Everis, una de las compañías de consultoría de TI más grande de España, sufrió un ataque con ransomware dirigido este lunes, lo que obligó a la compañía a cerrar todos sus sistemas informáticos hasta que el problema se resuelva completamente.

La compañía informó a sus empleados sobre el ataque cibernético generalizado de ransomware diciendo lo siguiente:

> *«Estamos sufriendo un ataque masivo de virus en la red Everis. Por favor, mantenga las PC apagadas. La red se ha desconectado con clientes y entre oficinas. Lo mantendremos actualizado. Por favor, transfiera urgentemente el mensaje directamente a sus equipos y colegas debido a problemas de comunicación estándar».*

Según el consultor de seguridad cibernética, Arnau Estebanell Castellví, el malware cifró los archivos en las computadoras de Everis con un nombre de extensión similar al nombre de la compañía, es decir, *«.3v3r1s»*, lo que sugiere que el ataque fue selectivo.

Hasta el momento, se desconoce qué familia específica de ransomware se utilizó para atacar a la compañía, pero los atacantes exigieron 750 mil euros, equivalente a unos 835 mil dólares, como rescate para descifrar los archivos.

Sin embargo, considerando la naturaleza altamente dirigida del ataque, el fundador de VirusTotal dijo en Twitter que el tipo de ransomware podría ser BitPaymer/IEncrypt, el mismo malware recientemente descubierto que explota una vulnerabilidad de día cero en el software iTunes e icloud de Apple.

Según informes locales, otras empresas españolas y europeas también se vieron afectadas por un ransomware similar durante el mismo período.

> *«La cadena SER ha sufrido esta mañana un ataque de un virus informático del tipo*

> *ransomware, encriptador de archivos, que ha tenido una afectación grave y generalizada de todos sus sistemas informáticos. Siguiendo el protocolo establecido en los ataques cibernéticos, el SER ha visto la necesidad de desconectar todos sus sistemas informáticos operativos»,* dijo la Cadena SER.

También mencionó que sus *«técnicos ya están trabajando para la recuperación progresiva de la programación local de cada una de sus estaciones».*