Written by **Angeline Tan** on March 27, 2024

# US Sanctions Chinese Firm Saying It Hacked US Energy Industry

mirsad sarajlic/iStock/Getty Images Plus

On March 25, Washington slapped sanctions on a China-based firm it said was a Ministry of State Security front company, accusing it of acting as a cover for various malicious cyber operations and targeting critical U.S. infrastructure.

In a statement, the U.S. Treasury Department said the sanctions were on Wuhan Xiaoruizhi Science and Technology and two Chinese nationals. Treasury said this was part of an effort adopted alongside the U.S. Justice Department, FBI, and State Department, and the United Kingdom. London announced the sanctions against Wuhan Xiaoruizhi, Zhao Guangzong, and Ni Gaobin, on Monday. According to the British government, they are responsible for two cyber attacks on British voting.

China state-sponsored malicious cyber actors remain one of the greatest and most persistent threats to U.S. national security, Treasury declared. The cyber security industry has labeled such entities as advanced persistent threats (APTs), and the government also uses that acronym.

Treasury said APT31 is a collection of Chinese intelligence officers working for the Hubei branch of China's Ministry of State Security (MSS) who carry out cyber espionage campaigns on behalf of the state, and that those same officers created a company, Wuhan Xiaoruizhi Science and Technology, to use as a front to carry out those campaigns.

The department said APT31 has targeted high-ranking U.S. officials and their advisors, including at the White House; in the departments of Justice, Commerce, Treasury, and State; members of Congress; and others.

Wuhan Xiaoruizhi Science and Technology's activity led to the surveillance of U.S. and foreign politicians, foreign policy experts, academics, journalists, pro-democracy activists, and others, Treasury said, adding that in 2018 employees of the company carried out an APT31 malicious cyber operation on a Texas-based energy company.

"The United States is focused on both disrupting the dangerous and irresponsible actions of malicious cyber actors, as well as protecting our citizens and our critical infrastructure," Treasury's Under Secretary for Terrorism and Financial Intelligence, Brian Nelson, said in the statement. "Through our whole-of-government approach and in close coordination with our British partners, Treasury will continue to leverage our tools to expose these networks and protect against these threats."

Similarly, New Zealand's spy agency posited that a hacking group sponsored by the Chinese government staged a cyberattack against that country's parliament, stealing data on some of its MPs.

Beijing has rebuffed the accusation, which it alleges is not supported by any evidence.

The alleged breach occurred in 2021 and targeted the Parliamentary Counsel Office and the Parliamentary Service, Government Communications Security Bureau (GCSB) Minister Judith Collins said in a statement on March 25.

The "malicious cyber activity" was swiftly detected by New Zealand's authorities, which prevented the hackers from accessing data of a "strategic or sensitive" nature, she said.

As per Collins, APT40, which the GCSB claims is linked to China's Ministry of State Security, was responsible for the attack. "The use of cyber-enabled espionage operations to interfere with democratic institutions and processes anywhere is unacceptable," she said.

The GCSB minister said Wellington had confronted Beijing about the alleged cyberattack, but underscored that New Zealand had no plans to sanction China over the incident.

Notably, the statement by Collins came on the same day the U.S. Department of Justice released photos of seven Chinese nationals wanted on charges of infiltrating the communications of British and American targets over a 14-year period through malicious emails.

The men were said to be members of APT31, the state-sponsored hacking group also known as "Violet Typhoon."

Collins highlighted the importance of a collective response by the West to the alleged cyber-security threat posed by China, saying "it's important [that] liberal democracies stand up for other liberal democracies."

The Chinese embassy in New Zealand disavowed the accusations by Wellington as "groundless and irresponsible," saying Beijing had voiced "strong dissatisfaction and resolute opposition" to the island nation's authorities.

"When investigating and determining the nature of cyber cases, one needs to have adequate and objective evidence, instead of smearing other countries when facts do not exist, still less politicize or even weaponize cybersecurity issues," the embassy said in a statement on March 26.

In an apparent reference to the United States, the Chinese diplomats claimed that Beijing does not meddle in the internal affairs of other countries, and that "accusing China of foreign interference is completely barking up the wrong tree."

China is ready to promote cooperation with Wellington "on the basis of mutual respect," and hopes that New Zealand will work in the same direction and refrain from "megaphone diplomacy," the statement read.

Additionally, the Chinese government said on March 26 that British claims about the alleged hacking by Wuhan Xiaoruizhi, Zhao, and Ni of the U.K. Electoral Commission are false and groundless.

"The UK's hype-up of the so-called 'Chinese cyber attacks' without basis and the announcement of sanctions is outright political manipulation and malicious slander," the Chinese embassy in London said. "We have no interest or need to meddle in the UK's internal affairs."

The embassy demanded the U.K. "immediately stop spreading false information" about China.

British evidence provided to Beijing about APT31 was "inadequate," while the "relevant conclusions lack professionalism," Chinese Foreign Ministry spokesman Lin Jian told reporters on March 26, adding

that China "will take necessary measures to safeguard our lawful rights and interests."

British Foreign Secretary David Cameron announced his country's sanctions on China on March 25, accusing the latter of "attacks on our democracy" and vowing that such actions "will not be tolerated."

The cyber attacks on the U.K. Electoral Commission between August 2021 and October 2022 allegedly accessed voter databases as well as sensitive emails of "control systems" and officials involved in six by-elections.