



| Flash |

UK Confirms Chinese State-Sponsored Cyber Attacks

F-2024-03-25a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Data Breach, State-Affiliated Cyber Activity

March 25, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 AM (EDT) on March 25, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | UK Confirms Chinese State-Sponsored Cyber Attacks

> Key Findings

- On March 25, 2024, the UK Government publicly warned of a growing threat from Chinese State-sponsored entities targeting and undermining the country's democratic processes. The announcement attributed two cyber attacks against UK political entities to Chinese State-sponsored actors.
- On the same day, the United States Justice Department and Federal Bureau of Investigation unsealed an indictment against seven alleged Chinese hackers associated with APT31 involved in targeting United States-based critics, businesses, and political officials over approximately 14 years.
- Illicitly-obtained personal information of UK citizens is unlikely to be leveraged in directly influencing the results of UK general elections, which are due to take place in late 2024-early 2025. However, illicit access to sensitive communications between political figures and policy decisions could be of significant value to adversarial nation state entities.
- These events are likely part of broader Chinese strategic initiatives, seeking to gather information, exert strategic influence, demonstrate cyber capabilities, undermine Western institutions, and conduct targeted punitive measures in response to recent political disagreements.

Details

On March 25, 2024, the UK Government publicly warned of a growing threat from Chinese State-sponsored entities targeting and undermining the country's democratic processes. The announcement comes in advance of upcoming UK local elections in 2024 and a general election set to take place in 2024 or early 2025. The United States has also unsealed an indictment against seven individuals associated with the Chinese Government for malicious activity against United States-based entities.

The announcement—made by UK Deputy Prime Minister Oliver Dowden—attributed two cyber attacks against UK political entities to Chinese State-sponsored actors. ZeroFox can neither confirm nor deny the identification of any further undisclosed attacks against UK political targets.

- In a recently disclosed attack, UK Members of Parliament (MPs) and Peers are reportedly among 43 MPs—likely those to have taken stances critical of the Chinese state—targeted by cyber attacks directed by the Chinese state.
- The speech also confirmed that in August 2021, Chinese State-sponsored entities hacked the UK's Electoral Commission, reportedly gaining access to 40 million voters' personal details. The attack was only publicly disclosed in 2022.
- In response, Oliver Dowden announced the sanctioning of two individuals and one entity associated with the Chinese State-affiliated APT 31 for its involvement in malicious cyber activity targeting officials, government entities, and parliamentarians globally.¹

ZeroFox can provide no further detail on the nature of these attacks; the techniques leveraged, the extent of the targets, the likely intent, or the timeframe.

- Illicitly-obtained personal information of UK citizens is unlikely sufficient to directly influence the results of UK general elections, which are due to take place in late 2024-early 2025. There is a roughly even chance that aspects of the stolen information will be sold in deep and dark web marketplaces, as the alleged nature and quantity of the stolen data would very likely carry considerable value in deep and dark web marketplaces.

¹

<https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity>

- While the nature of the targeting of UK political figures is unknown, illicit access to sensitive communications and policy decisions could be of significant value to adversarial nation state entities.

These attacks are very likely part of broader Chinese strategic initiatives seeking to:

- Gather information,
- Exert strategic influence,
- Demonstrate cyber capabilities,
- Undermine Western institutions,
- Conduct punitive retaliation in response to recent political disagreements.

Chinese State-affiliated entities have a history of conducting cyber attacks against targets in nations deemed in opposition to its economic and foreign policy objectives, including with regard to Hong Kong and Taiwan. State-affiliate entities are known to conduct financially-motivated data theft against targets including foreign government departments, as seen in the February 2024 iSoon data breach.²

- In March 2024, a U.S. Army intelligence analyst was arrested and charged with conspiring to sell sensitive defense information to China.³
- In 2023, a UK parliamentary researcher was arrested on suspicion of spying for the Chinese State. The named individual reportedly worked for the China Research Group, as well as holding a role as a researcher for the Chair of the UK's Foreign Affairs Select Committee. Another unnamed individual was also arrested at the time.⁴
- In 2023, the Belgian and French foreign ministries publicly confirmed Chinese state-sponsored cyber attacks against its members.⁵

The announcement follows a spate of disagreements between the UK and China in recent years, in areas such as geopolitics, national security, and espionage.

