Czechia blames China for Ministry of Foreign Affairs cyberattack

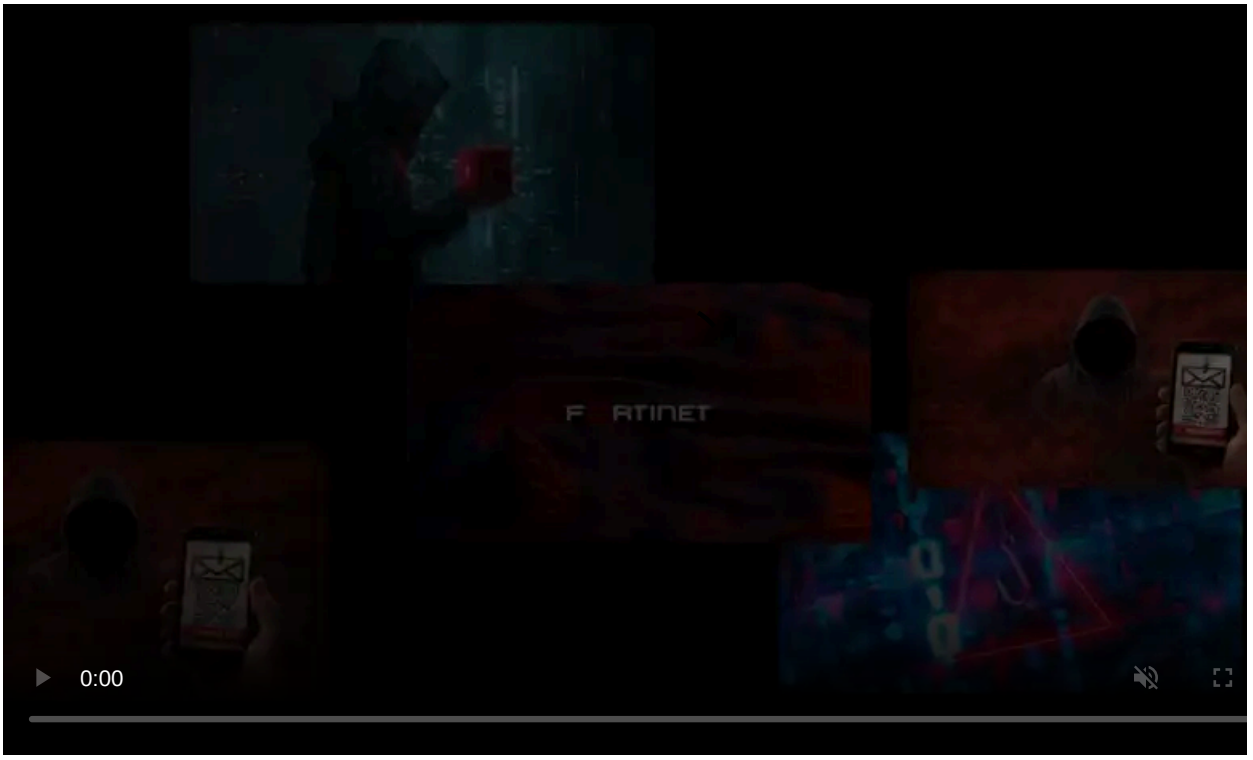
By Sergiu Gatlan

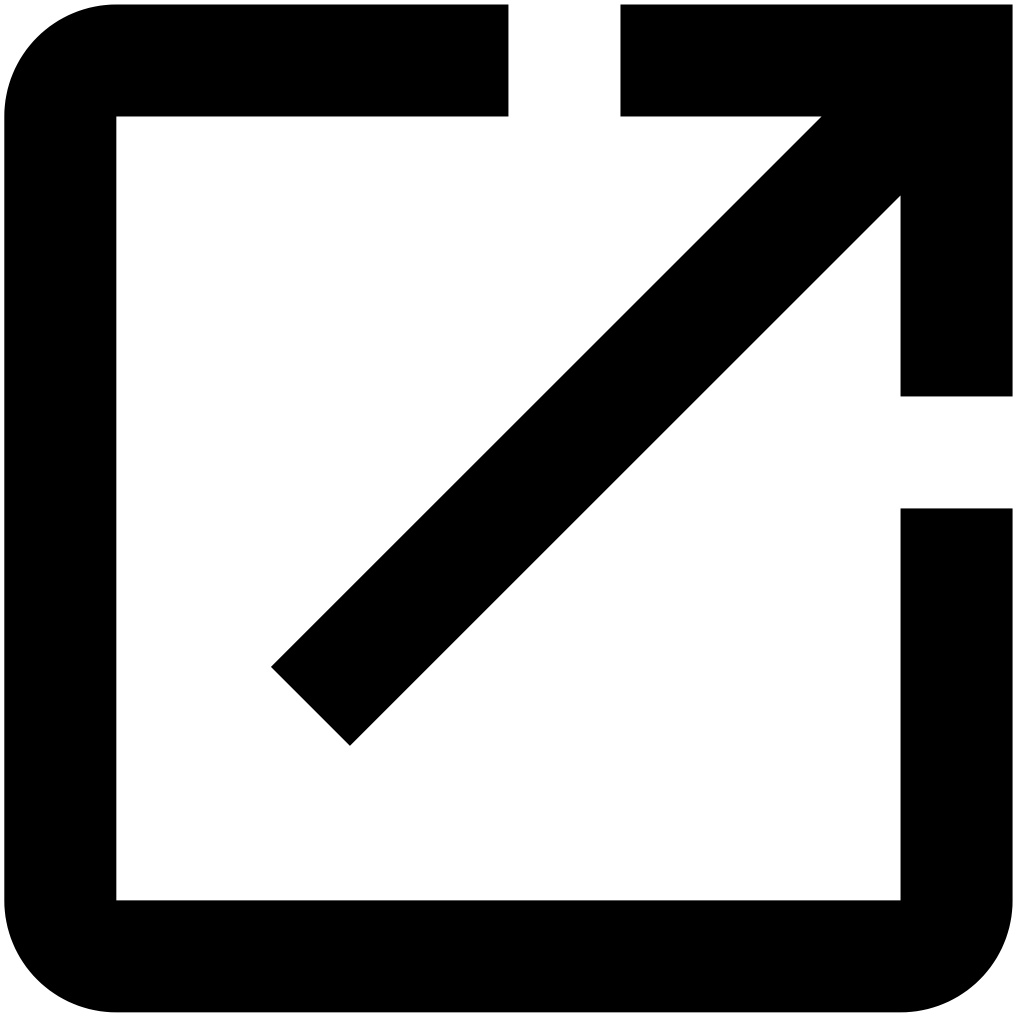
Published: 2025-05-28 · Archived: 2026-04-05 21:24:05 UTC

The Czech Republic says the Chinese-backed APT31 hacking group was behind cyberattacks targeting the country's Ministry of Foreign Affairs and critical infrastructure organizations.

"The malicious activity, which lasted from 2022 and affected an institution designated as Czech critical infrastructure, was perpetrated by the cyberespionage actor APT31 that is publicly associated with the Ministry of State Security," the Czech government said.

"The Government of the Czech Republic strongly condemns this malicious cyber campaign against its critical infrastructure. Such behavior undermines the credibility of the People's Republic of China and contradicts its public declarations."


F RTINET
0:00



European Union member states and NATO allies condemned the attack on Wednesday, asking China to adhere to the UN norms and respect international law.

Two months ago, the Finnish Police confirmed that APT31 hackers were behind a March 2021 breach of the country's parliament when the attackers compromised multiple email accounts, including some belonging to Finnish MPs.

In July 2021, the United States and its allies blamed the Chinese MSS-linked APT31 and APT40 threat groups for an extensive hacking campaign that targeted over a quarter of a million Microsoft Exchange servers belonging to tens of thousands of organizations worldwide.

"In recent years, malicious cyber activities linked to this country and targeting the EU and its Member States have increased. In 2021, we urged Chinese authorities to take action against malicious cyber activities undertaken from their territory," the Council of the EU said on Wednesday.

