

Ataques cibernéticos: Londres acusa a China de hackear los datos de 40 millones de británicos y la califican de "amenaza a la seguridad nacional"

26/03/2024

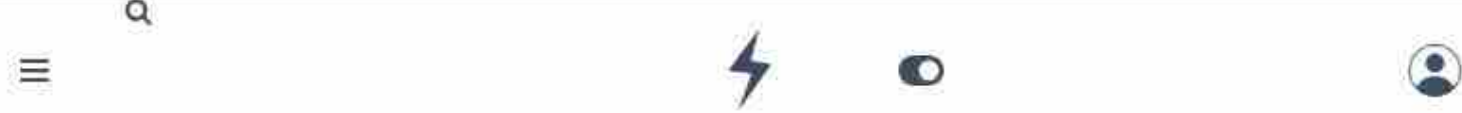
Argentina - Flipr (Online) [Online]

Tier:N/D Circulación: 2551 Audiencia 2551

P. -- 0 cm² 11524 cc N/D N/D Sin autor

Ref.: 516455710

The advertisement features the Codere logo on the left, with the text "Casa de Apuestas Oficial" and the River Plate crest. The central text reads "DUPLICAMOS EL 100% DE TU 1ER DEPÓSITO HASTA \$5.000" with a "REGISTRATE >" button. The background shows three River Plate players celebrating. The bottom right corner includes logos for "Codere" and "Gub. de Tucumán".



VOLVER

GUARDAR

Ataques cibernéticos: Londres acusa a China de hackear los datos de 40 millones de británicos y la califican de "amenaza a la seguridad nacional"

CLARÍN » ÚLTIMO MOMENTO » 26/03 | 20:09

China **accedió maliciosamente a 40 millones de británicos** en sus ataques cibernéticos. Gran Bretaña y Estados Unidos han acusado a Beijing de lanzar una "prolífica" campaña global de ciberataques, dirigidos a la información personal de **políticos, periodistas, académicos y millones de votantes**.

Las dos personas sancionadas por el Reino Unido son **Zhao Guangzong**, de 38 años, y **Ni Gaobin**, de 38. Se dice que ambos son miembros del grupo de hackers **APT31**, así como de **Wuhan Xiaoruizhi** de Science and Technology Company Ltd, que según el gobierno era una organización fachada para APT31.

Los ministros también están preparados para declarar formalmente a China "**una amenaza a la seguridad nacional de Gran Bretaña**", tras las revelaciones de la escala de su ciberataque al Reino Unido, indicó un alto funcionario.

Los parlamentarios conservadores británicos dijeron que las acciones del gobierno no fueron lo suficientemente lejos, dada la magnitud de la amenaza.

Sir Iain Duncan Smith, ex oficial de inteligencia del ejército, un ex líder conservador que ha sido sancionado por Beijing y atacado por piratas informáticos, comparó la posición del gobierno con "un elefante que da a luz a un ratón".

El ataque a la Comisión Electoral dio a los piratas informáticos chinos **acceso a los nombres y direcciones de más de 40 millones de personas** en el censo electoral, que estaban registradas para votar entre 2014 y 2022. Los piratas informáticos también obtuvieron **correos electrónicos del sistema**.

Los funcionarios creen que los datos podrían asignarse a otros conjuntos de datos para ayudar a identificar a individuos, especialmente a **grupos disidentes en el Reino Unido**. La recopilación masiva de datos es una táctica bien conocida de Beijing y la inteligencia artificial ha permitido al Estado hacer un mejor uso de ella.

Operación conjunta

En una operación conjunta sin precedentes **para exponer el espionaje chino**, Londres y Washington revelaron detalles de una campaña de una década de duración por parte de Beijing para "reprimir a los

Ataques cibernéticos: Londres acusa a China de hackear los datos de 40 millones de británicos y la califican de "amenaza a la seguridad nacional"

26/03/2024

Argentina - Flipr (Online) [Online]

Tier:N/D Circulación: 2551 Audiencia 2551

0 cm² 11524 cc N/D N/D Sin autor

Ref: 516455710

revelación de detalles de una campaña de una red de duración por parte de Beijing para "reprimir a los críticos, comprometer las instituciones gubernamentales y robar secretos comerciales".





