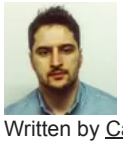
# Norway says Russian hacking group APT28 is behind August 2020 Parliament hack

zdnet.com/article/norway-says-russian-hacking-group-apt28-is-behind-august-2020-parliament-hack/


Home Innovation Security

Russian hackers breached the Norway's Parliament email accounts in August this year.

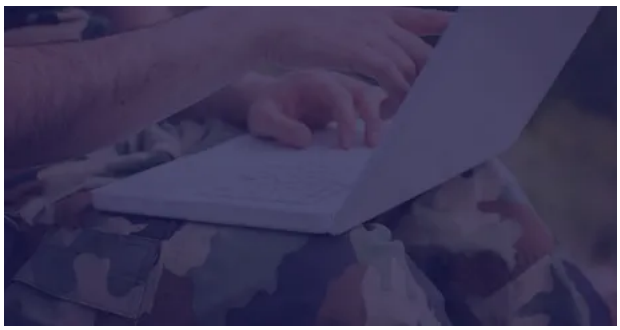


Written by Catalin Cimpanu, Contributor on Dec. 8, 2020

- 
- 
- 
- 
- 


APT28, one of Russia's military hacking units, was most likely responsible for hacking the email accounts of the Norwegian Parliament, the Norwegian police secret service (PST) said today.

## Special feature





The Norwegian Parliament (Stortinget) hack was disclosed earlier this year on September 1. At the time, Stortinget director Marianne said that hackers gained access to the Parliament's email system and accessed inboxes for Stortinget employees and government elected officials.

**SEE: Meet the hackers who earn millions for saving the web, one bug at a time (cover story PDF) (TechRepublic)**

No details about the hack were made public in September, but in a follow-up in October, Foreign Minister Ine Eriksen Søreide said that initial clues suggested that the attack was most likely carried out by Russian hackers, an accusation that Moscow immediately denied.

The next day, Russian Foreign Ministry spokeswoman Maria Zakharova dismissed the allegations as "a planned provocation" from Norwegian officials looking to "destroy bilateral relations" with "no evidence."

Konstantin Kosachev, Head of the Russian Federation Council's Committee on Foreign Affairs, also commented on the matter, calling Oslo's accusations of Russian involvement in the Stortinget hack as "groundless."

## Norwegian secret service publishes its findings

But in a PST press release today, Norway's cyber-security agency held the line with the government's initial October accusations.

"The analysis shows that it is likely that the operation was carried out by a cyber actor referred to in open sources as APT28 and Fancy Bear," PST officials said.

"This actor is linked to Russia's military intelligence service GRU, more specifically their 85th Special Services Center (GTsSS)," they added.

PST officials said APT28 hackers breached Stortinget email accounts and tried to pivot to the Parliament's internal networks but failed.

Investigators said Stortinget was to blame for the intrusion as officials and employees used weak email passwords and failed to use two-factor authentication to protect accounts.

Other details about the intrusions couldn't be revealed due to the sensitive nature of the hack.

PST officials said the attack against its Parliament was part of a larger APT28 campaign that began in 2019 and which targeted multiple other targets, both inside Norway and abroad.

While the PST press release doesn't mention it by name, the Norwegian cyber-security agency appears to be referring to a recent Microsoft report detail a recent shift in APT28 tactics.

According to this report, from September 2019, the APT28 group started using brute-force and credentials harvesting attacks on a larger scale and began targeting Office365 accounts in order to gain access to email accounts of more than 200 private and government organizations.

PST officials said that despite linking the attacks to known APT28 tactics, they weren't able to gather enough evidence to file a formal indictment, as Germany did earlier this year against an APT28 member involved in the hack of its Parliament (the Bundestag) in 2015.

The APT28 group is also known in the cyber-security industry under other names, including Sofacy, Fancy Bear, Sednit, Strontium, and more. It is one of the most active Russian state-sponsored hacking groups, believed to have been involved in hacks against the Pentagon, the German Parliament, NATO, the DNC in 2016, the World Anti-Doping Agency, and many more. The group's members are subject to many indictments and international sanctions.

"Although we have not seen the activity mentioned in [the PST] report, during the last years, we have researched several Sofacy operations targeting entities in Scandinavian countries," Costin Raiu, Director of the Kaspersky Global Research & Analysis Team (GReAT), told *ZDNet*.

"It is important to mention the activities we observed are not recent and date back to 2016-2018," Raiu added.

"Most recently, it would appear that Sofacy changed their TTPs, with a focus on credentials harvesting and then expanding access through cloud services and various network equipment, as opposed to their traditional endpoint infection ops. This makes them much harder to track and detect then before and especially way more difficult to attribute, due to lack of custom software artifacts," the Kaspersky security researcher said.

*Article updated shortly after publication with comments from Kaspersky.*

**The world's most famous and dangerous APT (state-developed) malware**