



ESTARÍAN VINCULADOS AL GOBIERNO DE XI

Hackers chinos roban 20 mdd a EU; eran para atender Covid

El grupo APT41 además hace espionaje y recopila datos sobre activistas en Hong Kong, asegura el Servicio Secreto

Expertos temen que sea sólo el inicio de un esquema de estafas más grande

WASHINGTON, DC
AGENCIAS

Hackers con vínculos al régimen chino robaron al menos 20 millones de dólares en Estados Unidos al conseguir fraudulentamente fondos

de la asistencia económica para la pandemia del Covid-19, revelaron fuentes del Servicio Secreto.

Se trata de un grupo de piratas informáticos conocido como APT41, con sede en Chengdu, y se teme que sea sólo el inicio de un esquema de estafas más grande, según indicaron fuentes policiales y expertos en ciberseguridad a la cadena NBC.

Aunque se han detectado múltiples y millonarios préstamos fraudulentos durante la pandemia y

solicitudes irregulares al seguro de desempleo en todo el país, es la primera vez que desde el gobierno estadounidense se reconoce el fraude de ciberdelincuentes vinculados a un Estado extranjero.

Cuando el gobierno federal y las autoridades estatales ofrecieron los programas de apoyo económico, APT41, con más de una década de actividad, puso manos a la obra. Según el Servicio Secreto, se trata de un "grupo de ciberamenazas patrocinado por el Estado chino y muy hábil para llevar a cabo misiones de espionaje y delitos financieros en beneficio propio".

Como los gobiernos estatales no tienen los niveles de protección más sofisticados, sus infraestructuras

FOCOS

El caso. En 2020, el Departamento de Justicia de EU denunció a APT41 por otro hackeo a más de 100 compañías e instituciones y en el extranjero, incluidas empresas de

informáticas quedan más vulnerables a amenazas extranjeras.

Según publicó NBC, el esquema de fraude de APT41 comenzó a mediados de 2020 y abarcó 2 mil cuentas asociadas con más de 40 mil transacciones financieras.

Hasta ahora, el Servicio Secreto ha podido recuperar la mitad de los 20 millones de dólares robados, mientras todavía continúan las investigaciones en más de mil casos abiertos a criminales nacionales y transnacionales.

Los expertos consultados por la cadena estadounidense dudan si la intrusión de APT41 fue impulsada por el régimen chino o si Pekín simplemente hizo la vista gorda.

No hay certezas de los vínculos con el gobierno de Xi Jinping, pero sí múltiples indicios. APT41 recopiló, por ejemplo, información sobre activistas prodemocracia en Hong Kong y sobre un monje budista en el Tíbet, dos territorios chinos donde Pekín se enfrenta a cierta inestabilidad política. Aunque muchas de las actividades del grupo parecen estar motivadas sólo por intereses financieros. Uno de los hackers habría presumido de chantajear a víctimas

desarrollo de software y proveedores de telecomunicaciones.

Malos manejos. Las estafas en los programas de ayuda están siendo investigadas en el Congreso de EU. Un análisis mostró que 42.4% de las prestaciones por la pandemia se pagó indebidamente.

"Nunca antes les había visto apuntar al dinero del gobierno. Eso sería una escalada"

JOHN HULTQUIST
Jefe de Análisis de Inteligencia de Mandiant



ricas durante una conversación en línea.

"Nunca antes les había visto apuntar al dinero del gobierno. Eso sería una escalada", dijo a NBC John Hultquist, jefe de Análisis de Inteligencia de la firma de ciberseguridad Mandiant. "Sería una locura pensar que este grupo no tenía como objetivo los 50 estados", dijo a su vez Roy Dotson, coordinador nacional de recuperación del fraude pandémico del Servicio Secreto.