EE.UU. acusa a China de montar una red de extorsión en internet

- Por primera vez, la Casa Blanca atribuye varios ciberataques, incluido el de Microsoft, al régimen comunista
- La OTAN y la UE se suman a Biden en su condena, y advierten a Pekín en contra de amparar a 'hackers'

DAVID ALANDETE
CORRESPONSAL EN WASHINGTON

La Casa Blanca ha acusado directamente a China de un gigantesco ciberataque al servidor de correo electrónico Exchange de Microsoft que afectó este mismo año a decenas de miles de dispositivos, además de una larga lista de amenazas digitales y extorsiones que le atribuye al régimen comunista, incluidos varios ataques de tipo 'ransomware' de 'hackers' en la órbita del Gobierno chino, que supusieron el robo de millones de dólares.

Según reveló el lunes la Casa Blanca, EE.UU. está convencido y dice tener pruebas de que el ministerio chino de Seguridad Estatal recluta a piratas informáticos que participan en entramados mundiales de extorsión y robo. La palabra 'ransomware' (de 'ransom', que en inglés es 'rescate') se refiere a un programa informático difundido por internet que toma el control del sistema o dispositivo que infecta y pide un rescate para devolverle el control a su dueño.

Según dijo el domingo en una llamada con periodistas un funcionario de la Casa Blanca, el hecho de que el régimen comunista de China entre en este tipo de chantajes alarmó a EE.UU. «Esto nos sorprendió. Y de hecho, una de las razones por las que hemos trabajado tanto en esta atribución pública es porque realmente nos brindó nuevos conocimientos sobre el trabajo del ministerio chino de Seguridad Estatal y sobre el tipo de comportamiento agresivo que estamos viendo por parte de China».

El Gobierno estadounidense está a la vez tratando de contener los ataques de 'ransomware' de grupos de delincuentes radicados en Rusia, que han llegado a interrumpir el suministro de gasolina y de carne en partes de EE.UU. hace apenas unas semanas. Ese fue un punto que Joe Biden trató con su homólogo ruso, Vladímir Putin, en la cumbre que ambos mantuvieron en Suiza el mes pasado, y donde marcó unas líneas rojas.

Sin sanciones

De momento esta acusación, que se formula en conjunto con la Unión Europea y la OTAN, no viene acompañada de sanciones al régimen chino, pero ese funcionario de EE.UU. dijo que primero Washington prefiere llamar la atención de la ciudadanía mundial sobre este problema, y lanzar una advertencia a Pekín.

«Lo más importante ahora mismo es denunciar públicamente este patrón de actividad cibernética maliciosa e irresponsable y hacerlo junto con aliados y socios», dijo ese funcionario. «Esta era la primera atribución pública de la OTAN a China de este tipo de actividad cibernética maliciosa. Creemos que estamos en una primera etapa importante de llamar la atención y desvelar la autoría, y enfocarnos con nuestros socios en nuestros esfuerzos colectivos de seguridad y de promover la defensa de la red y otras acciones necesarias para interrumpir estas amenazas».

La Unión Europea ha acusado paralelamente al régimen comunista de China de lo que ha descrito como «actividades maliciosas» con «efectos significativos». El ataque «se hizo desde el territorio de China con el objetivo de espionaje y robo de propiedad intelectual», según dijo en un comunicado el jefe de Exteriores de la UE, Josep Borrell, en un comunicado emitido el lunes.

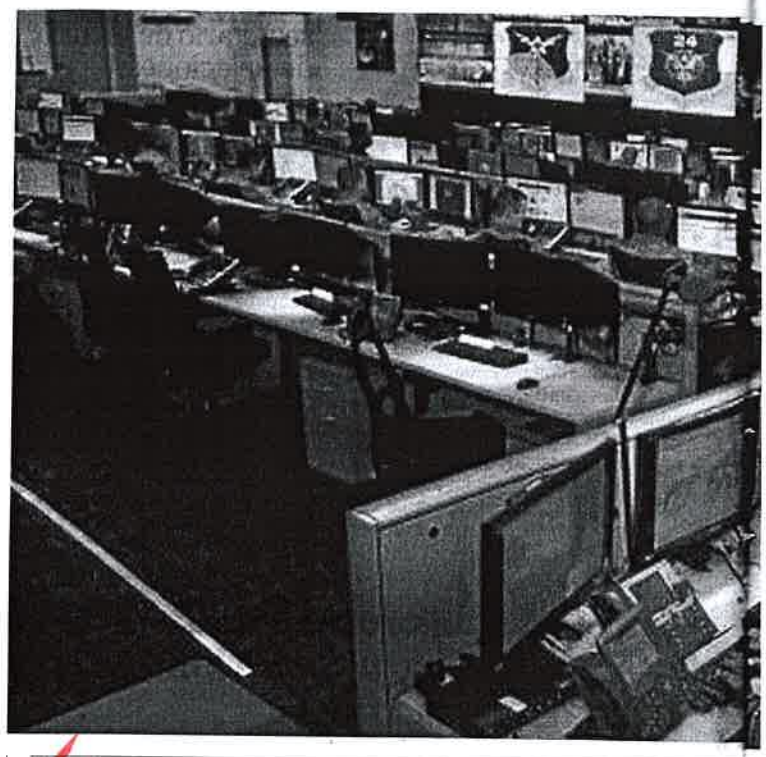
El ataque a Microsoft Exchange, que afectó a miles empresas y personas en todo el mundo, se identificó ya en enero y fue rápidamente atribuido a hackers chinos. Pero no es el único que EE.UU. le atribuye a China. Existe, según la Casa Blanca, un gran entramado de espionaje y extorsión digital que supervisa Pekín.

