Ciberdelincuentes exigen $5 millones por rescate de datos de usuarios de Digitel

El dato más preocupante mostrado por el grupo es que supuestamente tiene en su poder un archivo de Excel de más de 30 GB de peso con datos de los clientes de Digitel, incluyendo edades, números de cédula, nombres, estados donde residen, entre otros

En los últimos días, la operadora Digitel sufrió un fuerte ataque cibernético, mediante el cual los hackers accedieron a prácticamente todo el sistema de la compañía y sus bases de datos, incluyendo la información personal de los usuarios del servicio, por la cual el grupo de ciberdelincuentes exige $5 millones de rescate.

Los atacantes lograron infectar todo el sistema de Digitel con el virus Medusa, que tiene la función de bloquear archivos, encriptándolos, e impedir su acceso a los propietarios originales.

El grupo de piratas digitales publicó en su web —a la cual solo se puede acceder en la darknet con buscadores como Tor— una cuenta regresiva de nueve días para pagar por el rescate de los datos, junto a un perfil de la empresa atacada.

«Digitel es una empresa telefónica de Venezuela fundada en 1995. Cuenta con más de 5 millones de suscriptores y su número de empleados excede las 1.100 personas. La oficina corporativa está ubicada en el Edificio El Cubo Negro, Torre Banaven, Piso

8», es la única información que presenta la publicación, junto a tres opciones de pago.

Los atacantes piden un pago de $100.000 para añadir un día a la cuenta regresiva, $5 millones para borrar todos los datos o $5 millones para descargar los datos.

La empresa no ha hecho pública su respuesta ante la solicitud de rescate. Solo se limitó a publicar un comunicado este jueves 1 de febrero en el que ratificó el bloqueo de los sistemas que soportan algunos canales de atención de la compañía», y que activaron mecanismos de seguridad que «permitieron que la amenaza fuera atendida, impidiendo la vulneración de data de nuestros usuarios».

El grupo de hackers ha publicado durante la última semana capturas de pantalla en el que se evidencia el supuesto acceso con el que cuentan, mostrando la manipulación de la consola de recargas telefónicas (e incluso ofreciendo saldo gratuito a usuarios en X), acceso al dominio con el que controla una red de usuarios y equipos, así como también a la herramienta con la que gestionan los usuarios de los trabajadores de la compañía.

El dato más preocupante mostrado por el grupo, que opera a través de la cuenta @x00x01x01 en la red social X, es que supuestamente tiene en su poder un archivo de Excel de más de 30 GB de peso con datos de los clientes de la empresa, incluyendo edades, números de cédula, nombres, estados donde residen, entre otros; contradiciendo el comunicado de Digitel en el que aseguraban que los datos de los clientes no habían sido vulnerados.

https://talcualdigital.com/hackers-exigen-5-millones-por-rescate-de-datos-de-usuarios-de-digitel/