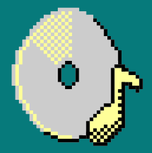
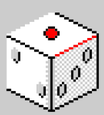



RANSOMWARE

WEB II

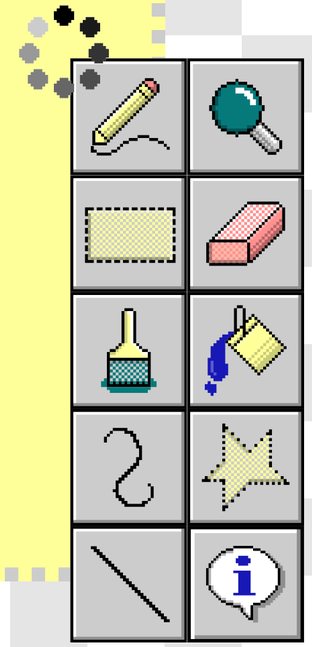


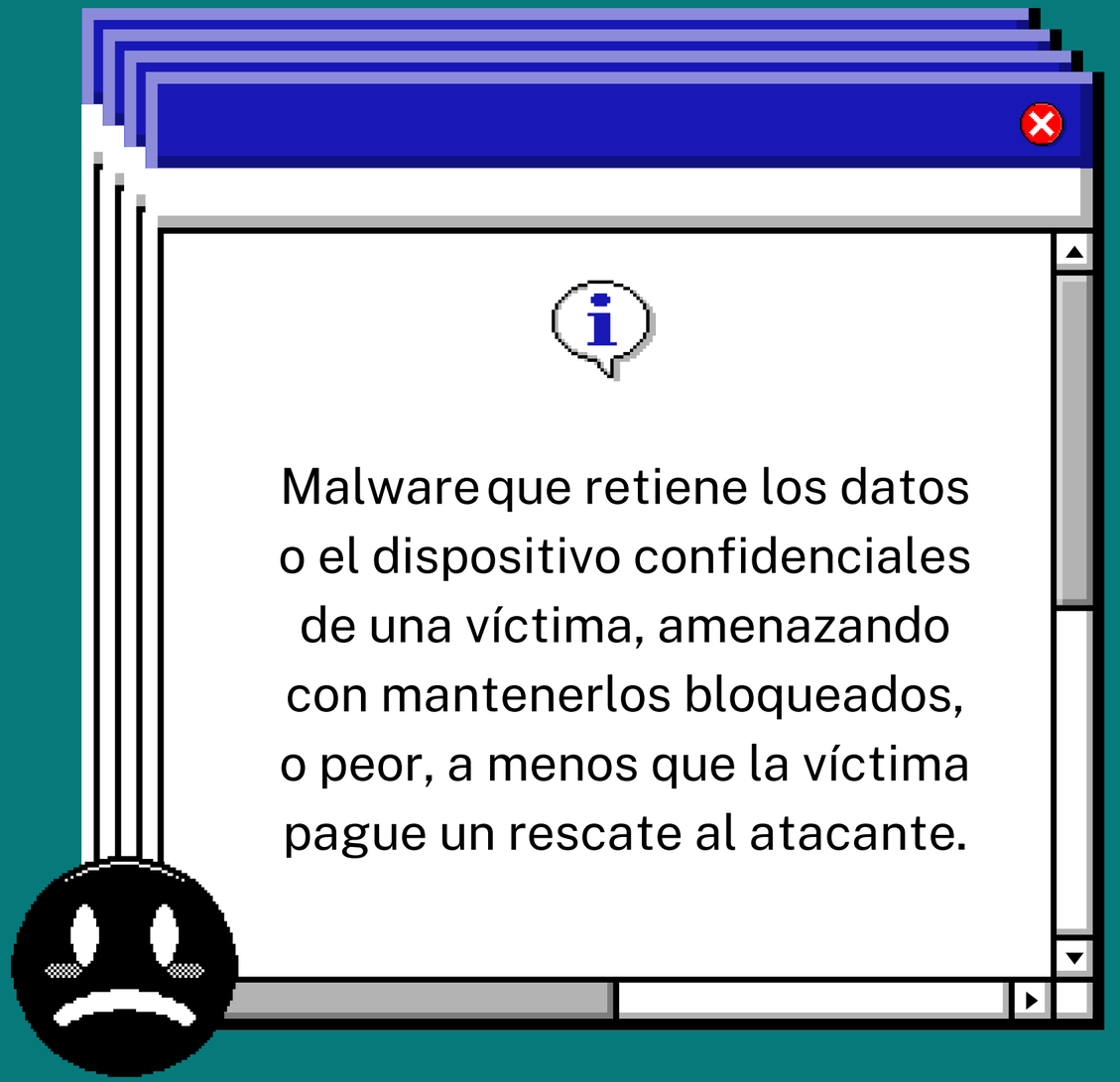
11:11 AM

ransom = rescate

malware = software malicioso



Secuestro Digital



casi el 100% de los rescates se exigen en criptomonedas (como Bitcoin o Monero) para que el rastro del dinero sea imposible de rastrear.

Vuelve a la página Agenda

CARACTERISTICAS

Cifrado Robusto

Utilizan algoritmos de grado militar (como AES-256 o RSA).

