Chinese nation state hackers linked to Finnish Parliament hack

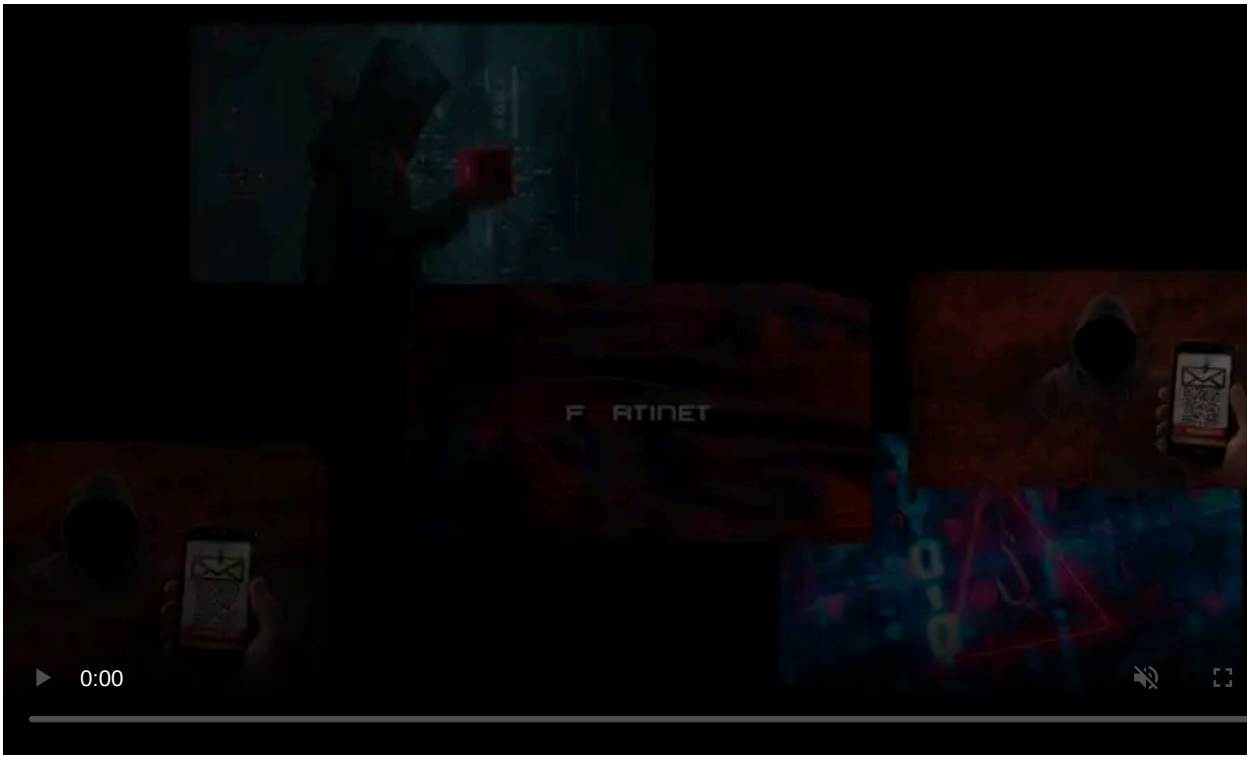
By Sergiu Gatlan

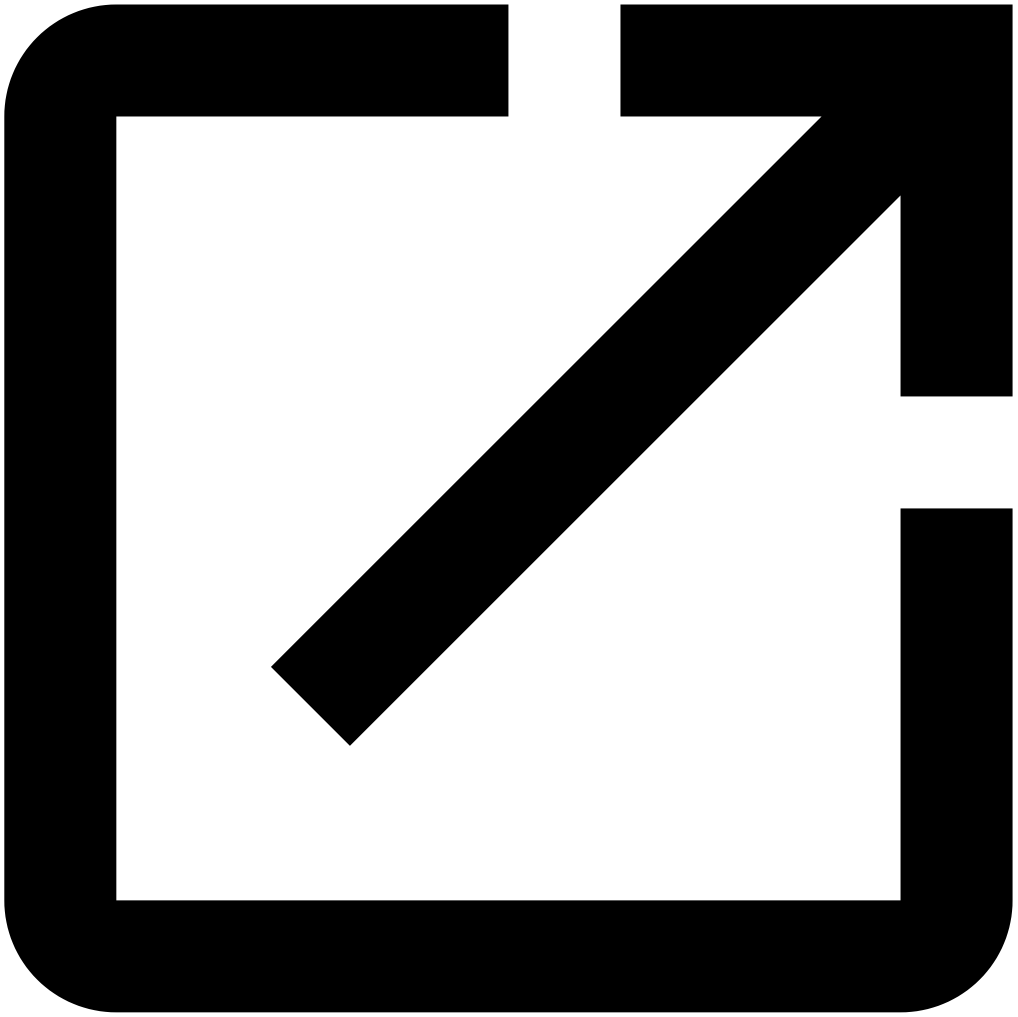
Published: 2021-03-18 · Archived: 2026-04-05 20:21:48 UTC

Chinese nation-state hackers have been linked to an attack on the Parliament of Finland that took place last year and led to the compromise of some parliament email accounts.

"Some parliament e-mail accounts may have been compromised as a result of the attack, among them e-mail accounts that belong to MPs," Parliament officials said at the time.

The attack was detected by the Finnish Parliament's security team and is being investigated by the Finnish National Bureau of Investigation (NBI), with the help of the Security Police and the Central Criminal Police.


F RTINET
0:00



"Last year, the Security Police has identified a state cyber-espionage operation against Parliament, which tried to infiltrate Parliament's information systems," a statement issued today reads. "According to intelligence from the Security Police, this was the so-called APT31 operation."

Central Criminal Police Commissioner Tero Muurman added that further details regarding the attack will not be disclosed while the investigation is still ongoing.

"When the investigated criminal offenses are aggravated espionage, aggravated computer break-in, and aggravated message interception everyone understands how serious offenses we are dealing with," Parliament Speaker Anu Vehviläinen said.

APT31 espionage campaigns

APT31 (also tracked as Zirconium and Judgment Panda) is a China-backed hacking group known for its involvement in numerous information theft and espionage operations, working at the behest of the Chinese Government.

