PROTECCIÓN ANTE EL SECUESTRO DE INFORMACIÓN O RANSOMWARE

En los últimos años, se ha dado un aumento de ataques de secuestro de información o Ransomware, un software malicioso que infecta un equipo y lo bloquea desde una ubicación remota y encripta los archivos y datos ubicados en equipos como computadoras, servidores, medios externos de almacenamiento, quitándole el control al usuario.

El virus lanza un mensaje emergente, en el que pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (bitcoins por ejemplo). A cambio, el criminal promete entregar al usuario la clave que le permitirá desbloquear su dispositivo, cosa que no siempre sucede.

Ejemplo de un equipo con sistema operativo Windows infectado con Ransomware Wannacry:

¿CÓMO LLEGA EL RANSOMWARE?

- En un archivo adjunto a través de correos electrónicos.
- Como consecuencia de visitar un sitio web que contiene un programa malicioso.
- A la hora de descargar un archivo infectado que se presenta al usuario como un programa legítimo e inofensivo.

¿CÓMO PROTEGERSE O PREVENIR UN ATAQUE DE RANSOMWARE?

- No visite sitios web de dudosa procedencia.
- No descargue archivos ejecutables o de otro tipo de dudosa procedencia
- Actualice su equipo con los parches de seguridad brindados por la empresa correspondiente del sistema operativo.
- Proteja su equipo con un antivirus y verifique mediante el ícono que esté activo. Configure las actualizaciones automáticas.

SEPA RECONOCER UN CORREO FALSO

- Revise detenidamente el dominio del correo electrónico del remitente: preste especial atención a la cuenta del dominio que está después del signo de arroba (@) y desconfíe de direcciones de correo desconocidas.
- Corrobore el nombre de la empresa o institución de la que proviene el correo: en ocasiones, los correos maliciosos utilizan nombres similares a los reales con el fin de engañar al usuario, por ejemplo cambiar Centro de Informática por Centro de Información.
- Lea detenidamente el cuerpo del correo: los correos falsos suelen tener errores ortográficos o de gramática.
- No se deje presionar: las instituciones o empresas no presionan a los usuarios para brindar o datos personales vía correo electrónico.
- Cuidado con enlaces falsos: antes de dar clic en los enlaces incluidos en los correos electrónicos, coloque el cursor sobre el vínculo y asegúrese de que la dirección URL que aparece sea la misma que figura en el texto del vínculo.
- Cuando utilice enlaces contenidos en el correo, asegúrese que son sitios calificados como seguros por medio del "candado" o "etiqueta verde" que muestran los navegadores casi siempre en la barra de navegación.
- No descargue archivos si no está seguro de su contenido, más si son archivos ejecutables, con extensión (.exe), estos son los principales responsables de las infecciones por correo electrónico.

Como recomendación general, uno de los métodos claves para evitar problemas de este tipo es disponer de copias de seguridad de sus datos (respaldos) en discos externos, almacenamiento en la nube, dispositivos USB, DVD y/o sistemas de respaldos automáticos.

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
UNIVERSIDAD DE COSTA RICA
CI
Centro de **Informática**