Doble (y Triple) Extorsión

Bloqueo de datos además de amenazar con filtrar información

Ransomware-as-a-Service (RaaS)

Los desarrolladores del software "alquilan" el código a otros criminales

CASOS REALES

DragonForce

Junio de 2025

"servicio de análisis de datos" para crear materiales de extorsión personalizados para aliados

Grupo de ransomware y un "cartel"

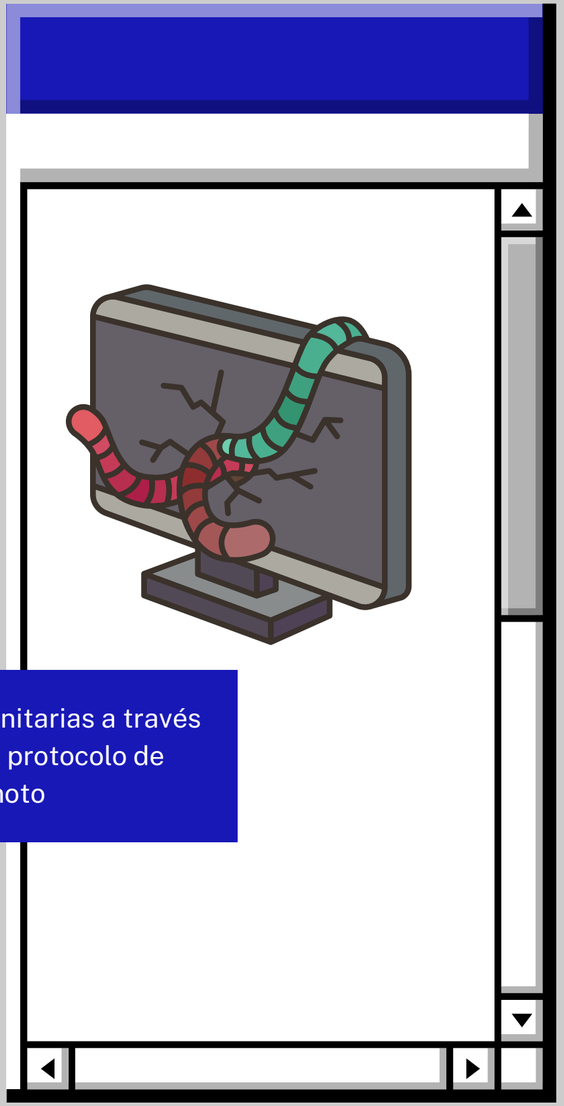
Ataques a conocidos minoristas del Reino Unido

GoodWill
2023

No obligaba a las víctimas a pagar dinero, que pedía que realizaran alguna obra benéfica.

MedusaLocker
2023

Ataco a organizaciones sanitarias a través de vulnerabilidades del protocolo de escritorio remoto



Akira

Principios de 2023

Ataque a pequeñas y medianas empresas de varios sectores

Cifró archivos con la extensión "**.akira**" y exigía pagos en bitcoins

2024
Había comprometido a más de 250 organizaciones y reclamó aproximadamente 42 millones de dólares

FORMA DE ATAQUE

PUERTA

Phishing
Vulnerabilidades de Software
RDP (Remote Desktop Protocol)

Reconocimiento y Movimiento Lateral

Obtiene permisos de administrador.
Salta de una computadora a otra.
El atacante busca y borra o cifra las copias de seguridad.

Exfiltración de Datos

Los criminales copian archivos sensibles y los suben a sus propios servidores.dística destacada.

.wannacry
.locky
.badrabbit.

Cifrado

El malware comienza a transformar cada archivo en código ilegible.

.dragonforce
.interlock
.medusa
.ryuk
.locked

Extorsión

El malware cambia el fondo de pantalla de la víctima o deja archivos de texto llamados LEEME_PARA_RECUPERAR.txt.

OJO CON...

Vulnerabilidades no parcheadas

expuestos a internet sin actualizaciones de seguridad

Ej Pishing

Word, Excel o PDF falso). Al abrirlo, el malware se descarga en segundo plano.

La evolución del ataque

buenos respaldos (backups).

Doble extorción:

"Paga el rescate para recuperar tus datos. Y si usas tus propios respaldos y decides no pagarnos, publicaremos toda la información de tus clientes en internet"

Triple extorción:

(Ataque DDoS) para tirar su página web y presionarlos aún más a pagar

Casos

El Hackeo a PEMEX (2019)

Víctima de un ataque de ransomware llamado DoppelPaymer.

impacto:

pantallas bloqueadas. PEMEX tuvo que apagar miles de computadoras administrativas a nivel nacional para evitar que el virus se propagara a los sistemas

rescate:

Los atacantes exigieron 565 Bitcoins (que en ese momento equivalían a casi 5 millones de dólares). PEMEX declaró públicamente que no pagaron el rescate y tuvieron que formatear y recuperar la información desde cero.

- Definición
- Objetivo principal
- ¿Necesita acción humana para propagarse?
- Impacto visible

GUSANO

- La categoría principal (Software malicioso).
- Causar daño, espiar o robar (general).
- Depende del tipo.
- Variado.

Enfermedad

MALWARE

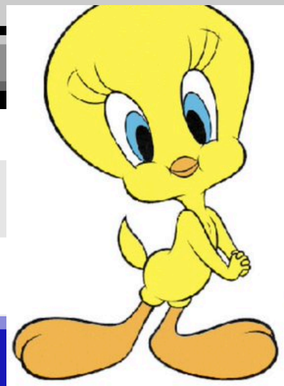
- Un tipo específico de malware.
- Multiplicarse e infectar toda una red rápidamente.
- No, busca vulnerabilidades y salta solo de PC en PC.
- Lentitud extrema en la red y colapso de servidores.

RANSOMWARE

- Un tipo específico de malware.
- Secuestrar datos para cobrar un rescate.
- Sí, suele requerir que la víctima ejecute el archivo infectado.
- Pantalla de bloqueo con una cuenta regresiva para pagar.

¡Muchas gracias!

Inserta aquí un mensaje de despedida o llamada a la acción.



PREGUNTAS (fáciles)
COMENTARIOS (bonitos)
CRÍTICAS (constructivas)
APORTACIONES (monetarias)