Ya el viernes, en otro caso distinto pero relacionado, un juzgado federal en San Diego, en el estado de California, le imputó a Ding Xiaoyang, Cheng Qingmin, Zhu Yunmin y Wu Shurong, funcionarios del ministerio de Seguridad de China, dos delitos relacionados con ataques cibernéticos. Según la acusación, revelada por medios estadounidenses, esos funcionarios trataron de ocultar el papel del régimen chino en el robo de información al crear una empresa fantasma, Hianan Xiandun Technology Development Co., Ltd., radicada en la provincia Hainan.

La Fiscalía imputa a cuatro funcionarios chinos delitos de ciberespionaje por participar en robo de información en la red

La fiscalía estadounidense acusa a Ding, Cheng y Zhu de «coordinar, facilitar y emitir órdenes a los hackers y traductores que operaban en la empresa fantasma». A Wu le imputa haber creado el virus e infiltrarlo en sistemas informáticos de empresas, instituciones educativas y gobiernos extranjeros en EE.UU., Austria, Canadá, Alemania, Noruega, Arabia Saudí, Suiza y Reino Unido, entre muchos otros.

Según esa otra causa judicializada, el régimen comunista de China se infiltró maliciosamente en los servidores de esas entidades y personas para difundir por todo el mundo virus cibernéticos de espionaje y chantaje.



Unidad de comando cibernético de EE.UU., en Texas // ABC

AVISO A EE.UU. Y LOS 'SECESIONISTAS' DE LA ISLA

Simulacro de desembarco de militares chinos cerca de Taiwán

ABC MADRID

El Ejército y la Marina chinos realizaron el pasado viernes unos ejercicios anfibios conjuntos en una provincia próxima a Taiwán en los que simularon un desembarco militar. Las maniobras tuvieron lugar al día siguiente de que aterrizara en la isla el segundo avión militar de Estados Unidos en menos de dos meses.

El periódico 'Global Times', vinculado al Partido Comunista Chino, informó el pasado domingo de los ejercicios en aguas frente a la provincia oriental de Fujian, que deberían verse como un aviso y un gesto disuasorio por EE.UU. y los «secesionistas de Taiwán», según habría indicado a la citada publicación un experto militar sin identificar. Así mismo, aseguró que probablemente se realizarán maniobras milita-

Parte de la investigación la han conducido el FBI, que es la policía judicial, la Agencia de Seguridad Nacional y la Agencia de Seguridad de Infraestructura y Ciberseguridad.

Cooperación trasatlántica

Para la Administración Biden es crucial la cooperación con los socios europeos en la contención de los ciberataques. Sobre todo dados los desafíos que plantea Rusia en ese apartado. A pesar de que Biden le exigió a Putin que pusiera coto a esas operaciones de chantaje digital, se ha dado otra a gran escala después, que ha afectado a una compañía de software radicada en Miami y que há afectado a miles de usuarios en todo el mundo.

Según dijo el domingo el funcionario de la Casa Blanca en la llamada con reporteros, «ninguna acción en solitario puede cambiar el comportamiento de China en el ciberespacio y tampoco un solo país puede actuar por sí solo. Nuestros aliados y socios son una tremenda fuente de fortaleza y una ventaja única para EE.UU., y nuestro enfoque para el intercambio de información sobre amenazas cibernéticas y defensa va a ser colectivo».