As BleepingComputer previously reported, this APT group has also been linked to the theft and repurposing of the EpMe NSA exploit years before Shadow Brokers publicly leaked it in April 2017.

Last year, Microsoft observed APT31 attacks against international affairs community leaders and high-profile individuals associated with the Joe Biden for President campaign.

APT31 was also spotted by Google while targeting "campaign staffers' personal emails with credential phishing emails and emails containing tracking links."

Norwegian, German Parliaments targeted in similar attacks

In August 2020, Norway disclosed a strikingly similar incident that led to the compromise of several email accounts belonging to Norwegian Parliament representatives and employees.

In October, Norway's Minister of Foreign Affairs Ine Eriksen Søreide revealed that the August attack was coordinated by Russian state hackers who stole data from each of the hacked email accounts.

The Norwegian Police Security Service later revealed that the Russian state-sponsored APT28 hacking group was likely behind the intrusion.

The same month, Council of the European Union announced sanctions against multiple APT28 members for their involvement in the 2015 attack of the German Federal Parliament (Deutscher Bundestag) and the hacking of several parliament members' email accounts.

The US Cyber Command also shared info on malware implants used by Russian hacking groups in attacks targeting several national parliaments, ministries of foreign affairs, and embassies.

Source: https://www.bleepingcomputer.com/news/security/chinese-nation-state-hackers-linked-to-finnish-parliament-hack/