CONSEJOS

EUROPOL EC3 | European Cybercrime Centre

para prevenir que el ransomware infecte tus dispositivos electrónicos

El ransomware es un tipo de malware que puede bloquear tu ordenador o dispositivo móvil, o puede también encriptar tus archivos electrónicos, solicitando el pago de un rescate económico (dentro de un breve plazo de tiempo) a través de ciertos métodos de pago online para recuperar el control sobre el sistema o la información.

Se puede descargar mediante actualizaciones falsas de aplicaciones o visitando páginas web infectadas. También puede ir oculto en adjuntos de un correo, en correo spam o incluso puede descargarse a través de otro malware, por ejemplo un troyano o un gusano.

Es un programa informático diseñado por los grupos de crimen organizado para generar grandes beneficios. Para prevenir y minimizar los efectos del ransomware, sigue las siguientes recomendaciones:

SIEMPRE

REALIZA ACTUALIZACIONES DE SOFTWARE REGULARMENTE.

Muchas de las infecciones por malware son resultado de la explotación de vulnerabilidades en navegadores web, sistemas operativos, herramientas habituales, etc. Cuando tu sistema operativo o aplicaciones actualicen a una nueva versión, instálalas. Y si el software tiene la opción de actualizarse automáticamente, úsala.

UTILIZA UN BUEN SOFTWARE ANTIVIRUS.

Instala tanto un antivirus (AV) como un cortafuegos. El AV ayudará a frenar los tipos más comunes de malware. Escanea siempre con el AV los archivos descargados en tu ordenador. Asegúrate de mantener actualizada la protección, de lo contrario ésta no podrá reconocer las nuevas amenazas.

CONSULTA Y DESCARGA SOFTWARE SÓLO DE SITIOS OFICIALES.

Acude a websites oficiales y seguras para mantener tu software al día con las últimas actualizaciones de seguridad. Descarga siempre la versión oficial de los programas informáticos.

HAZ COPIAS DE SEGURIDAD REGULARMENTE.

Contar con un sistema de recuperación de datos impedirá que una infección de ransomware pueda destruir tus archivos para siempre. Es recomendable crear dos copias de seguridad: una para ser almacenada en la nube (recuerda usar un servicio que realice automáticamente copias de tus archivos) y otra en un dispositivo físico (disco duro portátil, memoria USB, otro equipo portátil, etc.). Desconéctalos de tu PC cuando se haya realizado la copia.

DENUNCIA.

Si eres víctima de ransomware, denúncialo inmediatamente a los servicios policiales. Cuantos más datos puedas facilitar, más eficientemente se podrá llevar a cabo la investigación para identificar y arrestar a los presuntos autores.

CONSULTA A TU PROVEEDOR DE ANTIVIRUS CÓMO DESBLOQUEAR Y REMOVER LA INFECCIÓN.

Existen numerosos blogs y websites oficiales que facilitan instrucciones para remover este tipo de malware. Visita la página www.nomoreransom.org para saber si existe una herramienta gratuita para desencriptar la variante de ransomware que está afectando a tu ordenador.

NUNCA

PINCHES EN ADJUNTOS, VENTANAS EMERGENTES O LINKS SIN CONOCER SU ORIGEN.

Un anuncio aparentemente inofensivo o una foto pueden en realidad dirigirte hacia una página web desde la cual se descargue el malware automáticamente. Lo mismo puede ocurrir al abrir archivos adjuntos recibidos por correo electrónico.

INSTALES APPS EN TU DISPOSITIVO MÓVIL QUE NO PROVENGAN DE SITIOS OFICIALES.

Evita las descargas que no sean de fuentes de confianza. Si tienes un teléfono o tablet Android, recuerda desactivar la opción "Fuentes desconocidos" y activar "Verificar aplicaciones".

CREAS TODO LO QUE VES.

Desconfía si una página web te indica que tu antivirus u otros programas instalados en tu ordenador están desactualizados (drivers, codecs, etc.). Es muy fácil para los piratas informáticos crear logos o mensajes falsos. Una exploración rápida de tu dispositivo puede confirmarte si tu software realmente necesita ser actualizado o no.

INSTALES O EJECUTES SOFTWARE DESCONOCIDO.

No instales programas o aplicaciones en tu ordenador sin saber de dónde proceden. El software gratuito se utiliza a menudo para atraer a víctimas confiadas. Algunos tipos de malware pueden instalar programas ocultos con el fin de robar tu información personal.

PAGES EL RESCATE.

Pagar no te garantiza el acceso a los archivos afectados, y tu dispositivo puede seguir infectado igualmente. Además, estarás financiando las actividades ilegales de los piratas informáticos y promoviendo su modelo de crimen organizado.

Created by Europol