguros, sospechosos o falsos ; abrir archivos adjuntos inesperados o de personas desconocidas.

COMO ES POSIBLE EVITARLO

Realizar copias de seguridad de los datos, actualizar con regularidad el software y utilizar un enfoque de seguridad Zero Trust son formas de evitar que las infecciones de ransomware acaben con una red.

HTTPS://WWW.ESET.COM/ES/CARACTERISTICAS/RANSOMWARE/?SRSLTID=AFMBOOR6TBKBCP8XTE66PWF2MO9HKQ8I-JJKGFODZOP3BIEXH9QMV7AX

SNIFFING

DEFINICIÓN

el sniffing es una técnica de intrusión informática que consiste en interceptar y analizar el tráfico de datos que circula por una red, con el objetivo de obtener información sensible como contraseñas, datos bancarios o información personal

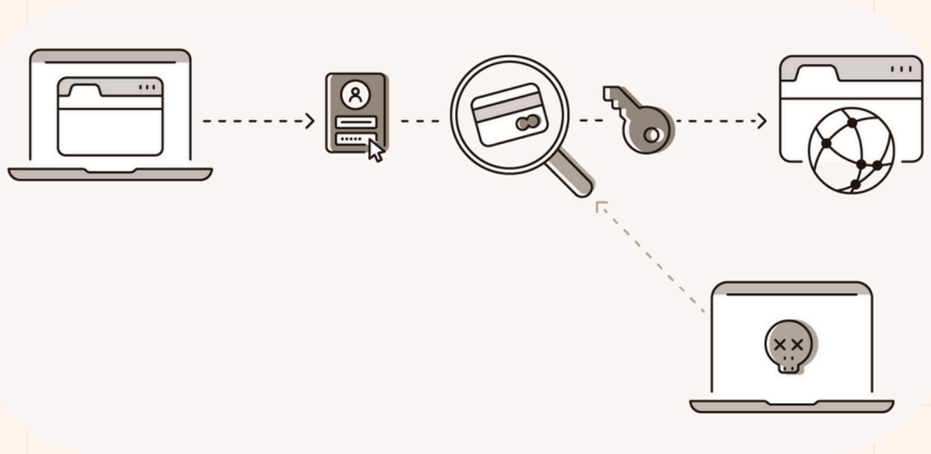
CARASTERISTICAS

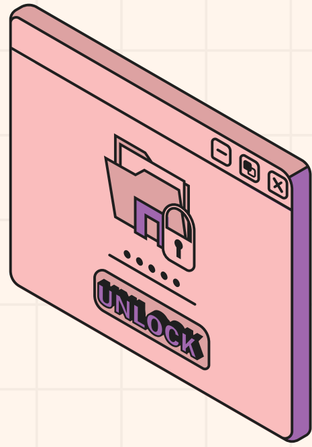
Permite interceptar la información que va de un punto a otro en una red, especialmente si no está cifrada.

Suele ser difícil de detectar porque el atacante no modifica los datos, solo los observa.

Utiliza software especializado,se lleva a cabo con herramientas como Wireshark, tcpdump, Cain & Abel, entre otras.

Amenaza la privacidad y seguridad,pone en riesgo información sensible de usuarios y organizaciones.





COMO ES OCASIONADO

El sniffing es ocasionado cuando un atacante logra interceptar el tráfico de red, aprovechando fallas de seguridad o malas configuraciones en los dispositivos o redes.

Redes sin cifrado
Protocolos inseguros
Conexión a dispositivos comprometidos
Uso de herramientas de sniffing
Falta de medidas de seguridad

COMO ES POSIBLE EVITARLO

Usar conexiones cifradas (HTTPS, SSL/TLS)
Asegurate de que los sitios web que visites empiecen con https://. Eso significa que los datos están cifrados y no pueden ser leídos fácilmente si son interceptados.

