El gobierno de Estados Unidos y sus aliados clave, incluyendo la Unión Europea, Reino Unido y la OTAN, atribuyeron firmemente el ataque cibernético masivo contra los servidores de correo electrónico de Microsoft Exchange a los equipos de hackers patrocinados por el estado que trabajan afiliados al Ministerio de Seguridad del Estado (MSS) de la República Popular de China.

En un comunicado emitido por la Casa Blanda el lunes, la administración dijo:

> *«Con un alto grado de confianza en que los ciberactores maliciosos afiliados al MSS de la República Popular China llevaron a cabo operaciones de ciberespionaje utilizando las vulnerabilidades de día cero en Microsoft Exchange Server reveladas a inicios de marzo de 2021».*

También agregaron que el Gobierno del Reino Unido acusó a Beijing de un *«patrón generalizado de piratería informática y sabotaje cibernético sistémico».*

La amplia campaña de espionaje aprovechó cuatro vulnerabilidades no descubiertas antes, en el software Microsoft Exchange y se cree que ha afectado al menos a 30,000 organizaciones en Estados Unidos y cientos de miles más en el resto del mundo. Microsoft identificó al grupo detrás del hackeo como un actor calificado respaldado por el gobierno que opera desde China llamado Hafnium.

Al llamarla *«la intrusión cibernética más importante y extendida contra el Reino Unido y sus aliados», el Centro Nacional de Seguridad Cibernética (NCSC) dijo que era muy probable que el ataque permita «adquirir información de identificación personal y propiedad intelectual».*

Además, el MSS también se destacó como la parte detrás de una serie de actividades cibernéticas maliciosas rastreadas bajo los sobrenombres *«APT40» y «APT31»,* y el Reino Unido atribuyó los grupos para atacar industrias marítimas y contratistas de defensa naval en Estados Unidos y Europa, y también por ejecutar el ataque al parlamento finlandés en 2020.

Además, el lunes, la Oficina Federal de Investigaciones (FB), la Agencia Nacional de Seguridad (NSA), y la Agencia de Ciberseguridad e Infraestructura (CISA), liberaron en conjunto una lista de más de 50 tácticas, técnicas y procedimientos empleados por APT40 y otros actores chinos cibernéticos patrocinados por el estado.

> *«Han pasado unos meses desde que los atacantes explotaron los errores relacionados con Hafnium en Exchange para implementar ransomware, como DearCry y Black Kingdom. En general, para protegerse, los operadores de ransomware suelen operar desde la web oscura o mediante uno o más servidores comprometidos alojados en países distintos de la ubicación física de los atacantes. Esto hace que la atribución de ataques sea difícil, pero no imposible»*, dijo Mark Loma, directos de ingeniería de Sophos.

Estados Unidos acusa a miembros de APT40

En otro desarrollo relacionado, el Departamento de Justicia (DoJ), impuso cargos criminales contra cuatro hackers del MMSS que pertenecen al grupo APT40 relativos a una campaña de varios años de orientación a los gobiernos y entidades extranjeras en el transporte marítimo, la aviación, la defensa, la educación y los sectores de la salud en lo más mínimo una docena de países para facilitar el robo de secretos comerciales, propiedad intelectual e información de alto valor.

De forma separda, el NCSC también anunció que un grupo conocido como APT10, actuó en nombre del MSS para llevar a cabo una campaña cibernética sostenida centrada en proveedores de servicios a gran escala con el objetivo de buscar acceso a secretos comerciales y datos de propiedad intelectual en Europa, Asia y Estados Unidos.

> *«APT10 tiene una relación duradera con el Ministerio de Seguridad del Estado Chino, y opera para cumplir con los requisitos del Estado chino»*, dijo la agencia de inteligencia.

En un comunicado de prensa, la Unión Europea instó a las autoridades chinas a tomar medidas contra las actividades cibernéticas maliciosas llevadas a cabo desde su territorio, afirmando que los ataques al servidor de Microsoft Exchange dieron lugar a riesgos de seguridad y pérdidas económicas significativas para las instituciones gubernamentales y las empresas privadas.

El gobierno chino ha negado repetidamente las afirmaciones de intrusiones patrocinadas por el estado. Un portavoz de la embajada de China en Washington, según Associaten Press, describió a China como *«una víctima grave del robo cibernético, las escuchas y la vigilancia de Estados Unidos», y dijo que «Estados Unidos ha realizado de forma repetida ataques infundados y difamación maliciosa contra China en la seguridad cibernética».*

> *«La República Popular China ha fomentado una empresa de inteligencia que incluye piratas informáticos contratados que también realizan operaciones cibernéticas no autorizadas en todo el mundo, aún para su propio beneficio personal. Hackers con un historial de trabajo para el Ministerio de Seguridad del Estado de la República Popular China (MSS) se han involucrado en ataques de ransomware, extorsión cibernética habilitada, cryptojacking y robo de rango de víctimas en todo el mundo, todo para obtener ganancias financieras»*, dijo la Casa Blanca.