RANSOMWARE

Es un tipo de software malicioso que se introduce en los equipos impidiendo el acceso a la información, generalmente cifrándola, y solicitando un rescate para que vuelva a ser accesible.

CÓMO FUNCIONA

Método de propagación: el más común es mediante el envío de ***correos maliciosos*** a las víctimas, que son engañadas para que abran ***archivos adjuntos infectados*** o hagan ***clic en un vínculo*** que les lleva al sitio web del atacante, donde se infectan.

Una vez en el equipo, el ransomware trata de extenderse por la red infectando a otros equipos.

El ransomware **cifra** archivos o todo el disco duro, impidiendo que el usuario acceda a sus ficheros, solicitando pagar un **rescate** para recuperar el acceso al sistema y los ficheros.

CÓMO ACTUAR

Desconecta el equipo de la red.

Si has sido infectado con un ransomware desconecta el equipo de la red (por cable o wifi) y comunícalo a tu Centro de Atención a Usuarios de Informática.

En general, ante cualquier tipo de sospecha de poder estar infectado con software sospechoso, contacta con tu Centro de Atención a Usuarios de Informática.

CÓMO PREVENIR

No hacer clic en enlaces desconocidos o en archivos adjuntos sospechosos.

Evitar hacer clic en enlaces de correos sospechosos o en sitios web desconocidos.

No abrir archivos adjuntos que soliciten activar macros.

No utilices software de origen dudoso.

Muchos sitios de intercambio de software no oficiales distribuyen software modificado que incorpora software malicioso.

No uses dispositivos externos desconocidos.

Conectar memorias USB u otros soportes de almacenamiento externos es un peligro si no sabemos de dónde provienen. A veces los ciberdelincuentes los infectan dejándolos en lugares públicos para incitar a que alguien lo use.

Mantén las aplicaciones y sistemas operativo actualizados.

Asegúrate de que dispones de las actualizaciones y parches de seguridad más recientes.

Evita revelar información personal.

Los ciberdelincuentes recopilan información para utilizarla después y elaborar correos personalizados de spam y phishing.

Si dudas sobre si el contenido de un correo es legítimo, aunque sea de un contacto conocido, contacta directamente con el remitente para contrastarlo.