UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity

Foreign, Commonwealth & Development Office ⋮⋮ 3/25/2024

The United Kingdom, supported by allies globally, have today identified that Chinese state-affiliated organisations and individuals were responsible for 2 malicious cyber campaigns targeting democratic institutions and parliamentarians. Partners across the Indo-Pacific and Europe also express solidarity with the UK's efforts to call out malicious cyber activities targeting democratic institutions and electoral processes.

First, the UK can reveal today that the National Cyber Security Centre (NCSC) – a part of GCHQ – assesses that the UK Electoral Commission systems were highly likely compromised by a Chinese state-affiliated entity between 2021 and 2022.

Second, NCSC assesses it is almost certain that the China state-affiliated Advanced Persistent Threat Group 31 (APT31) conducted reconnaissance activity against UK parliamentarians during a separate campaign in 2021. The majority of those targeted were prominent in calling out the malign activity of China. No parliamentary accounts were successfully compromised.

This is the latest in a clear pattern of malicious cyber activity by Chinese state-affiliated organisations and individuals targeting democratic institutions and parliamentarians in the UK and beyond.

In response, the Foreign, Commonwealth and Development Office has today summoned the Chinese Ambassador to the UK, and sanctioned a front company and 2 individuals who are members of APT31. Concurrently, the United States is designating the same persons and entity for malicious cyber activity. We greatly value our close coordination and cooperation with the US in addressing these threats. This sends a clear message that we will not tolerate malicious cyber activity against democratic institutions and parliamentarians.

Foreign Secretary Lord Cameron said:

> It is completely unacceptable that China state-affiliated organisations and individuals have targeted our democratic institutions and political processes. While these attempts to interfere with UK democracy have not been successful, we will remain vigilant and resilient to the threats we face.
>
> I raised this directly with Chinese Foreign Minister Wang Yi and we have today sanctioned 2 individuals and one entity involved with the China state-affiliated group responsible for targeting our parliamentarians.
>
> We will always defend ourselves from those who seek to threaten the freedoms that underpin our values and democracy. One of the reasons that it is important to make this statement is that other countries should see the detail of threats that our systems and democracies face.

Deputy Prime Minister Oliver Dowden said:

> The UK will not tolerate malicious cyber activity targeting our democratic institutions. It is an absolute priority for the UK government to protect our democratic system and values. The Defending Democracy Taskforce continues to coordinate work to build resilience against these threats.
>
> I hope this statement helps to build wider awareness of how politicians and those involved in our democratic processes around the world are being targeted by state-sponsored cyber operations.
>
> We will continue to call out this activity, holding the Chinese government accountable for its actions.

Home Secretary James Cleverly said:

> It is reprehensible that China sought to target our democratic institutions.
>
> China's attempts at espionage did not give them the results they wanted and our new National Security Act has made the UK an even harder target. Our upcoming elections, at local and national level, are robust and secure.
>
> Democracy and the rule of law is paramount to the United Kingdom. Targeting our elected representatives and electoral processes will never go unchallenged.

This statement today sees the international community once again call on the Chinese government to demonstrate its credibility as a responsible cyber actor. The UK will continue to call out malicious cyber activity that infringes on our national security and democracy.

The UK believes these behaviours are part of large-scale espionage campaign. We have been clear that the targeting of democratic institutions is completely unacceptable. To date, cumulative attempts to interfere with UK democracy and politics have not been successful. The UK has bolstered its defences against these types of incidents. The Defending Democracy Taskforce and the National Security Act 2023 give government, Parliament, the security services, and law enforcement agencies the tools they need to disrupt hostile activity. The NCSC has also published guidance to help high-risk individuals, including

parliamentarians, to bolster their resilience to cyber threats, as well as advice to help organisations improve their security.

Find out more: FCDO summons Chinese Chargé d'Affaires over malicious cyber activity.

You can also view the full UK Sanctions List.

Background

Sanctions

The individuals and entity being designated in the UK are:

- Wuhan Xiaoruizhi Science and Technology Company Limited, which is associated with APT31, operating on behalf of the Chinese Ministry of State Security (MSS) as part of China's state-sponsored apparatus
- Zhao Guangzong, who is a member of APT31, operating on behalf of the Chinese Ministry of State Security (MSS), and has engaged in cyber activities targeting officials, government entities, and parliamentarians in the UK and internationally
- Ni Gaobin who is a member of APT31, operating on behalf of the Chinese Ministry of State Security (MSS), and has engaged in cyber activities targeting officials, government entities, and parliamentarians in the UK and internationally

Electoral Commission

The Electoral Commission oversees elections and regulates political finance in the UK. It is independent of UK government and reports to the UK, Welsh and Scottish Parliaments. Between late 2021 and October 2022 the Electoral Commission's systems were compromised by a China state-affiliated cyber actor.

As the Electoral Commission stated in 2023, the malicious cyber activity has not had an impact on electoral processes, has not affected the rights or access to the democratic process of any individual, nor has it affected electoral registration. The Electoral Commission has taken steps to secure its systems against future activity. When the compromise was discovered, the Commission worked with NCSC and security specialists to investigate the incident, and acted to secure its systems to reduce the risk of future attacks.

Targeting of UK parliamentarians by APT31

NCSC assesses it is highly likely that the China state-affiliated cyber actor APT31 conducted reconnaissance activity against UK parliamentarians during a separate campaign in 2021. Parliamentary Cybersecurity Team identified this reconnaissance and were able to confirm that no accounts had been compromised.

APT31 was one of a number of Chinese state-affiliated organisations the UK publicly linked to the Chinese Ministry of State Security in 2021 following the hacking of Microsoft Exchange Server globally. Similar statements were issued by allies in condemning these actions.

Further information

- earlier this year, NCSC and partners issued a warning about state- sponsored cyber attackers hiding on critical infrastructure networks, and released an advisory on China state-sponsored cyber actors compromising and maintaining persistent access to US critical infrastructure
- in December 2023, the UK also condemned attempted Russian cyber interference in politics and democratic processes
- in May 2023, NCSC and partners issued a warning around China state-sponsored cyber activities targeting Critical National Infrastructure (CNI) networks
- an asset freeze prevents any UK citizen, or any business in the UK, from dealing with any funds or economic resources which are owned, held or controlled by the designated person. It also prevents funds or economic resources being provided to or for the benefit of the designated person. UK financial sanctions apply to all persons within the territory and territorial sea of the UK and to all UK persons, wherever they are in the world
- a travel ban means that the designated person must be refused leave to enter or to remain in the United Kingdom, providing the individual is an excluded person under section 8B of the Immigration Act 1971