Londres apunta a miembros del grupo de hackers APT31. Foto: AFP

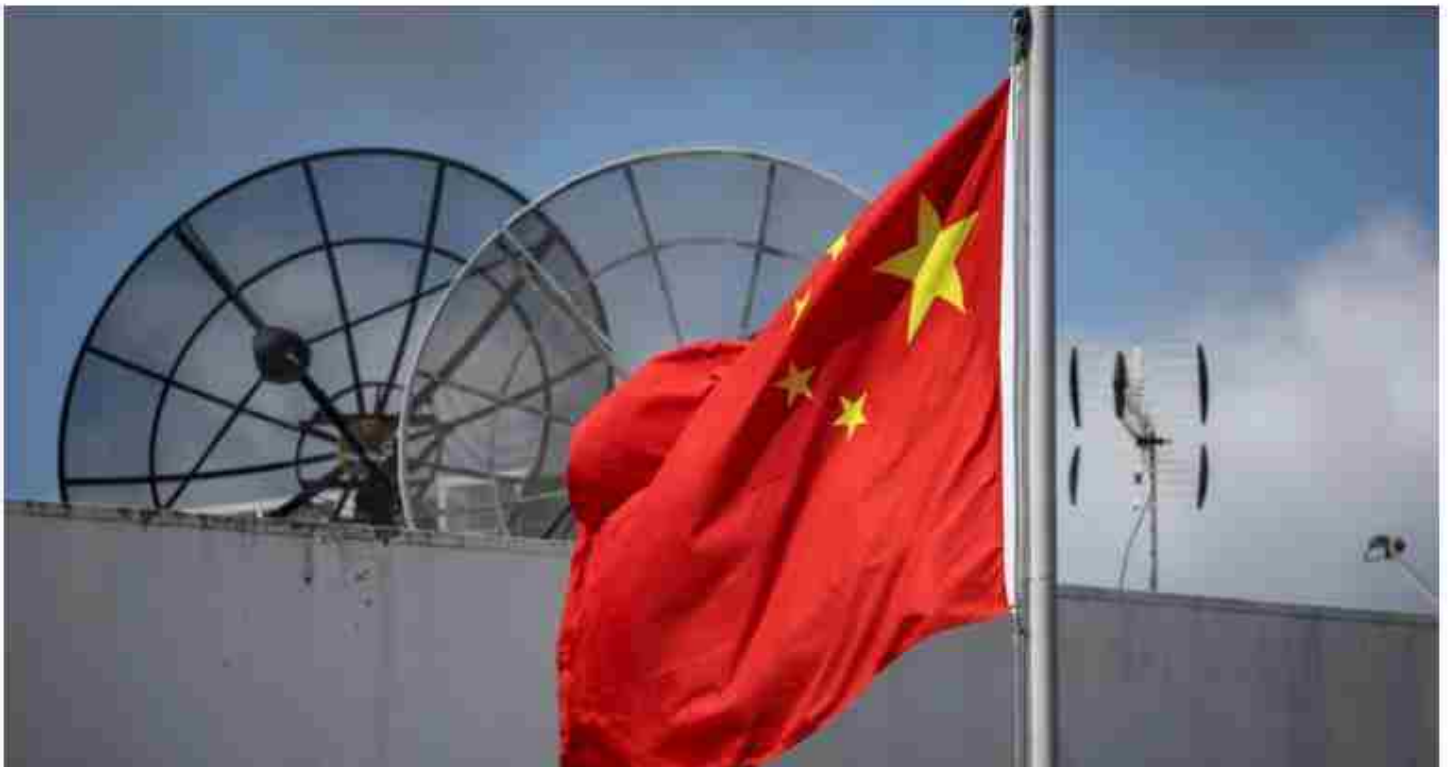
Nueva Zelanda reveló el martes que agentes chinos **también habían pirateado su parlamento** y condenó a China por "su ciberactividad maliciosa".

En el Reino Unido, los ministros dijeron que China había logrado acceder a un "tesoro escondido" de información personal, en un ciberataque al organismo de control electoral de Gran Bretaña y había intentado espiar a parlamentarios críticos con Beijing. Esos ataques se intensifican a medida que se acercan las elecciones generales británicas este año.

