Hackeo a la eléctrica EDP: piden 10 millones para desbloquear sus archivos

Así ha sido el hackeo a la eléctrica portuguesa EDP, con una petición de rescate de unos 10 millones de euros para desbloquear sus archivos

La empresa eléctrica portuguesa EDP ha sufrido un ataque hacker. Concretamente, un ciberataque **mediante ransomware**, el mismo malware que se usó para el ciberataque que Europa recibió meses atrás.

Los ciberdelincuentes no sólo han conseguido robar una cantidad ingente de información, sino que además le piden a la eléctrica EDP **unos 10 millones de euros** para desbloquear sus archivos secuestrados mediante cifrado, tal y como cuenta la web especializada en ciberseguridad BleepingComputer.

El ciberataque, que se produjo a principios de semana, ha robado unos **10 terabytes de información** de calado importante para la firma. De hecho, sus sistemas están encriptados y los mismos autores han advertido a la firma que no intenten descifrar sus archivos sin que la empresa les pague dicho rescate, que por cierto, piden en forma de criptomoneda.

La eléctrica EDP, hackeada

La eléctrica, que cuenta con sede en España y que cuenta con más de 1.300 trabajadores opera con alrededor de unos 2 millones de contratos de luz y gas. Su página web no funciona, y no ha sido hasta que BleepingComputer ha dado más detalles que no se ha sabido a ciencia cierta la magnitud del ataque.

El sistema usado para realizar el hackeo ha sido, como ya hemos visto en otras ocasiones, **el ransomware.** Esta técnica consiste en cifrar archivos e información sensible para la compañía y secuestrar tanto estos como los sistemas que los guardan. Después, los autores del ataque piden un rescate millonario para descifrar estos archivos. Las empresas, sobre todo las pymes, suelen ser el principal objetivo de estos ataques.

Esta clase de ataques son capaces de infectar hasta una red informática de equipos bastante grande. Se pretende atacar toda la red de ordenadores, para que el flujo de trabajo se corte y que el pánico de que se pierdan estos archivos motive a las firmas implicadas a pagar los rescates. Rescates que, las autoridades españolas recomiendan no pagar nunca.

Ragnar Locker, el ransomware implicado

El ransomware usado se llama **Ragnar Locker**, y se ha estado usando desde el año 2019. Se suele ejecutar desde **la deep web** y es bastante conocido por estos lares cibernéticos. El comunicado que los hackers han lanzado a EDP a modo de nota de rescate amenaza a la compañía pidiendo un rescate de 10 millones de euros.

El ransomware Ragnar Locker tiene un modo de funcionar muy específico; ataca a las brechas de seguridad de los programas MSP, usualmente empleados por empresas de todo el mundo para gestionar las infraestructuras tanto tecnológicas como digitales de las mismas. Ragnar Locker hace uso de estas brechas para colarse en el sistema e infectar toda la red.

No es para menos; los hackers se enorgullecen de haber sustraido unos **10 teras de información**. Como prueba de ello, han estado filtrando ciertos archivos para mostrar este hecho y para insuflar miedo a la firma. Aquí tenéis un par de archivos y pantallazos de vuestra red, como prueba de nuestra posesión.

Este comunicado es temporal pero será permanente y publicaremos esta filtración en importantes periódicos y blogs. Se lo diremos a todos vuestros clientes, socios y competencia. Depende de vosotros que esto sea confidencial o público, reza la nota que se puede leer en BleepingComputer. Si nos basamos en los archivos filtrados, se puede observar cómo los hackers han cifrado credenciales de trabajadores, notas internas, direcciones de empleados, etcétera.

Los ciberdelincuentes piden que se contacte con ellos mediante el navegador TOR, especializado para poder entrar en la deep web y así comunicarse con los mismos para determinar los detalles del pago del rescate. A modo de sorna, los atacantes han llegado a ofrecer un descuento si se paga en 2 días la increíble cantidad de **9.9 millones de euros** en forma de 1.580 bitcoins. En caso de no hacerlo, el rescate será de un total de 10 millones de euros.

Como decimos, las autoridades recomiendan encarecidamente **no pagar esta clase de rescates**, ya que el pago del mismo no garantiza que se vayan a recuperar los archivos cifrados. Además, pagar esta clase de rescates motiva a los ciberdelincuentes a seguir realizando estas fechorías.

Fuente: El Español