Es significativo que EE.UU. incluya a la OTAN en estas deliberaciones, señal de que la Alianza comienza a incorporar la defensa en el ciberespacio en sus prioridades, tras los ataques que interrumpieron el suministro de gasolina y de carne en grandes partes de EE.UU. Aun así, no ha habido de momento operaciones conjuntas de respuesta a estos ciberataques.

Según dijo ayer la agencia Ap, un portavoz del ministerio chino de Exteriores al que se preguntó en el pasado por el ataque a Microsoft Exchange dijo que China «se opone con firmeza y combate los ciberataques y el robo cibernético en todas sus formas» y advirtió que la atribución de ciberataques debía basarse en pruebas y no en «acusaciones sin ningún fundamento».

res más complejas en el futuro. «Como tropas de primer nivel con base en la costa sureste, debemos entrenar duro en escenarios como los de las batallas reales, estar preparados para el combate en todo momento y salvaguardar resueltamente la soberanía nacional y la integridad territorial», ha dicho el general Zhu Chaojun a los medios chinos y recoge Ep.

Estas maniobras militares en las cercanías de la isla reclamada por Pekín se producen precisamente después de que el Ministerio de Defensa chino advirtiera el pasado jueves de que la entrada de aviones extranjeros en el espacio aéreo del país sin su autorización llevaría a «graves consecuencias».

Un avión del Ejército norteamericano aterrizó en Taiwán el pasado jueves, justo el día en que el director del Instituto Americano de Taiwán, que actúa como Embajada 'de facto' de EE.UU., Brent Christensent, terminase su mandato para ser relevado por la diplomática Sandra Oudkirk, informa 'The South China Morning Post'.

Estados Unidos es el principal aliado de Taiwán y principal proveedor de armas de la isla. Sin embargo, el coordinador para la región del Indo-Pacífico de la Casa Blanca, Kurt Campbell, señaló a principios de este mes que aunque Washington apoya su relación con Taipéi, no apoya la independencia formal de Taiwán.

El 'software' israelí Pegasus se utilizó contra periodistas de todo el mundo

▸ 'The Washington Post' dice que se usó con familiares de Jamal Khashoggi

S. I.
WASHINGTON

Un programa digital de una empresa israelí se utilizó contra periodistas, funcionarios gubernamentales y activistas a favor de los derechos humanos de todo el mundo, según una investigación de 17 medios que fue publicada el domingo. Uno de esos medios, 'The Washington Post' reveló que el 'software' espía Pegasus creado por la empresa NSO Group, con sede en Israel, se usó para infiltrar los teléfonos de la exmujer y la pareja actual de Jamal Khashoggi, el columnista del 'Post' asesinado en un consulado saudí en Turquía en 2018.

La investigación de esos medios no reveló quién está tras esos ciberataques ni por qué los acometió. Los números de teléfono que supuestamente fueron objeto de ese espionaje estaban en una lista proporcionada por Forbidden Stories y Amnistía Internacional a los 17 medios de comunicación. Los medios identificaron a más de mil personas en más de 50 países, dijo el 'Post'.

Entre ellos hay, según esas pesquisas, varios miembros de la familia real árabe, al menos 65 ejecutivos de empresas globales, 85 activistas de derechos humanos, 189 periodistas y más de 600 políticos y funcionarios gubernamentales, incluidos varios jefes de estado y primeros ministros. No hay nombre de ello de momento.

'The Guardian' dijo que en los datos figuraban las cifras de más de 180 periodistas, incluidos reporteros, editores y ejecutivos de 'Financial Times', CNN, 'The New York Times', 'The Economist', Associated Press y Reuters. Los ejecutivos de esas compañías han protestado por estas supuestas intromisiones en el derecho a la libertad de prensa.

Más regulación

En un comunicado, el grupo de derechos humanos Amnistía Internacional condenó lo que denominó «la falta total de regulación» del sector del software de vigilancia digital. «Hasta que esa empresa (NSO) y la industria en su conjunto puedan demostrar que son capaces de respetar los derechos humanos, debe haber una moratoria inmediata sobre la exportación, venta, transferencia y uso de tecnología de vigilancia», dice el comunicado.

La compañía israelí emitió después un comunicado en su sitio web negando los informes de los 17 medios liderados que operan en el consorcio periodístico Forbidden Stories. «El informe de Forbidden Stories está lleno de suposiciones erróneas y teorías no corroboradas que plantean serias dudas sobre la fiabilidad y los intereses de las fuentes», dijo la empresa que creó ese programa digital de espionaje. NSO dijo que su tecnología no estaba asociada de ninguna manera con el asesinato de Khashoggi.

Una israelí usa su móvil ante la sede de la empresa que gabricó Pegasus // AFP