El Reino Unido sancionó a dos funcionarios chinos y a una organización en respuesta a los ataques. Estados Unidos **acusó a siete personas** por ataques que, según dijeron, habían ocurrido desde, al menos, el 2010.

China se defiende

El Ministerio de Asuntos Exteriores chino afirmó que Gran Bretaña había proporcionado pruebas insuficientes de los ataques. Calificó las acusaciones de **"poco profesionales"**. Acusó a Estados Unidos de trabajar para "exaltar los llamados ciberataques chinos" y anunció que había "realizado fuertes gestiones con Estados Unidos y las partes relevantes".





El Ministerio de Asuntos Exteriores chino afirmó que Gran Bretaña había proporcionado pruebas insuficientes de los ataques. Foto: AP

Gran Bretaña convocó al embajador de China al Foreign Office para protestar.

En Estados Unidos

Las autoridades estadounidenses revelaron que un pequeño grupo de piratas informáticos chinos, conocido como *Advanced Persistent Threat 31* (APT31), había comprometido los correos electrónicos, el almacenamiento en la nube y los registros de llamadas telefónicas de **millones de estadounidenses**. Los piratas informáticos enviaron 10.000 correos electrónicos "maliciosos" a sus objetivos **para comprometer sus sistemas**.

Los parlamentarios piden una **"nueva era de relaciones con China"** en medio de informes de ciberataques.

Estados Unidos advirtió que esta información podría divulgarse en apoyo de una "influencia maligna", dirigida a procesos e instituciones democráticas, planes económicos, propiedad intelectual y secretos comerciales pertenecientes a empresas estadounidenses.

En Nueva Zelanda

Agentes chinos, respaldados por el Estado, también atacaron la oficina de asesoría parlamentaria y el servicio parlamentario de Nueva Zelanda en 2021, dijo Judith Collins, ministra de seguridad de Nueva Zelanda.

Una evaluación encontró que los actores patrocinados por el estado chino, conocidos como Amenaza Persistente Avanzada 40 (APT 40), eran los responsables. **Están vinculados con el Ministerio de Seguridad del Estado de China**, según la Oficina de Seguridad de las Comunicaciones del Gobierno de Nueva Zelanda (GCSB).

La GCSB dijo el martes que, si bien los datos habían sido eliminados de los sistemas informáticos del parlamento de Nueva Zelanda, no eran de naturaleza "estratégica".





El director general de la Oficina de Seguridad gubernamental de Nueva Zelanda apunta a China. Foto: AP

"El uso de operaciones de espionaje cibernéticas para interferir con las instituciones y procesos democráticos en cualquier lugar **es inaceptable**", afirmó Collins.

Al igual que el Reino Unido y los Estados Unidos, Nueva Zelanda también es miembro de **la red de inteligencia occidental Five Eyes**, que incluye a Canadá y Australia.

Los ministros también están preparados para declarar formalmente a China una amenaza a la seguridad nacional de Gran Bretaña tras las revelaciones de la escala de su ciberataque al Reino Unido, indicó el viceprimer ministro.

En la Cámara de los Comunes, Oliver Dowden, viceprimer ministro, insistió en que los procesos políticos y las instituciones del Reino Unido no habían resultado perjudicados.

"No afectará la forma en que las personas se registran, votan o participan de otro modo en los procesos democráticos", dijo. "Quiero asegurarle a la gente que la puesta en peligro de esta información, si bien es obviamente preocupante, normalmente no crea un riesgo para los afectados", dijo.

China desmiente

China negó las acusaciones. La embajada china dijo: "Los llamados ciberataques de China contra el Reino Unido son calumnias completamente inventadas y maliciosas. Nos oponemos firmemente a tales acusaciones. China siempre ha luchado firmemente contra todas las formas ciberataques".

"China no fomenta, apoya ni tolera los ciberataques" dijo.

Robert Jenrick, ex ministro de Inmigración británico, describió la respuesta como **irrisoria** y acusó al gobierno de "dejar que China salga libre de costos". "Esta débil respuesta sólo envalentonará a China para continuar su agresión hacia el Reino Unido. Está muy claro que China debería ser clasificada como **un Estado hostil**", dijo.

