PREVENCIÓN DE SECUESTRO DE INFORMACIÓN (RANSOMWARE)

SECUESTRO DE INFORMACIÓN o RANSOMWARE es el término para referirse a todo tipo de software malicioso (malware) que daña datos o bloquea la pantalla del equipo para exigir al usuario el pago de un rescate.

- Los códigos que actúan de este modo se conocen como cifradores de archivos.
- Ransomware está dirigido a cualquier sistema operativo, aunque la mayoría de los ataques son orientados a Windows.

Un buen antivirus puede remover el ransomware pero no garantiza la descodificación de los archivos.

MECANISMO DE INFECCIÓN POR RANSOMWARE:

La forma más común de infección es mediante archivos adjuntos o compartidos a través de correos electrónicos no solicitados o al hacer clic en vínculos que aseguran provenir de entidades bancarias o de empresas de mensajería.

La infección también se produce a través la conexión a redes puerto a puerto o peer-to-peer (P2P) para compartir archivos; el malware se hace pasar por claves de activación para programas populares como por ejemplo: Adobe Photoshop y Microsoft Office.

TIPOS DE RANSOMWARE MÁS COMUNES

WANNCRY: El ransomware WannaCry ataca a las redes usando SMBv1, un protocolo que ayuda a los equipos a comunicarse con las impresoras y otros dispositivos conectados a la red.

LOCKSCREEN: bloquea el equipo e impide que se lo utilice hasta que se realice el pago del rescate. Este malware a veces utiliza trucos psicológicos para engañar a la víctima y apresurar el pago.

UCR

SCAREWARE: (programas intimidatorios) es un software que intenta asustar y engañar a las víctimas para que tomen un curso de acción determinado. El más frecuente simula ser un producto antivirus que muestra una advertencia sobre problemas de seguridad presentes en el equipo o smartphone, con la intención de engañar al usuario para que pague a los estafadores o descargue más códigos maliciosos desde la red.

CRYPTOLOCKER: busca una amplia gama de archivos para cifrarlos y, una vez que termina el trabajo, muestra un mensaje donde exige una transferencia electrónica para descifrar los archivos.

CONSECUENCIAS DEL RANSOMWARE:

En la mayoría de los ataques, hay una fecha límite para realizar el pago: si el mismo no se realiza a tiempo,se podría perder el acceso a los archivos de manera permanente.

En la mayoría de los casos, un buen software de seguridad debería ser capaz de quitar el ransomware del equipo. Sin embargo, si se trata de un cifrado sofisticado, los archivos seguirán bloqueados.

El pago del rescate no significa que la víctima recuperará sus archivos ni que esté fuera de peligro. El pago podría favorecer otro ataque en el futuro.

La mejor recomendación es la prevención utilizando software de seguridad y respaldos.

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