Un grupo de hacers que cerraron una instalación de petróleo y gas natural de Arabia Saudita en 2017, ahora está apuntando a las compañías de electricidad de Estados Unidos y Asia, según confirmó la compañía de seguridad cibernética Dragos Inc.

El grupo de piratas informáticos denominado como Xenotime, ha estado investigando servicios públicos desde finales de 2018, aseguró Dragos, con sede en Hanove, Maryland. Se ha centrado principalmente en los sistemas de control electrónico que administran las operaciones en los sitios industriales.

Por otro lado, la compañía de seguridad cibernética FireEye Inc., vinculó al grupo una institución de investigación en Moscú, propiedad del gobierno ruso, llamado Instituto Central de Investigación Científica de Química y Mecánica. Xenotime es uno de los pocos grupo en el mundo que usa malware diseñado para sistemas de control industrial, dijo Benjamin Read, gerente senior de FireEye.

Un portavoz de la embajada rusa en Washington no respondió a la solicitud de comentarios por parte de Bloomberg. Los funcionarios estadounidenses advirtieron durante mucho tiempo que las redes son vulnerables a los ataques cibernéticos.

La interrupción de la infraestructura eléctrica de una región podría causar un caos generalizado, desencadenar apagones y paralizar los mercados financieros, los sistemas de transporte, entre otros.

> *«La mayoría de los hackers en el mundo no quieren matar gente, pero el historial de Xenotime sugiere que es una de las cosas que les gustaría hacer»,* dijo Sergio Caltagirone, vicepresidente de inteligencia de amenazas de Dragos.

Dragos mencionó en su blog que los atacantes parecen estar investigando vulnerabilidades en los sistemas de energía de los Estados Unidos, un paso menos serio que un ataque real, y hasta ahora no existe evidencia de *«una intrusión conocida y exitosa».*

La investigación realizada por Dragos indica una actividad en *«etapa muy temprana»,* dijo Read de FireEye.

> *«No significa de manera inherente que Rusia vaya a querer cerrar la red la próxima semana o incluso que hayan tomado la decisión de hacerlo cuando estén listos»*, agregó.

El grupo de hackers recibió un aviso luego de un ataque de malware en 2017 en una instalación petroquímica de Arabia Saudita, aseguró Dragos. Los atacantes apuntaron a los sistemas de seguridad para causar *«pérdida de vidas o daños físicos».*

Xenotime es el único grupo que Dragos ha visto apuntar a diferentes sectores industriales. *«El costo y los recursos para moverse entre los sectores son enormes. La investigación de servicios públicos de casi un año del grupo, muestra más que un interés pasajero»,* dijo Caltagirone.