Merrick Garland, fiscal general de Estados Unidos, dijo que la investigación mostraba "los fines a los que el gobierno chino está dispuesto a llegar para atacar e intimidar a sus críticos" y amenazar la "seguridad nacional de Estados Unidos y nuestros aliados".

Lisa Monaco, su adjunta, añadió: "El Departamento de Justicia perseguirá, expondrá y responsabilizará implacablemente a los ciberdelincuentes que socavarían las democracias y amenazarían nuestra seguridad nacional".

El año pasado, The Times reveló que un espía chino **estaba utilizando perfiles de LinkedIn** para atraer a funcionarios británicos para que entregaran secretos de estado a cambio de dinero.

Durante cinco años, el agente, cuyo alias principal es Robin Zhang, creó una serie de alias y empresas falsas, para atacar a funcionarios de seguridad, funcionarios públicos, científicos y académicos, con acceso a información clasificada o tecnología comercialmente sensible.

China, quinto socio comercial británico

China es el quinto socio comercial de Gran Bretaña. Si bien las importaciones totales desde China disminuyeron el año pasado, **las exportaciones británicas crecieron casi un 12 por ciento**.

Las cifras del gobierno muestran que el comercio de bienes y servicios en los 12 meses hasta finales de septiembre ascendió a 100,9 mil millones de libras esterlinas. De esto, las exportaciones a China representaron 37,5 mil millones de libras (un aumento del 11,9% respecto a los 12 meses anteriores) y las importaciones representaron 63,5 mil millones de libras (un descenso del 12,6%).

La consultora Grant Thornton descubrió este mes que 970 empresas de propiedad china emplean a más de 59.000 personas en el Reino Unido. En el 2023 contribuyeron con 116.400 millones de libras esterlinas de ingresos totales a la economía.

El dominical El Sunday Times informó que EVE Energy, el fabricante chino de baterías cilíndricas para automóviles tipo Tesla, estaba a punto de invertir **miles de millones en la construcción de la gigafábrica más grande de Gran Bretaña**. Se entiende que se encuentran en negociaciones avanzadas para construir una fábrica de 60 gigavatios-hora en las afueras de Coventry. La empresa se comprometerá inicialmente a invertir al menos 1.200 millones de libras esterlinas en una gigafábrica de 20 GWh, según fuentes cercanas a las negociaciones.

Algunas de las mayores inversiones de China **se han producido en el sector energético**, específicamente en

la energía nuclear.

China General Nuclear (CGN), propiedad del Estado chino, compró una participación del 33,5 por ciento en la central eléctrica Hinkley Point C en Somerset, la primera nueva instalación nuclear construida en el Reino Unido en más de 20 años.

CGN, que ha sido incluida en la lista negra de Estados Unidos por supuestamente ayudar a adquirir tecnología estadounidense para uso militar en China, finalmente se vio obligada a abandonar el proyecto utilizando el dinero de los contribuyentes. Pero el comité de inteligencia y seguridad advirtió el año pasado que tenía serias dudas sobre proyectos futuros.

El Estado chino también ha acumulado participaciones en empresas británicas de petróleo y gas y en los sectores de tecnología y educación.

Consejos para contraseñas

Las personas con acceso a información confidencial han recibido **nuevos consejos para proteger sus contraseñas** y dispositivos de los espías chinos.

La nueva guía, publicada por el Centro Nacional de Seguridad Cibernética (NCSC), acepta que "puede ser difícil recordar las contraseñas, por lo que está bien escribirlas". Pero insta a las personas a "mantenerlas seguras, donde otras personas no puedan acceder a ellas".

"Sepárelo de sus dispositivos", sugieren.

Recomienda utilizar **un administrador de contraseñas en línea**, que ofrecerá una forma segura de almacenar contraseñas, ya sea en un navegador de Internet o en una aplicación, que utilice una contraseña maestra o datos biométricos.

El NCSC dice que cuando los atacantes comprometen una cuenta, a menudo roban o adivinan la contraseña, en lugar de utilizar un método más sofisticado. Las contraseñas débiles a menudo contenían nombres, lugares o una serie de números. El consejo añade: "El NCSC recomienda utilizar una secuencia de tres palabras aleatorias para hacer una contraseña compleja pero fácil de recordar".