"Since then, several Member States have attributed similar activities at their national level. We have repeatedly raised our concerns during bilateral engagements and we will continue to do so in the future."

"We strongly condemn malicious cyber activities intended to undermine our national security, democratic institutions and critical infrastructure," NATO added.

APT31 charges and sanctions

APT31 (also tracked as Zirconium and Judgment Panda), previously linked to the Chinese Ministry of State Security (MSS), is known for numerous espionage operations and its involvement in the theft and repurposing of the EpMe NSA exploit years before Shadow Brokers leaked it in April 2017.

Microsoft observed APT31 attacks targeting high-profile individuals associated with Joe Biden's presidential campaign four years ago, while Google spotted them around the same time targeting "campaign staffers' personal email" accounts in phishing attacks.

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned two APT31 operatives (Zhao Guangzong and Ni Gaobin) in March for their work as contractors for Wuhan XRZ, an OFAC-designated front company used by the Chinese MSS attacks against U.S. critical infrastructure.

They were also sanctioned by the United Kingdom for targeting U.K. parliamentarians, breaching the GCHQ intelligence agency, and hacking into the country's Electoral Commission systems.

Additionally, the U.S. Justice Department charged the two APT31 hackers, along with five other defendants, for their involvement in the operations of Wuhan XRZ over at least 14 years.

Now, the U.S. State Department is offering rewards of up to $10 million for information about Wuhan XRZ and APT31 that could assist in locating and/or arresting any of the seven Chinese hackers.

Source: https://www.bleepingcomputer.com/news/security/czechia-blames-china-for-ministry-of-foreign-affairs-cyberattack/