Finland confirms APT31 hackers behind 2021 parliament breach

By Sergiu Gatlan

Published: 2024-03-26 · Archived: 2026-04-05 21:36:32 UTC

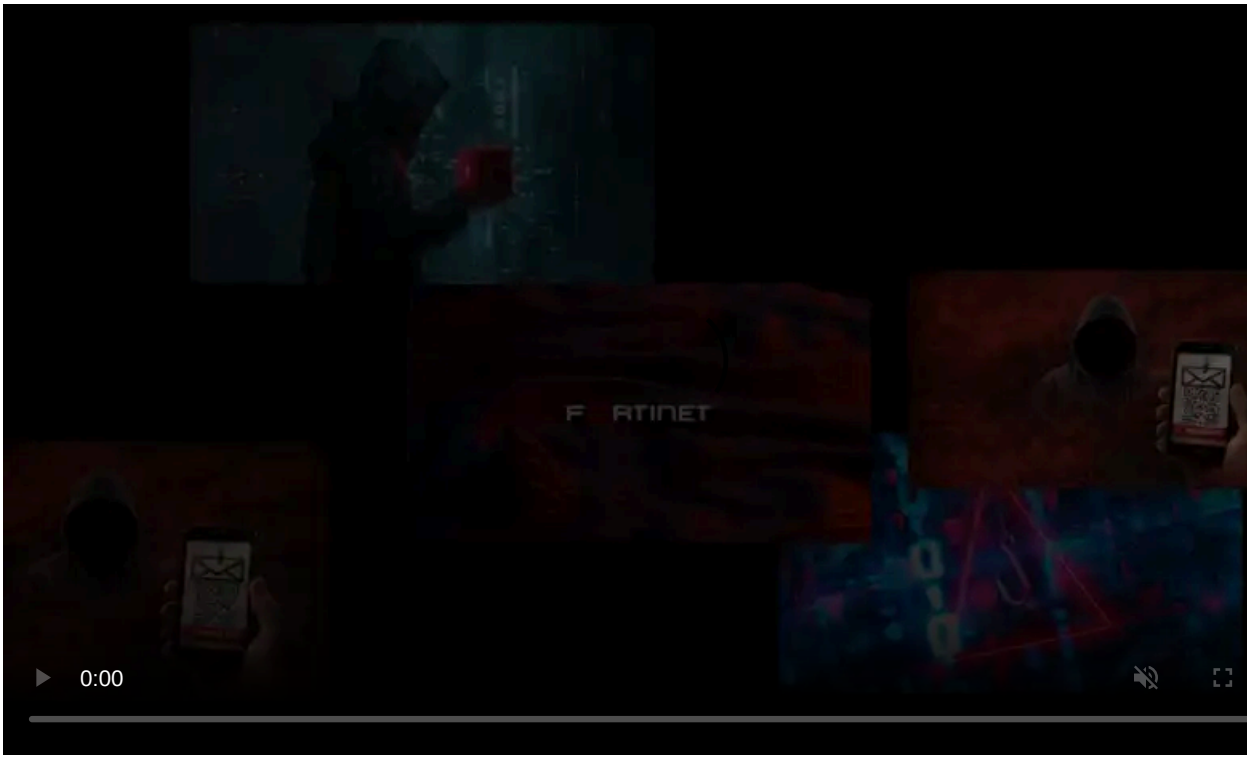
Image: Midjourney

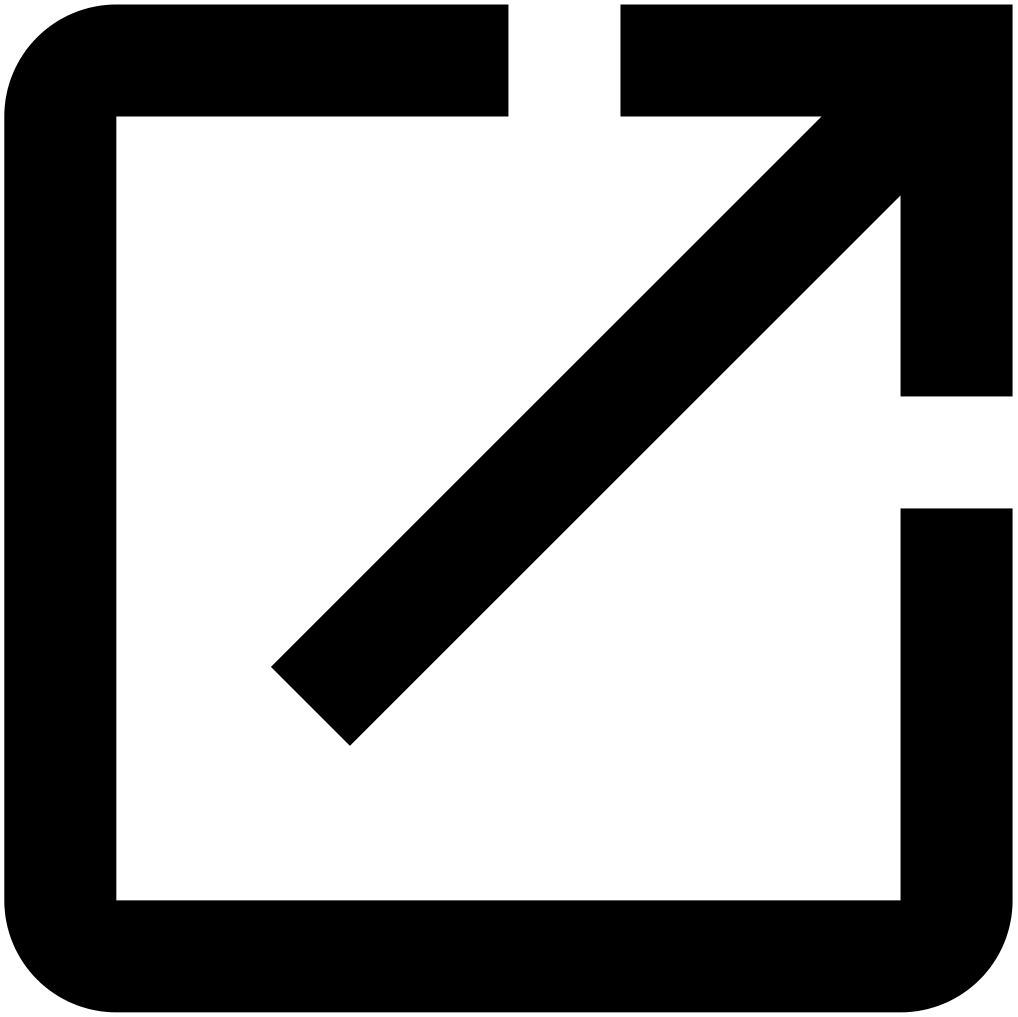
The Finnish Police confirmed on Tuesday that the APT31 hacking group linked to the Chinese Ministry of State Security (MSS) was behind a breach of the country's parliament disclosed in March 2021.

Since then, a joint criminal investigation with the Finnish Security and Intelligence Service and international partners has looked into multiple suspected offenses, including aggravated espionage, violation of communication secrecy, and breaking into the Finnish Parliament's information systems.

This investigation has exposed a "complex criminal infrastructure," according to Detective Chief Inspector Aku Limnéll of the National Bureau of Investigation.

"It is suspected that the offences were committed between autumn 2020 and early 2021. The police have previously informed that they investigate the hacking group APT31's connections with the incident," said the Finnish Police.


F RTINET
0:00



"These connections have now been confirmed by the investigation, and the police have also identified one suspect."

As Finnish Parliament officials said three years ago, when describing the incident as a "state cyber-espionage operation" believed to be linked to "the so-called APT31 operation," the attackers gained access to multiple parliament email accounts, including some belonging to Finnish MPs.

APT31 sanctions and charges

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

The United Kingdom also sanctioned Wuhan XRZ and the two APT31 hackers for breaching the GCHQ intelligence agency, targeting U.K. parliamentarians, and hacking into the country's Electoral Commission systems.

The same day, the U.S. Justice Department charged Zhao Guangzong, Ni Gaobin, and five other defendants (i.e., Weng Ming, Cheng Feng, Peng Yaowen, Sun Xiaohui, Xiong Wang) for their involvement in Wuhan XRZ operations over a span of at least 14 years.

The State Department is now also offering rewards of up to $10 million for information on Wuhan XRZ and APT31 that could help locate and/or apprehend any of the seven Chinese MSS hackers.

In July 2021, the U.S. and its allies, including NATO, the European Union, and the U.K., blamed the Chinese MSS-linked APT40 and APT31 threat groups for an extensive Microsoft Exchange hacking campaign.

APT31 (aka Zirconium and Judgment Panda) is known for numerous information theft and espionage operations and its involvement in the theft and repurposing of the EpMe NSA exploit years before Shadow Brokers leaked it in April 2017.

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

Source: https://www.bleepingcomputer.com/news/security/finland-confirms-apt31-hackers-behind-2021-parliament-breach/