Microsoft anunció hoy la eliminación exitosa de 50 dominios web utilizados anteriormente por un grupo de piratería respaldado por el gobierno de Corea del Norte.

La compañía informó que los 50 dominios fueron utilizados para lanzar ataques cibernéticos por un grupo que la compañía ha estado rastreando como Thallium, también conocido como APT37.

Microsoft dijo que los equipos de la Unidad de Delitos Digitales (DCU) y el Centro de Inteligencia de Amenazas de Microsoft (MSTIC), han estado monitoreando a Thallium durante meses, rastreando las actividades del grupo y mapeando su infraestructura.

El 18 de diciembre, la compañía con sede en Redmond presentó una demanda contra Thallium en un tribunal de Virginia. Poco después de Navidad, las autoridades estadounidenses otorgaron a Microsoft una orden judicial, permitiendo a la compañía tecnológica tomar más de 50 dominios que los hackers norcoreanos estuvieron utilizando como parte de sus ataques.

Los dominios se utilizaron para enviar correos electrónicos de phishing y alojar páginas de phishing. Los hackers de Thallium atraterían a las víctimas en estos sitios, robarían sus credenciales y luego obtendrían acceso a redes internas, desde donde escalarían aún más sus ataques.

Microsoft dijo que además de rastrear las operaciones ofensivas de Thallium, también rastreó hosts infectados.

> *«Con base en la información de las víctimas, los objetivos incluyeron empleados del gobierno, grupos de expertos, miembros del personal universitario, miembros de organizaciones enfocadas en la paz mundial y los derechos humanos, y personas que trabajan en temas de proliferación nuclear»,* dijo Tom Burt, vicepresidente corporativo de atención al cliente en Microsoft.

> *«La mayoría de los objetivos se basaron en Estados Unidos, así como en Japón y Corea del Sur»,* agregó.

El ejecutivo de la compañía también mencionó que en muchos de los ataques, el objetivo final era infectar a las víctimas con malware, como KimJongRAT y BabyShark, dos troyanos de acceso remoto.

> *«Una vez instalado en la computadora de la víctima, este malware extrae información de él, mantiene una presencia persistente y espera más instrucciones»,* dijo Burt.

Esta no es la primera vez que Microsoft usa una orden judicial para obstaculizar las operaciones de grupos de piratería respaldados por el gobierno extranjero.

La compañía utilizó el mismo enfoque 12 veces contra un grupo ruso conocido como Strontium (APT28, Fancy Bear), eliminando con éxito 84 dominios, por última vez en agosto de 2018.

También utilizó una orden judicial para confiscar 99 dominios operados por Phosphorus (APT35), un equipo de ciberespionaje vinculado a Irán.

Además, la compañía utilizó órdenes judiciales para interrumpir las operaciones de Barium, un grupo de piratería respaldado por el gobierno chino, aunque los detalles acerca de esas acciones son poco claras.