El consejo está dirigido a personas de "alto riesgo", incluidos políticos, su personal, activistas, académicos, periodistas y abogados, que tienen acceso o influencia sobre información sensible que "podría ser de interés para los actores estatales nacionales".

Aconseja a las personas que siempre **instalen actualizaciones para aplicaciones y dispositivos** y que reemplacen teléfonos y computadoras portátiles antiguas cuando los fabricantes dejen de publicar actualizaciones de seguridad.

Fuente: https://www.clarin.com/mundo/ataques-ciberneticos-londres-acusa-china-hackear-datos-40-millones-britanicos-califican-amenaza-seguridad-nacional_0_5QOCbYsQ34.html

Etiquetas:

INTELIGENCIA ARTIFICIAL

CONDICIONES DE USO



Todas las voces

Flipr monitorea y distribuye noticias de medios nacionales, provinciales y locales segmentadas por palabras, categorías y ubicación.



Para profesionales y lectores

Ofrece herramientas que facilitan el seguimiento y análisis de temáticas, instituciones y protagonistas de la agenda pública de cada lugar.

Act
pri



[...] erlinas . De esto, las exportaciones a China representaron 37,5 mil millones de libras (un aumento del 11,9% respecto a los 12 meses anteriores) y las importaciones representaron 63,5 mil millones de libras (un descenso del 12,6%). La consultora Grant Thornton descubrió este mes que 970 empresas de propiedad china emplean a más de 59.000 personas en el Reino Unido. En el 2023 contribuyeron con 116.400 millones de libras esterlinas de ingresos totales a la economía. El dominical El Sunday [...]

China accedió maliciosamente a 40 millones de británicos en sus . Gran Bretaña y Estados Unidos han acusado a Beijing de lanzar una "prolífica" campaña global de ciberataques, dirigidos a la información personal de políticos, periodistas, académicos y millones de votantes. Las dos personas sancionadas por el Reino Unido son Zhao Guangzong , de 38 años, y Ni Gaobin , de 38. Se dice que ambos son miembros del grupo de hackers APT31 , así como de Wuhan Xiaoruizhi de Science and Technology Company Ltd, que según el gobierno era una organización fachada para

Los ministros también están preparados para declarar formalmente a China "una amenaza a la seguridad nacional de Gran Bretaña" , tras las revelaciones de la escala de su ciberataque al Reino Unido, indicó un alto funcionario.

Los parlamentarios conservadores británicos dijeron que las acciones del gobierno no fueron lo suficientemente lejos, dada la magnitud de la amenaza.

Sir Iain Duncan Smith, ex oficial de inteligencia del ejército, un exlíder conservador que ha sido sancionado por Beijing y atacado por piratas informáticos, comparó la posición del gobierno con "un elefante que da a luz a un ratón".

El ataque a la Comisión Electoral dio a los piratas informáticos chinos acceso a los nombres y direcciones de más de 40 millones de personas en el censo electoral, que estaban registradas para votar entre 2014 y 2022. Los piratas informáticos también obtuvieron correos electrónicos del sistema.

Los funcionarios creen que los datos podrían asignarse a otros conjuntos de datos para ayudar a identificar a individuos, especialmente a grupos disidentes en el Reino Unido . La recopilación masiva de datos es una táctica bien conocida de Beijing y la inteligencia artificial ha permitido al Estado hacer un mejor uso de ella.

Operación conjunta

En una operación conjunta sin precedentes para exponer el espionaje chino , Londres y Washington revelaron detalles de una campaña de una década de duración por parte de Beijing para "reprimir a los críticos, comprometer las instituciones gubernamentales y robar secretos comerciales".

Nueva Zelanda reveló el martes que agentes chinos también habían pirateado su parlamento y condenó a China por "su ciberactividad maliciosa".

En el Reino Unido, los ministros dijeron que China había logrado acceder a un "tesoro escondido" de información personal, en un ciberataque al organismo de control electoral de Gran Bretaña y había intentado espiar a parlamentarios críticos con Beijing. Esos ataques se intensifican a medida que se acercan las elecciones generales británicas este año.

El Reino Unido sancionó a dos funcionarios chinos y a una organización en respuesta a los ataques. Estados Unidos acusó a siete personas por ataques que, según dijeron, habían ocurrido desde, al menos, el 2010.

