La semana pasada, Pemex sufrió un ataque con ransomware en el que los hackers pedían 5 millones de dólares en Bitcoin como rescate.

Sin embargo, este no es el primer ataque que registra Petróleos Mexicanos, ya que según el Informe de Rendición de Cuentas de Conclusión de la Administración 2012-2018, hasta ahora la compañía había prevenido el 100% de un total de 600 mil casos mensuales.

> *«Se ha fortalecido la seguridad de la información, con los que se previno el 100 por ciento de los más de 600 mil ataques mensuales en promedio, a los 160 portales de Pemex. Asimismo, se evitó el secuestro (WannaCry 1&2) de la información en los 46 mil equipos de cómputo».*

El documento especifica que hasta el año pasado, la infraestructura base que soportaba y permitía la continuidad operativa asociada a las telecomunicaciones de Pemex, consideraba 472 estaciones de microondas y 20 mil radios trucking.

Además de los dispositivos que permiten la comunicación en centros operativos industriales, 4,523 puntos de acceso a Internet, 1024 puntos de colaboración por videoconferencia y 72 mil servicios telefónicos, además de una red de datos con capacidad de 120 mil puertos.

El equipo de cómputo para usuario final consistía en 32,408 equipos bajo el esquema de servicio administrado y 14,522 que son propiedad de la petrolera nacional, las cuales soportaban la funcionalidad y colaboración de más de 65 mil usuarios.

Por otro lado, Kaspersky, la compañía de seguridad cibernética, afirma que en los primeros seis meses de 2019, sus productos de seguridad se activaron en 41.6 por ciento de las computadoras con sistemas de control industrial (ICS), en el sector energético.

La compañía dice que entre los programas maliciosos que fueron bloqueados, los que representaban el mayor peligro eran extractores de criptomonedas, en 2.9 por ciento de los casos, mientras que los gusanos representaron el 7.1 por ciento y una variedad de spyware

versátil con el 3.7 por ciento.

Entre el malware identificado, se encuentra AgentTesla, un troyano especializado, diseñado para robar datos de autenticación, capturas de pantalla y datos capturados por la cámara web y teclado.