**¿Qué tipo de amenaza es?**

Un ataque Ransomware:

Básicamente, el ransomware es un software malicioso que al infectar un determinado equipo le da al hacker la capacidad de bloquear una computadora desde una ubicación remota, encriptar todos los archivos y quitarle al usuario el control de toda la información y datos almacenados.

Para desbloquearlo el virus lanza una ventana emergente en la que generalmente pide el pago de un rescate.

**¿Cómo comienza y cómo se propaga esta amenaza?**

Este tipo de software tiene la capacidad de camuflarse dentro de otro archivo o programa que invite al usuario a hacer click:

Archivos adjuntos en correos electrónicos, videos de páginas de dudoso origen o incluso en actualizaciones de sistemas y programas en principio fiables como Windows o Adobe Flash.

Una vez que ingresó en el sistema, el virus se activa y provoca el bloqueo de todo el sistema operativo y lanza el mensaje de advertencia.

El mensaje no siempre es el mismo y puede variar en función del tipo de ransomware.

**¿Hay más de una amenaza aplicada?**

El ransomware tiene doble amenaza: la primera es que te encriptan los datos y podes perder toda tu información, y la otra es que pueden publicar información sensible en la dark web o en internet.