China se defiende

El Ministerio de Asuntos Exteriores chino afirmó que Gran Bretaña había proporcionado pruebas insuficientes de los ataques. Calificó las acusaciones de "poco profesionales" . Acusó a Estados Unidos de trabajar para "exaltar los llamados ciberataques chinos" y anunció que había "realizado fuertes gestiones con Estados Unidos y las partes relevantes".

Gran Bretaña convocó al embajador de China al Foreign Office para protestar.

En Estados Unidos

Las autoridades estadounidenses revelaron que un pequeño grupo de piratas informáticos chinos, conocido como Advanced Persistent Threat 31 (APT31), había comprometido los correos electrónicos, el almacenamiento en la nube y los registros de llamadas telefónicas de millones de estadounidenses . Los piratas informáticos enviaron 10.000 correos electrónicos "maliciosos" a sus objetivos para comprometer sus sistemas.

Los parlamentarios piden una "nueva era de relaciones con China " en medio de informes de ciberataques.

Estados Unidos advirtió que esta información podría divulgarse en apoyo de una "influencia maligna", dirigida a procesos e instituciones democráticas, planes económicos, propiedad intelectual y secretos comerciales pertenecientes a empresas estadounidenses.

En Nueva Zelanda

Agentes chinos, respaldados por el Estado, también atacaron la oficina de asesoría parlamentaria y el servicio parlamentario de Nueva Zelanda en 2021, dijo Judith Collins, ministra de seguridad de Nueva Zelanda.

Una evaluación encontró que los actores patrocinados por el estado chino, conocidos como Amenaza Persistente Avanzada 40 (APT 40), eran los responsables. Están vinculados con el Ministerio de Seguridad del Estado de China, según la Oficina de Seguridad de las Comunicaciones del Gobierno de Nueva Zelanda (GCSB).

La GCSB dijo el martes que, si bien los datos habían sido eliminados de los sistemas informáticos del parlamento de Nueva Zelanda, no eran de naturaleza "estratégica".

"El uso de operaciones de espionaje cibernéticas para interferir con las instituciones y procesos democráticos en cualquier lugar es inaceptable ", afirmó Collins.

Al igual que el Reino Unido y los Estados Unidos, Nueva Zelanda también es miembro de la red de inteligencia occidental Five Eyes, que incluye a Canadá y Australia.

Los ministros también están preparados para declarar formalmente a China una amenaza a la seguridad nacional de Gran Bretaña tras las revelaciones de la escala de su ciberataque al Reino Unido, indicó el viceprimer ministro.

En la Cámara de los Comunes, Oliver Dowden, viceprimer ministro, insistió en que los procesos políticos y las instituciones del Reino Unido no habían resultado perjudicados.






"No afectará la forma en que las personas se registran, votan o participan de otro modo en los procesos democráticos", dijo. "Quiero asegurarle a la gente que la puesta en peligro de esta información, si bien es obviamente preocupante, normalmente no crea un riesgo para los afectados", dijo.

China desmiente

China negó las acusaciones. La embajada china dijo: "Los llamados ciberataques de China contra el Reino Unido son calumnias

Argentina - Flipr (Online) [Online]

Tier:N/D Circulación: 2551 Audiencia 2551

 P. --  0 cm²  11524 cc  N/D N/D  Sin autor

Ref.: 516455710

completamente inventadas y maliciosas. Nos oponemos firmemente a tales acusaciones. China siempre ha luchado firmemente contra todas las formas ciberataques".

"China no fomenta, apoya ni tolera los ciberataques" dijo.

Robert Jenrick, ex ministro de Inmigración británico, describió la respuesta como irrisoria y acusó al gobierno de "dejar que China salga libre de costos". "Esta débil respuesta sólo envalentonará a China para continuar su agresión hacia el Reino Unido. Está muy claro que China debería ser clasificada como un Estado hostil", dijo.

Merrick Garland, fiscal general de Estados Unidos, dijo que la investigación mostraba "los fines a los que el gobierno chino está dispuesto a llegar para atacar e intimidar a sus críticos" y amenazar la "seguridad nacional de Estados Unidos y nuestros aliados".

Lisa Monaco, su adjunta, añadió: "El Departamento de Justicia perseguirá, expondrá y responsabilizará implacablemente a los ciberdelinquentes que socavarían las democracias y amenazarían nuestra seguridad nacional".

