Un centro médico que está en espera para ayudar a probar cualquier vacuna contra el coronavirus, fue afectado por un grupo de hackers que propagan ransomware, mismo que prometió no atacar a las organizaciones médicas.

Los piratas informáticos detrás de los ataques con el ransomware Maze, atacaron nuevamente, robando datos de una víctima y publicándolos en Internet para que paguen el rescate exigido.

Los atacantes se habían comprometido a no atacar objetivos médicos y de salud. Sin embargo, su última víctima es Hammersmith Medicines Research, una compañía británica que previamente probó la vacuna contra el Ébola y se encuentra en espera para realizar los ensayo médicos de cualquier vacuna para el COVID-19.

Malcolm Boyce, director clínico de Hammersmith Medicines Research, dijo a Computer Weekly que el ataque cibernético, que ocurrió el 14 de marzo, fue visto en progreso, luego detenido y los sistemas fueron restaurados sin pagar ningún rescate.

> *«Repelimos el ataque y restauramos rápidamente todas nuestras funciones. No hubo tiempo de inactividad»,* dijo.

Los atacantes de Maze aparentemente lograron filtrar datos, en este caso, registros de pacientes, y publicaron algunos de ellos en línea. Boyce dijo a Computer Weekly que los piratas informáticos enviaron archivos de muestra de Hammersmith Medicines Research con detalles de personas que participaron en pruebas entre 8 y 20 años antes. Los operadores de Maze luego publicaron muestras de datos en la deep web.

El FBI advirtió sobre un aumento significativo en las estafas relacionadas con el COVID-19, por lo que alertó a los trabajadores de la salud sobre una nueva campaña de ransomware para Windows que aprovecha los temores causados por el coronavirus y los usan como cebo.

Los operadores de Maze declararon públicamente que *«detendremos toda la actividad frente*

a todo tipo de organizaciones médicas hasta la estabilización de la situación del coronavirus».

John Opdenakker, profesional de seguridad de la información, dijo que no está sorprendido de que los piratas informáticos rompieran su promesa.

> *«La ganancia financiera es, desafortunadamente, el único motivo para los actores criminales. Ellos también saben que las organizaciones médicas se encuentran actualmente en una situación muy vulnerable debido al brote de coronavirus, que solo aumenta la probabilidad de que paguen demandas de extorsión»,* dijo Boyce.

Por su parte, Brett Callow, analista de amenazas de Emsisoft, afirma que *«es casi seguro que los delincuentes aún no han publicado todos los datos robados».*

> *«Su modus operandi es nombrar por primera vez a las compañías a las que han accedido en su sitio web, y si eso no los convence de pagar, publicar una pequeña cantidad de sus datos, que es la etapa en la que parece estar el incidente. Si la compañía aún no paga, se publican más datos, a veces de forma escalonada, para aumentar la presión sobre la compañía»,* dijo Callow.

También dijo que *«el nivel de amenaza es el mismo de siempre, quizás incluso más alto, y los grupos de ransomware no deberían contar con una plataforma que les permita minimizar el hecho».* Mientras tanto, Emsisoft está ofreciendo ayuda a los hospitales y proveedores de servicios de salud afectados por el ransomware de forma gratuita.