Norway says Chinese group APT31 is behind catastrophic 2018 government hack

By Catalin Cimpanu

Published: 2022-12-16 · Archived: 2026-04-05 17:54:43 UTC

Norway's police secret service said this week that APT31, a cyber-espionage group operating on behalf of China, was responsible for a 2018 breach of the government's IT network.

According to the Norwegian Police Security Service (PST), the 2018 hack was as bad as it could get.

"The investigation revealed that the actor succeeded in acquiring administrator rights that gave it access to centralized computer systems used by all state administration offices in the country," the Norwegian agency said.

"The actor also succeeded in transferring some data from the offices' systems. No reliable technical findings have been made of what information was transferred, but the investigation shows that there were probably usernames and passwords associated with employees in various state administration offices," it added.

The PST said that while the group gained access into the government's network, investigators did not find any evidence that the Chinese hackers exfiltrated state secrets or the personal information of Norwegian citizens.

While in an official press release, the PST did not link the attack to APT31, Hanne Blomberg, the head of counterintelligence at the PST, gave an interview to state television network NRK formally pointing the finger at the Chinese hacking group.

The PST said the same group also hacked Norwegian cloud service provider Visma AG in the summer of 2018.

In a February 2019 report, cyber-security firms Rapid7 and Recorded Future attributed the Visma hack to Chinese hacking group APT10.

On Friday, analysts from Recorded Future's Insikt Group have told *The Record* that subsequent evidence found overlaps between APT10 and RedBravo, Recorded Future's internal name for APT31.

APT31 is also the same group that Finnish officials accused of hacking the internal IT systems of its Parliament in the fall of 2020.

This is the second time in a year that Oslo officials have accused a foreign government of hacking its government network. In December 2020, the PST said that Russia's APT28 hacking group (linked to Russia's military intelligence service) had hacked its Parliament's internal IT network months earlier in September 2020.

In March 2021, the Norwegian Parliament said its network was hacked again after intruders used an unpatched vulnerability to gain access to government systems via a Microsoft Exchange email server. The hack was not attributed to any particular group.

Recorded Future®

Know what matters.

Act first.

Get started

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

Source: https://therecord.media/norway-says-chinese-group-apt31-is-behind-catastrophic-2018-government-hack/