Petróleos Mexicanos (Pemex), fue víctima de un ataque cibernético con ransomware durante este fin de semana, afectando la distribución de combustibles a gasolineras de todo el país.

En un principio, Pemex trató de esconder el hecho, pero con el paso de las horas se ha vuelto más evidente e incontrolable, aún después de haber comunicado el lunes que todo estaba normalizado.

Este martes, miles de trabajadores de Pemex estaban sin hacer nada, debido a que sus computadoras no funcionan, pues fueron secuestradas por un ransomware. En la Torre de Pemex, en la Ciudad de México, varios pisos tienen hasta el 60 por ciento de las computadoras inutilizables.

Pemex asegura que los hackers solo afectaron el cinco por ciento de sus computadoras, pero la realidad es que existen alrededor de 59 mil computadoras en Pemex, y de esas, alrededor de 10 mil han resultado afectadas, según funcionarios de Pemex, que pidieron no ser identificados por temor a represalias.

En las pantallas de las computadoras infectadas, aparece un mensaje en inglés referente a supuestos hackers de «Tor Project», que explican los pasos a seguir para recuperar el control de la máquina. Según los piratas, al no seguir las indicaciones, los usuarios podrían perder para siempre sus archivos. *«Mientras más pronto nos contactes, puedes esperar un precio menor»*, dice el mensaje.

Hasta el momento, ningún sistema de las plantas industriales ha sido afectado, sólo equipos de cómputo, aunque esto ha causado graves problemas, pues afecta sistemas como el de facturación, que a su vez afectó la venta de gasolina.

> *«Pemex opera con normalidad, el domingo recibió intentos de ataques cibernéticos que fueron neutralizados oportunamente, afectando el funcionamiento a menos del 5% de los equipos personales de cómputo. No obstante lo anterior, Pemex reitera que la producción, abastecimiento e inventarios de combustible están*

> *garantizados»,* dice el comunicado oficial.

Los hackers pidieron 5 millones de dólares

Los hackers responsables del ataque a Pemex solicitaron un pago de 5 millones de dólares, según informó la agencia Reuters, agregando que Pemex perdió el plazo para obtener un *«precio especial»*.

Las computadoras afectadas muestran instrucciones para acceder a un sitio web vinculado a *«DoppelPaymer»*, un tipo de ransomware.

En ese sitio web, los piratas informáticos pedían 565 bitcoins, equivalentes a unos 5 millones de dólares, dando un plazo de 48 horas a la petrolera para realizar el pago.

Reuters contactó a los hackers y estos explicaron que Pemex perdió el plazo para obtener un «precio especial», en una referencia al descuento que ofrecen a las víctimas de ransomware por un pago anticipado.

Entre las tantas mentiras por parte de Pemex y funcionarios relacionados, hubo una confusión sobre el tipo de ransomware que infectó las computadoras. Un funcionario de Pemex mencionó en un correo electrónico interno que la compañía fue atacada por *«Ryuk»*, una variante de ransomware que según expertos, apunta a compañías con ingresos anuales de entre 500 y 1,000 millones de dólares.

Por otro lado, DoppelPaymer es un ransomware más nuevo, que según CrowdStrike, estuvo detrás de los ataques contra el Ministerio de Agricultura de Chile y la ciudad de Edcouch en Texas.

Pemex estuvo comunicándose con sus empleados por medio de WhatsApp, ya que los empleados no podían abrir sus correos electrónicos, dijo otra fuente a periodistas locales.

Esto deja en claro la poca capacidad por parte de los encargados de seguridad de la compañía, sin dejar de lado la culpabilidad de Pemex al no querer renovar licencias del software antivirus con el fin de ahorrar algo de dinero.