NAJERA SOLUTIONS

RANSOMWARE

ataques digitales explicados

01

Ataques por correos electrónicos phishing

Los **ciberdelincuentes envían correos electrónicos** aparentemente legítimos pero diseñados para engañar a los usuarios. Estos correos pueden incluir **enlaces maliciosos** o **archivos adjuntos infectados**.

El **ransomware se activa** en el dispositivo y el malware **cifra rápidamente** los archivos del usuario, **impidiendo su acceso** normal.

¡Manten actualizado tu software de seguridad!

02

Ataques por vulnerabilidades en software y sistemas operativos

Estas vulnerabilidades son como **puertas traseras** que los hackers pueden abrir para **ingresar a tu sistema sin permiso**, utilizan técnicas avanzadas para conectarse a tu computadora, una vez dentro, pueden **instalar el ransomware** y comenzar a **cifrar tus archivos.**

¡Ten actualizados tus equipos!

03

Ataques por sitios web maliciosos

Al visitar un **sitio web comprometido**, el ransomware puede intentar **descargar automáticamente archivos maliciosos** en tu computadora sin tu conocimiento.

Estos archivos pueden **contener el código del ransomware** que luego se ejecuta y cifra tus archivos.

¡Mantén tu navegador web y plugins siempre actualizados!

04

Ataques a través de los Active Directory

Los ciberdelincuentes **aprovechan debilidades** como **contraseñas débiles** o **sistemas sin actualizar**, generalmente entran a través correos engañosos o explotando los **errores de seguridad.**

De igual manera intentan **desactivar o cifrar** los sistemas de respaldo que están integrados con los **Active Directory.**

¡Monitorea tu servidor, detecta vulnerabilidades y fortalece tus contraseñas!