

Finnish Parliament attackers hack lawmakers' email accounts

By Sergiu Gatlan

Published: 2020-12-28 · Archived: 2026-04-05 15:03:12 UTC

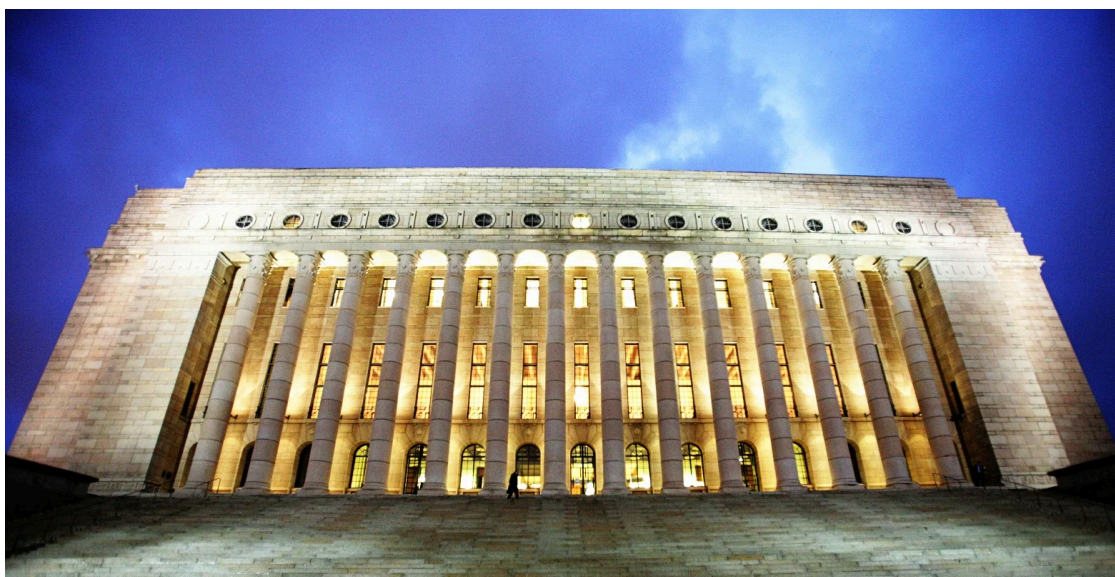


Image: Magnus Fröderberg

The email accounts of multiple members of parliament (MPs) were compromised following a cyberattack as revealed today by the Parliament of Finland.

"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](#).



Visit Advertiser website [GO TO PAGE](#)

The malicious activity was detected by the parliament's security team during the fall of 2020 and it is currently investigated by the National Bureau of Investigation (NBI).

Parliament Speaker Anu Vehviläinen said that this incident is a serious attack on Finnish society and democracy.

"We cannot accept any kind of hostile cyber activity, whether carried out by a governmental or non-governmental body," Vehviläinen [said](#).

"In order to strengthen cybersecurity, we need our own national measures as well as active action at the EU level and in other international cooperation. While the investigation is pending, Parliament will not comment on the matter at this stage."

Potential espionage attempt

Finland's Central Criminal Investigation Department has begun looking into the Finnish Parliament data breach at the end of the autumn and the case is also being investigated as a suspected espionage incident.

"At this stage, an alternative is that unknown threat actors behind the data breach have been able to obtain information either to benefit a foreign state or to harm Finland," NBI Detective Inspector Tero Muurman said in a [statement](#).

"The intrusion has been directed at more than one person, but unfortunately we can not, without jeopardizing the ongoing investigation, tell how many people are involved.

"This incident is exceptional for Finland, serious because of the attack's target and sad for the victims."



Similar attacks against Norwegian and German Parliaments

Another Scandinavian country, Norway, disclosed a strikingly similar incident with attackers compromising [email accounts belonging to Norwegian Parliament](#) representatives and employees in August 2020.

Norway's Minister of Foreign Affairs Ine Eriksen Søreide revealed in October that [Russian state-sponsored hackers were behind the August 2020 cyber-attack](#), stealing data from each of the hacked email accounts.

After concluding the attack investigation, the Norwegian Police Security Service said earlier this month that the [Russian state-sponsored APT28 hacking group was likely behind the attack](#).

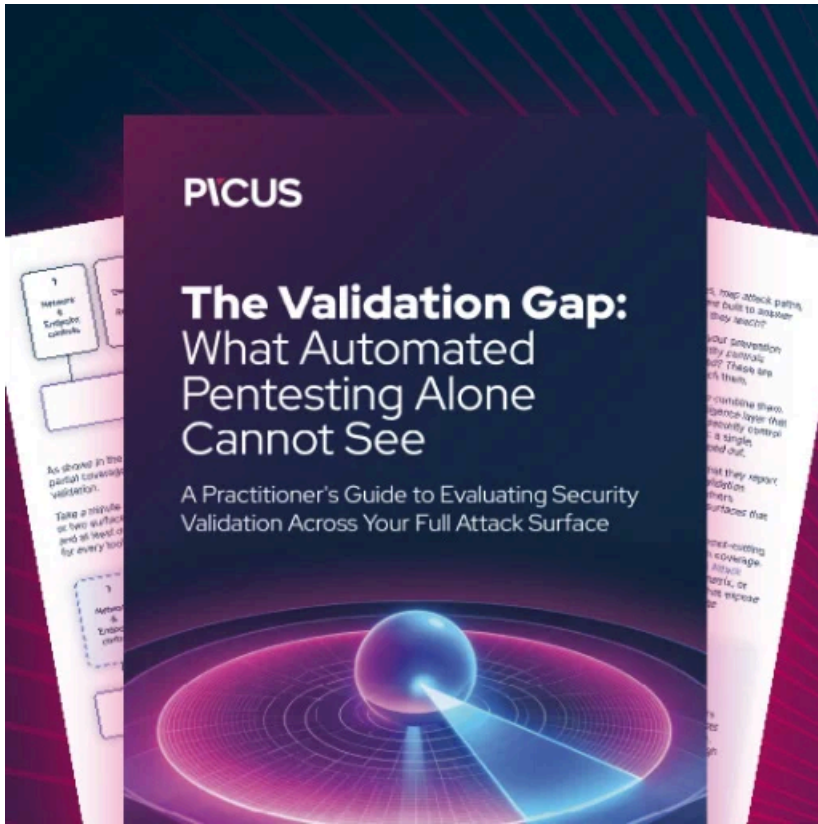
[APT28](#) operators hacked a large number of Stortinget email accounts via brute-force and logged into a limited number of accounts.

Russia officially denied Norway's accusations saying that they aren't based on evidence. "As usual, accusations are posed with no effort made to present any proof or to propose to discuss the incident at an expert level," Konstantin Kosachev, the head of the Russian Federation Council Committee on Foreign Affairs, said in a statement.

In October, the Council of the European Union [announced sanctions against multiple APT28 members](#) for their involvement in the 2015 hack of the German Federal Parliament (Deutscher Bundestag) which also led to the breach of several

parliament members' email accounts.

The same month, the [US Cyber Command shared info on malware implants](#) used by Russian hacking groups in attacks against several national parliaments, ministries of foreign affairs, and embassies.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/finnish-parliament-attackers-hack-lawmakers-email-accounts/>