UK Blames China for 2021 Hack Targeting Millions of Voters' Data

By Kevin Poireault

Published: 2024-03-25 · Archived: 2026-04-05 15:31:27 UTC

The UK government has called out China state-affiliated threat actors for carrying out hacking campaigns against UK institutions and political figures in 2021.

The House of Commons was briefed on March 25 by UK Deputy Prime Minister Oliver Dowden about cyber-attacks that accessed the personal details of millions of voters in August 2021.

Chinese-backed threat actors have been blamed following an investigation led by the UK National Cyber Security Centre (NCSC), which assessed that the attack originated from China.

Electoral Commission Hack Linked to Chinese Intelligence Services

In August 2023, the UK's Electoral Commission revealed that an attack on voters' data occurred in August 2021. The incident was first discovered in October 2022.

The threat actor had broken into the election watchdog's emails and "control systems" and gained access to copies of the electoral registers.

Although the Commission said at the time it could not identify how much data was compromised, its register contains the details of approximately 40 million people.

According to NCSC, it is highly likely that a China-backed threat actor accessed and exfiltrated data, including email data, from the Electoral Register during this time.

"The data, in combination with other data sources, would highly likely be used by the Chinese intelligence services for a range of purposes, including large-scale espionage and transnational repression of perceived dissidents and critics in the UK," the NCSC added in a public statement.

The threat group has not been named.

Speaking to *Infosecurity*, Camellia Chan, CEO and co-founder of Flexxon, commented that it is "incredibly concerning" that the cyber-attack which took place in 2021 has only today been linked to the cybercriminals responsible.

She added: "With more than 2 billion voters in more than 50 countries heading to the polls this year – the UK included – robust cybersecurity measures are needed to ensure threats are detected and dealt with as soon as possible, not only for voter safety but government protection too. This includes identifying cybercriminals and making them public to ensure others are aware of the threat posed."

China-Backed APT31 Behind MP Email Hacking Campaign

Separately, the NCSC investigation concluded that the Chinese-affiliated threat actor APT31 (aka Judgement Panda, Violet Typhoon, Zirconium) was “almost certainly” responsible for conducting online reconnaissance activity against the email accounts of UK parliamentarians in 2021.

The parliamentarians included former Conservative leader Sir Iain Duncan Smith, former Conservative minister Tim Loughton, and MP and Scottish National Party (SNP) member Stewart McDonald.

The three are all members of the Inter-Parliamentary Alliance on China, a committee that has often been critical of China.

The NCSC added that this latter cyber-attack “was identified and successfully mitigated by Parliament’s Security Department before any accounts could be compromised.”

During his address to British MPs, Dowden also said the UK issued sanctions against one Chinese-affiliated organization and two individuals involved in the malicious campaigns targeting the UK.

China Denies Involvement

Former British Army and UK Government intelligence specialist and co-founder of Ecliptic Dynamics, Tom Kidwell, told *Infosecurity* that this outright accusation was a first and could have a significant impact.

“The proposed sanctions from the UK to China marks a huge shift in the rhetoric against the Chinese State by the UK. Publicly accusing another member of the UN Security Council of attempting to influence or disrupt your election process is significant,” he said.

Kidwell added that China would never acknowledge any involvement in the attacks and that the relationship between the two states could worsen.

“Providing hard evidence of a direct link to Chinese state involvement will be difficult to release into the public domain,” he said. “This will likely just become a back and forth between the two states, with the UK making a public accusation and China inevitably denying involvement.”

The Chinese government has already denied involvement in either malicious campaign. During a press conference, Lin Jian, a Chinese Foreign Ministry spokesperson, described the UK accusations as “false information.” He invited the UK government to back their claims with “objective evidence.”

“We advocate all countries to deal with this together through dialogue and cooperation. We hope, rather that parties can stop spreading this false information and take a responsible attitude and jointly safeguard security and peace of cyberspace,” Jian added.

Cybersecurity Experts Question the Purpose of Such a Data Theft

The targeting of British politicians by a foreign power should not be a surprise to the UK government, according to Stephen Robinson, a senior threat intelligence analyst at WithSecure.

“Indeed, recent reporting on the I-Soon leaks has stated that organizations who were contracted to perform cyber operations for the Chinese government described the UK Foreign Office and Treasury as priority targets for the Chinese government,” he said.

Read more: I-Soon GitHub Leak: What Cyber Experts Learned About Chinese Cyber Espionage

However, Robinson warned not to draw hasty conclusions regarding the objectives of these malicious campaigns.

Like other large data breaches attributed to China, such as the Equifax hack in 2020, Robinson added that data theft from the Electoral Commission could be motivated by a desire for high-quality PII on UK citizens rather than an attempt at direct electoral influence.

Kidwell raised the same question: “What is interesting is the point of the attack. If China was responsible, what did they seek to achieve? Was it to collect data, or to disrupt or influence the outcome? If it was to influence the outcome of future elections, what would be the best outcome from a Chinese perspective?”

“For me, the key line in the reports I have seen is that the attacks targeted 'control systems.' This likely means that the attackers attempted to gain access to these systems to wait for a more impactful point in the future to deliver the intended payload and cause the desired disruption,” Kidwell commented.

“It isn’t a coincidence that the UK is releasing this information in the build-up to an election, and I would expect more of this in the coming months in terms of rhetoric from the UK and allies,” he concluded.

UK Releases New ‘Defending Democracy’ Guidance

Paul Chichester, NCSC Director of Operations, commented: “The targeting of our democratic system is unacceptable and the NCSC will continue to call out cyber actors who pose a threat to the institutions and values that underpin our society. The malicious activities we have exposed today are indicative of a wider pattern of unacceptable behavior we are seeing from China state-affiliated actors against the UK and around the world.”

“It is vital that organizations and individuals involved in our democratic processes defend themselves in cyberspace, and I urge them to follow and implement the NCSC’s advice to stay safe online.”

The Dowden address to British MPs coincided with the publication of new ‘Defending Democracy’ guidance.

This document offers advice to aid IT practitioners implement security measures that will help prevent common cyber-attacks.

These include establishing controls against spear-phishing and DDoS attacks as well as setting up multifactor authentication on cloud and internet-connected services.

US Sanctions APT31 Associates

While Dowden was speaking in the House of Commons, the US government issued sanctions against one Chinese entity and seven individuals, some of whom were also accused of being associated with APT31.

The sanctioned Chinese organization is Wuhan Xiaoruizhi Science and Technology Company, Limited (also known as Wuhan XRZ), a Ministry of State Security (MSS) front company based in Wuhan.

It “has served as cover for multiple malicious cyber operations,” said the US Department of the Treasury’s Office of Foreign Assets Control (OFAC) in a public statement.

Two of the seven individuals indicted by the US Justice Department, Zhao Guangzong and Ni Gaobin, are affiliated with Wuhan XRZ.

The indictment accused them of participating in a yearslong hacking effort that targeted “some of America’s most vital critical infrastructure sectors [and] resulted in the confirmed and potential compromise of data belonging to millions of Americans, [some of] which could be released in support of malign influence targeting US democratic institutions.”

On March 26, the New Zealand government also accused China of hacking the country's parliamentarian entities.

This article has been updated on March 26, 2024.