El año pasado, The Times reveló que un espía chino estaba utilizando perfiles de LinkedIn para atraer a funcionarios británicos para que entregaran secretos de estado a cambio de dinero.

Durante cinco años, el agente, cuyo alias principal es Robin Zhang, creó una serie de alias y empresas falsas, para atacar a funcionarios de seguridad, funcionarios públicos, científicos y académicos, con acceso a información clasificada o tecnología comercialmente sensible.

China, quinto socio comercial británico

China es el quinto socio comercial de Gran Bretaña. Si bien las importaciones totales desde China disminuyeron el año pasado, las exportaciones británicas crecieron casi un 12 por ciento.

Las cifras del gobierno muestran que el comercio de bienes y servicios en los 12 meses hasta finales de septiembre ascendió a 100,9 mil millones de libras esterlinas. De esto, las exportaciones a China representaron 37,5 mil millones de libras (un aumento del 11,9% respecto a los 12 meses anteriores) y las importaciones representaron 63,5 mil millones de libras (un descenso del 12,6%).

La consultora Grant Thornton descubrió este mes que 970 empresas de propiedad china emplean a más de 59.000 personas en el Reino Unido. En el 2023 contribuyeron con 116.400 millones de libras esterlinas de ingresos totales a la economía.

El dominical El Sunday Times informó que EVE Energy, el fabricante chino de baterías cilíndricas para automóviles tipo Tesla, estaba a punto de invertir miles de millones en la construcción de la gigafábrica más grande de Gran Bretaña. Se entiende que se encuentran en negociaciones avanzadas para construir una fábrica de 60 gigavatios-hora en las afueras de Coventry. La empresa se comprometerá inicialmente a invertir al menos 1.200 millones de libras esterlinas en una gigafábrica de 20 GWh, según fuentes cercanas a las negociaciones.

Algunas de las mayores inversiones de China se han producido en el sector energético, específicamente en la energía nuclear.

China General Nuclear (CGN), propiedad del Estado chino, compró una participación del 33,5 por ciento en la central eléctrica Hinkley Point C en Somerset, la primera nueva instalación nuclear construida en el Reino Unido en más de 20 años.

CGN, que ha sido incluida en la lista negra de Estados Unidos por supuestamente ayudar a adquirir tecnología estadounidense para uso militar en China, finalmente se vio obligada a abandonar el proyecto utilizando el dinero de los contribuyentes. Pero el comité de inteligencia y seguridad advirtió el año pasado que tenía serias dudas sobre proyectos futuros.

El Estado chino también ha acumulado participaciones en empresas británicas de petróleo y gas y en los sectores de tecnología y educación.

Consejos para contraseñas

Las personas con acceso a información confidencial han recibido nuevos consejos para proteger sus contraseñas y dispositivos de los espías chinos.

La nueva guía, publicada por el Centro Nacional de Seguridad Cibernética (NCSC), acepta que "puede ser difícil recordar las contraseñas, por lo que está bien escribirlas". Pero insta a las personas a "mantenerlas seguras, donde otras personas no puedan acceder a ellas".

"Sepárelo de sus dispositivos", sugieren.

Recomienda utilizar un administrador de contraseñas en línea, que ofrecerá una forma segura de almacenar contraseñas, ya sea en un navegador de Internet o en una aplicación, que utilice una contraseña maestra o datos biométricos.

El NCSC dice que cuando los atacantes comprometen una cuenta, a menudo roban o adivinan la contraseña, en lugar de utilizar un método más sofisticado. Las contraseñas débiles a menudo contenían nombres, lugares o una serie de números. El consejo añade: "El NCSC recomienda utilizar una secuencia de tres palabras aleatorias para hacer una contraseña compleja pero fácil de recordar".

El consejo está dirigido a personas de "alto riesgo", incluidos políticos, su personal, activistas, académicos, periodistas y abogados, que tienen acceso o influencia sobre información sensible que "podría ser de interés para los actores estatales nacionales".

Aconseja a las personas que siempre instalen actualizaciones para aplicaciones y dispositivos y que reemplacen teléfonos y computadoras portátiles antiguas cuando los fabricantes dejen de publicar actualizaciones de seguridad.

Fuente: