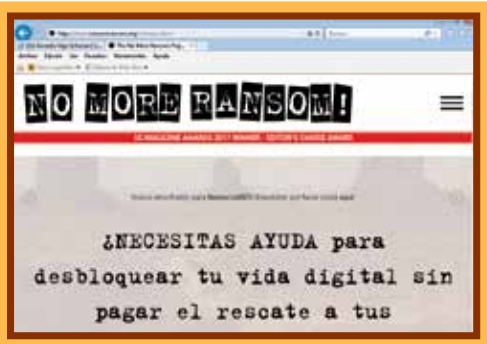
El valor de la colaboración

https://www.nomoreransom.org



De todos es ya conocido el efecto tan negativo en nuestras organizaciones y en nuestros hogares del software malicioso que cifra nuestros ficheros a la espera de que realicemos un pago, casi siempre en Bitcoin o similar, para recuperarlos. Una plaga que, aprovechándose de la existencia de vulnerabilidades no parcheadas en los sistemas operativos, cercena el acceso a nuestros datos, tanto corporativos como personales, independientemente de si tenemos o no copias en algún lugar seguro.

Las cifras de las pérdidas corporativas ocasionadas por estos programas de cifrado son cada vez más altas. En ocasiones, el valor emocional de los ficheros perdidos, en especial si son personales (fotos, apuntes, etc.) llega a ser comparable. El número de contagios sigue en aumento. Es todo un gran negocio; eso sí, ilegal. Probablemente el negocio ciberilegal tiene el ratio lucro/riesgo asumido más elevado. **Europol**, en su informe sobre esta industria, menciona a cuatro familias de software malicioso de cifrado pioneras: CryptoLocker, CryptoWall, TeslaCrypt y CTB-Locker.

El sitio web **nomoreransom.org** es un valioso proyecto fruto de la colaboración entre compañías de seguridad y policías europeas. Su objetivo es ofrecer ayuda en la prevención de contagio y recuperación de datos cifrados con este tipo de programas dañinos llamados "ransomware". Recomiendo su visita antes de sufrir las consecuencias de este tipo de código.

Nomoreransom.org fue creado en julio de 2016 por la policía holandesa y Europol, con Kaspersky Lab y McAfee como socios tecnológicos y está alojado en las nubes de Amazon y Barracuda. Los servicios que ofrecen son atractivos, no sólo para responsables de seguridad en compañías pequeñas sino también para particulares.

El uso de este sitio es sencillo. El usuario sube uno o dos ficheros cifrados e incluso la dirección Bitcoin proporcionada por el "malware" para pagar el rescate. Con estos indicadores, tratan de averiguar el tipo de *malware* y, si tienen éxito, ofrecen el antídoto en el caso de que esté disponible.

También ofrecen consejos para mitigar el riesgo de pérdida de datos. El más importante es sencillo: realizar con frecuencia copias de respaldo y comprobar su disponibilidad. La primordial medida preventiva es la actualización de software. Para finalizar, confirman la recomendación básica de nunca pagar el rescate.

Alberto Partida
Analista y autor en Seguridad TI
Sígueme en LinkedIn:
http://bit.ly/2partida