El gobierno de Estados Unidos anunció hoy cargos contra 5 presuntos miembros de un grupo de hackers patrocinado por el estado chino y 2 hackers malasios, responsables de piratear más de 100 empresas en todo el mundo.

Nombrado como APT41 y también conocido como Barium, Winnti, Wicked Panda y Wicked Spider, el grupo de hackers ha estado operando desde al menos 2012 y no solo está involucrado en la recopilación de inteligencia estratégica de objetivos valiosos en muchos sectores, sino también detrás de ataques con motivación financiera contra la industria del juego en línea.

Según un comunicado de prensa publicado por el Departamento de Justicia de Estados Unidos, dos de los cinco piratas informáticos chinos, Zhang Haoran y Tan Dailin, fueron acusados en agosto de 2019, y los otros tres: Jiang Lizhi, Qian Chuan, Fu Qiang, y dos co-conspiradores de Malasia, estaban en acusaciones separadas en agosto de 2020.

Los tres hackers chinos acusados posteriormente están asociados con una empresa de seguridad de red Chengdu 404 Network Technology, operada como fachada por el People´s Republic of China.

> *«FU ha estado trabajando estrechamente con JIANG desde al menos 2008, y trabajó con JIANG en varias empresas relacionadas con Internet y videojuegos. FU ha estado trabajando con QIAN y JIANG juntos desde al menos 2013. Antes de unirse a CHENGDU 404, FU se describió a sí mismo como un programador y desarrollador calificado»,* dicen los documentos judiciales.

Como se descubrió en varios informes anteriores, el grupo APT41 se especializa en ataques a la cadena de suministro de software, donde los hackers roban *«código fuente, certificados de firma de código de software, datos de cuentas de clientes e información comercial valiosa»*, y distribuyen versiones maliciosas firmadas digitalmente del software para infectar sistemas en organizaciones específicas.

Según los documentos judiciales, en algunos casos en los que los sistemas objetivo no tenían ninguna información valiosa, los acusados también utilizaron ransomware y malware de criptojacking para monetizar sus esfuerzos.

> Las industrias objetivo incluyen *«empresas de desarrollo de software, fabricantes de hardware informático, proveedores de telecomunicaciones, empresas de redes sociales, empresas de videojuegos, organizaciones sin fines de lucro, universidades, grupos de expertos y gobiernos extranjeros, así como políticos y activistas en favor de la democracia en Hong Kong»*.
>
> *«Los acusados también comprometieron las redes informáticas de gobiernos extranjeros en India y Vietnam, y atacaron, pero no comprometieron, las redes informáticas gubernamentales en el Reino Unido»*, dice el comunicado de prensa.

Los 2 hackers malasios, Wong Ong Hua y Ling Yang Ching, fueron arrestados por las autoridades malasias en Sitiawan el 14 de septiembre de 2020 y están siendo extraditados a Estados Unidos. El FBI confirmó que los 5 ciudadanos chinos siguen prófugos.

> *«Además de las órdenes de arresto para todos los acusados, en septiembre de 2020, el Tribunal de Distrito de Estados Unidos para el Distrito de Columbia, emitió órdenes de incautación que resultaron en la incautación reciente de cientos de cuentas, servidores, nombres de dominio de control y comando (C2) de las páginas web «dead drop» utilizadas por los acusados para llevar a cabo sus delitos de intrusión informática»*, dijo el Departamento de Justicia.
>
> *«Las acciones de Microsoft [además de Google, Facebook y Verizon Media] fueron una parte importante del esfuerzo general para negar a los acusados el acceso continuo a la infraestructura de piratería, herramientas, cuentas y nombres de*

> *dominio de comando y control».*

Las empresas objetivo estaban ubicadas en Estados Unidos y en todo el mundo, incluso en Australia, Brasil, Chile, Hong Kong, India, Indonesia, Japón, Malasia, Pakistán, Singapur, Corea del Sur, Taiwán, Tailandia y Vietnam.

Zhang y Tan han sido acusados de 25 cargos de fraude informático y lavado de dinero, que conllevan una sentencia máxima de 20 años de prisión.

Jiang, Qian y Fu también enfrentan cargos similares con nueve cargos que conllevan una sentencia máxima de 20 años de prisión.

La acusación contra Wong y Ling los acusa de 23 cargos similares, pero debido a que también están involucrados en el registro falso de nombres de dominio, aumentaría la pena máxima de prisión por lavado de dinero a 27 años.