Desde que las amenazas con ransomware comenzaron a aparecer por el año 2010, la gente aún no sabe qué hacer exactamente ante una infección de este tipo, si es conveniente o no pagar por el rescate de los archivos.

A finales de 2015, el FBI fue blanco de controversia cuando uno de sus agentes admitió públicamente que la oficina recomendaba, en muchos casos, que las víctimas pagaran las demandas de rescate.

En ese momento, muchos se sorprendieron al descubrir que el FBI les decía a las víctimas que paguen las demandas de ransomware y ayudaba a las bandas criminales a aumentar sus ganancias.

La oficina cambió su postura oficial unos meses más tarde, en 2016, luego de que los senadores estadounidenses enviaran cartas preguntando por qué la agencia estaba ayudando a los delincuentes.

Desde ese momento, la posición oficial del FBI ha sido diferir la decisión de pagar un rescate a la víctima, sin ningún consejo formal. En cambio, la agencia solo ha pedido una cosa, que las víctimas reporten las infecciones, para poder tener una idea de qué cepas y grupos de ransomware son los más activos actualmente, y la amplitud general de la epidemia de ransomware.

La controversia que rodeó el consejo inicial del FBI para lidiar con las infecciones de ransomware ha desencadenado un gran número de debates acerca de los méritos de pagar una demanda de ransomware, y qué postura tienen varias empresas y agencias al respecto.

Microsoft publicó hoy lo siguiente en su blog:

«Nunca alentamos a una víctima de ransomware a pagar ningún tipo de demanda de rescate», dijo Ola Peters, consultor senior de seguridad cibernética para el equipo de detección y respuesta de Microsoft (DART).

> *«Pagar un rescate a menudo es costoso, peligroso y solo reabastecer la capacidad de los atacantes para seguir sus operaciones»,* agregó.

Sin embargo, Microsoft entiende que en muchos casos, las organizaciones a veces solo tienen una opción sobre la mesa: pagar el rescate, ya que no tienen acceso a copias de seguridad recientes, o el ransomware también las cifró.

Pero aún si las víctimas eligen pagar el rescate, Microsoft advierte que *«pagar a los ciberdelincuentes para obtener una clave de descifrado de ransomware no garantiza que se restablecerán sus datos cifrados».*

La clave de descifrado podría no funcionar, la aplicación de descifrado podría contener errores y destruir los datos, o los piratas informáticos podrían haber perdido la clave original y solo estarían llevando a cabo una estafa.

Microsoft pretende que las compañías adopten un enfoque proactivo y traten al ransomware o cualquier otra forma de ataque cibernético como *«una cuestión de cuándo no y cuándo si»*.

La compañía afirma que las empresas deberían invertir en minimizar la superficie de ataque y en crear una estrategia de respaldo sólida para que puedan recuperarse de cualquier ataque. Microsoft recomienda que las compañías sigan seis pasos simples para prepararse para responder a un ataque de ransomware.

1.- Usar una solución efectiva de filtrado de correo electrónico
2.- Parcheo regular de sistemas de hardware y software y administración efectiva de vulnerabilidades
3.- Utilizar un antivirus actualizado y una solución de detección y respuesta de punto final (EDR)
4.- Separar las credenciales administrativas y privilegiadas de las credenciales estándar
5.- Implementar un programa efectivo de lista blanca de aplicaciones
6.- Hacer copias de seguridad de forma regular de los sistemas y archivos críticos.