² ZeroFox Intelligence Brief – iSoon Data Breach and China's Geopolitical Strategy, February 28, 2024

³

[hXXps://www.reuters\[.\]com/world/us/us-army-intelligence-analyst-charged-with-selling-military-secrets-china-2024-03-07/](https://www.reuters.com/world/us/us-army-intelligence-analyst-charged-with-selling-military-secrets-china-2024-03-07/)

⁴

[hXXps://www.theguardian\[.\]com/uk-news/2024/mar/23/china-targets-group-of-mps-and-peers-with-string-of-cyber-attacks](https://www.theguardian.com/uk-news/2024/mar/23/china-targets-group-of-mps-and-peers-with-string-of-cyber-attacks)

⁵ [hXXps://www.bbc\[.\]co.uk/news/live/uk-politics-68654299](https://www.bbc.com/news/live/uk-politics-68654299)

- The timing of the August 2021 Electoral Commission attack came after the UK publically began a special five-year visa for Hong Kongers to live in the UK that paves the way for UK citizenship. The visa was announced in response to mainland China imposing its National Security Law on Hong Kong. The national security law drastically reduces the political freedoms of residents of Hong Kong.⁶
- An updated Hong Kong-specific version known as Article 23 went into effect in Chinese law on March 23, 2024.⁷ The legislation expands the scope of what can be defined as a political crime, and seeks to mitigate against “espionage” and “the unlawful acquisition of state secrets.” The legislation was widely condemned as antidemocratic by the international community, including the UK, which expressed concern over the violation of the country’s autonomy.⁸

European nations have adopted U.S. policies on reducing China’s access to advanced technology and reducing China’s overall dominance of trade by encouraging Western manufacturers with operations inside of China to move those operations to other countries with friendlier relations with the West.

- In mid-June 2023, the European Union (EU) published its Economic Security Initiative. The economic element of the document highlights the industries Europe would like to cultivate—mainly advanced technology and clean energy.⁹ The document specified which industries the EU would need to trade and negotiate with in order to achieve those goals. The security element of the document unambiguously signaled China as the key threat to these goals, citing China’s domination of supply lines for assets such as rare earth metals, considered vital for “clean” energy technologies.
- The UK also recently announced its Critical Imports and Supply Chains Strategy,¹⁰ which highlighted imports deemed by the UK as critical to its economy, as well as the national security implications of the UK’s heavy reliance on China for many of these imports.

⁶

[hXXps://www.npr\[.\]org/2021/10/25/1048918729/the-u-k-is-welcoming-tens-of-thousands-from-hong-kong-on-a-new-path-to-citizenship](https://www.npr.org/2021/10/25/1048918729/the-u-k-is-welcoming-tens-of-thousands-from-hong-kong-on-a-new-path-to-citizenship)

⁷ [hXXps://www.gld\[.\]gov.hk/egazette/pdf/20242811e/es3202428112.pdf](https://www.gld[.]gov.hk/egazette/pdf/20242811e/es3202428112.pdf)

⁸ [hXXps://www.gov\[.\]uk/government/news/uk-statement-on-hong-kong-national-security-proposals](https://www.gov[.]uk/government/news/uk-statement-on-hong-kong-national-security-proposals)

⁹ [hXXps://www.csis\[.\]org/analysis/european-unions-economic-security-strategy-update](https://www.csis[.]org/analysis/european-unions-economic-security-strategy-update)

¹⁰ [hXXps://www.gov\[.\]uk/government/publications/uk-critical-imports-and-supply-chains-strategy](https://www.gov[.]uk/government/publications/uk-critical-imports-and-supply-chains-strategy)

- Both sets of policies mirror the U.S. CHIPS ACT and Inflation Reduction Act, which aim to prohibit Chinese access to advanced semiconductors and move manufacturing operations outside of China.

On March 25, 2024, the United States Justice Department and Federal Bureau of Investigation unsealed an indictment against seven alleged Chinese hackers associated with APT31 involved in targeting the United States and foreign individuals and companies over approximately 14 years.¹¹

- The statement claims that the individuals and associated APT31 operation targeted thousands of United States-based critics, businesses, and political officials.
- Some of this activity reportedly resulted in successful compromises of the targets' networks, email and personal accounts, cloud storage, and telephone records, with some surveillance of compromised email accounts lasting many years.
- It is claimed the activity was conducted to further China's economic, espionage, and foreign intelligence objectives.

Tensions between the UK, The West, and China are very likely to continue intensifying over the short to medium-term, as ongoing geopolitical affairs illuminate geopolitical, economic, and military divisions.

- Such tensions would be manifested by both overt and covert state-level activity focused on the furthering of strategic national agendas.
- China is likely to respond officially with retaliatory sanctions, as well as potential divestment of China-based business in the UK economy.

ZeroFox recommends that organizations safeguard classified, sensitive, or business-critical assets using secure, off-site backup methods, compartmentalization, and authentication mechanisms.

¹¹

[hXXps://www.justice\[.\]gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived](https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived)

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%