Garmin, fabricante de relojes inteligentes y wearables, cerró varios de sus servicios hoy para enfrentar un ataque de ransomware que ha encriptado su red interna y algunos servicios de producción.

La compañía está planeando una ventana de mantenimiento de varios días para trabajar con las secuelas del ataque, esto incluye el cierre de su sitio web oficial, el servicio de sincronización de datos de usuario de Garmin Connect e incluso, algunas líneas de producción en Asia.

En mensajes compartidos en su sitio web y en Twitter, Garmin informó que la misma interrupción también afectó a sus centros de llamadas, dejando a la compañía en la situación de no poder responder llamadas, correos electrónicos y chats en línea enviados por los usuarios.

Este incidente ha causado mucho enojo en los clientes de la compañía, pues muchos dependen del servicio Garmin Connect para sincronizar datos sobre carreras y paseos en bicicleta.

Aunque Garmin no confirmó directamente que está sufriendo un ataque por ransomware, varios empleados de la compañía compartieron en sus redes sociales algunos detalles del ataque, citando un ataque de ransomware.

Algunos de los empleados atribuyeron el incidente a una nueva variedad de ransomware que apareció a inicios de 2020, llamada WastedLocker.

iThome, un medio de noticias taiwanés dedicado a temas de TI y dispositivos inteligentes, compartió hoy un memorando interno que el personal de TI de Garmin envió a sus fábricas de Taiwán, anunciando dos días de modo de mantenimiento planeado para el viernes 24 y sábado 25 de julio.

Aunque el memo no especifica que el modo de mantenimiento es debido a un ataque de

ransomware, las fuentes informaron al sitio de noticias que el incidente fue causado por un «*virus*».

Cabe mencionar que actualmente, solo los ataques de ransomware tienen el efecto destructivo de provocar que las empresas cierren las líneas de producción, los servicios en línea, los sitios web, servidores de correo electrónico y los centros de llamadas en cuestión de horas.