Aviso importante sobre malware de tipo "Ransomware"

¿Qué es el Ransomware?

El **Ransomware** es un tipo de software malicioso que al infectar un equipo permite a los ciberdelincuentes la capacidad de bloquearlo desde una ubicación remota y encriptar/cifrar los archivos quitando al usuario el control de toda su información y datos almacenados. Algunos tipos de Ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar un rescate económico para poder recuperar su información.

¿Qué efectos tiene?

Una vez que un malware de este tipo entra en la red de una organización, se puede transmitir entre sus ordenadores con sistema Windows a través de una vulnerabilidad para la que existe una solución (una actualización del sistema).

Si un equipo se infecta, se cifrarán y quedarán inutilizables tanto sus ficheros como los de los dispositivos (pendrives, disco duros externos, carpetas de red compartidas, Google Drive, Dropbox…) a los que tenga acceso. Actualmente no se conoce una forma de recuperar esta información salvo a partir de una copia de seguridad.

¿Qué debo hacer para prevenir?

Para evitar verse infectado por éste y otro tipo de malware le recomendamos que siga las recomendaciones publicadas en la guía práctica:

- Recomendaciones generales de seguridad

Más información

- CCN-CERT: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
- Microsoft: https://blogs.technet.microsoft.com/microsoftlatam/2017/05/13/orientacion-al-cliente-para-ataques-wannacrypt/

Enlaces relacionados

- Guías de Seguridad UJA - Ransomware