Evitar redes Wi-Fi públicas o abiertas
Estas redes suelen ser inseguros y fáciles de espiar. Si tenés que usarlas, no ingreses contraseñas ni datos sensibles.

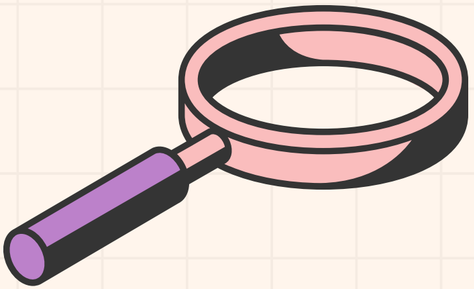
Usar una VPN (Red Privada Virtual)
Cifra todo tu tráfico de internet, incluso si estás en una red pública. Es una de las mejores defensas contra el sniffing.

https://www.redseguridad.com/actualidad/sniffing-que-es-como-evitar_20230713.html

TROYANO

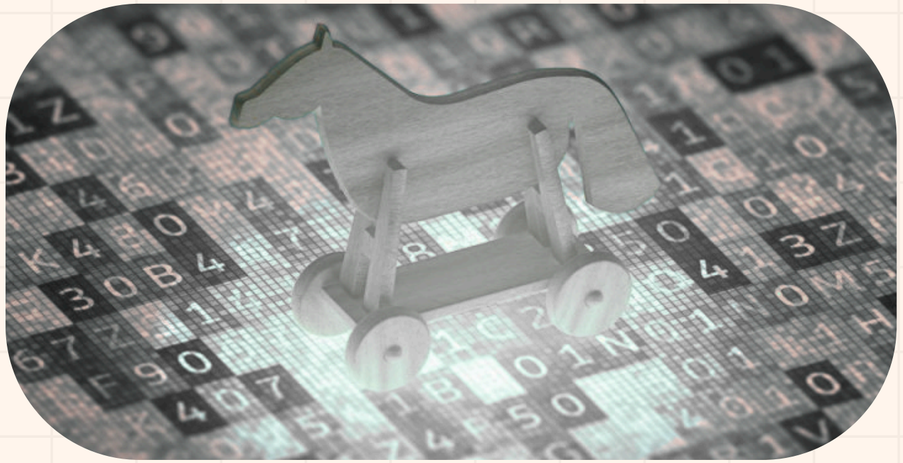
DEFINICIÓN

es un tipo de malware que se disfraza como un programa legítimo para engañar al usuario y obtener acceso a su sistema.



CARASTERISTICAS

Suele infiltrarse a través de correos electrónicos de suplantación de identidad (phishing), intercambio de archivos en redes infectadas y parches de software.
Su objetivo es robar datos confidenciales y compartirlos con hackers.
También puede brindarles acceso remoto a los hackers para llevar a cabo tareas dañinas.



COMO ES OCASIONADO

Un usuario descarga desde un sitio web no confiable un programa cuyo editor es desconocido. Los atacantes instalan un troyano aprovechando una vulnerabilidad del software o mediante un acceso no autorizado. Los hackers crean una red Wi-Fi falsa que se parece a una a la que el usuario está intentando conectarse.

COMO ES POSIBLE EVITARLO

Seguridad en línea

- Instala software antivirus
- Actualiza tu sistema operativo
- Descarga software de fuentes confiables

Prácticas seguras

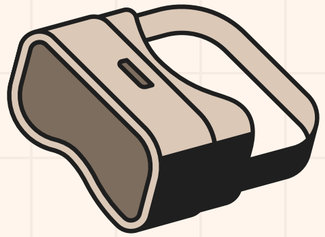
- Utiliza contraseñas fuertes:
- No compartas información sensible
- Utiliza una VPN

Precauciones al abrir archivos

- 1Verifica la fuente
- No abras archivos adjuntos sospechosos

https://www.fortinet.com/lat/resources/cyberglossary/trojan-horse-virus

STUDIO
SHODWE



¡GRACIAS!