Russian cyber-espionage group hits Sanoma

Published: 2016-05-30 · Archived: 2026-04-05 19:42:49 UTC

The article is more than 9 years old

Yle has obtained new evidence of cyber-attacks on Finnish targets by a cyber-espionage group linked to Russian state intelligence. The group, known as Sofacy or Pawn Storm, has attempted to hack into data communications of Finland's largest group, Sanoma, as well as of a Finnish member of Bellingcat, an international group investigating the Ukraine conflict.

Sanoma publishes many of Finland's top newspapers and magazines. Image: Jyrki Lyytikkä / Yle

30.5.2016 20:47Updated 30.5.2016 21:02

The Tokyo-based security software firm Trend Micro has found strong evidence that employees of Finland's Sanoma corporation have been targeted by an attempted cyber-attack.

The Russian cyber-espionage group set up a fake server that closely resembled Sanoma's webmail server, Trend Micro’s Senior Threat Researcher, Feike Hacquebord tells Yle.

He says the group registered a web address that differed by just one character from the address of Sanoma's genuine webmail server.

Hacquebord says the attack most likely occurred last August, and that the fake corporate webmail server operated for a few weeks before it was shut down.

Sanoma confirms attempted breach

Sanoma's Chief Technology Officer Kai Taka-Aho has confirmed the information to Yle.

"In late April, we were informed by the National Cyber Security Centre Finland (NCSC-FI) of a cyber-espionage campaign aimed at targets including Sanoma. Other media outlets were also involved," he says.

Sanoma owns several of Finland's largest newspapers including Helsingin Sanomat and Ilta-Sanomat, along with Nelonen Television and an array of other media outlets.

Hacquebord explains that spies use such tactics to gain access to employee emails and to send emails in their names.

Taka-Aho says that Sanoma immediately launched its own probe into whether employees had been subjected to phishing emails, such as requests to change passwords.

"So far we have not found any evidence that the attackers succeeded or that we even received any phony messages. However we cannot completely rule this out, he says.

Shadowy group with many names

Data security firms refer to the cyber-espionage group behind the attacks by various names including Pawn Storm, APT28, Sednit and Sofacy. Hacquebord says the group is part of Russia's state intelligence apparatus. The German intelligence service has confirmed this assessment.

The shadowy organisation has been blamed for cyber-attacks in France, Germany, the US and elsewhere.

Taka-Aho says that Sanoma takes the cyber-espionage attempt seriously.

"Apparently Sanoma is sufficiently large and interesting to make it a target of various players. These kinds of attacks will very likely continue to be made against us and other Finnish companies in the future," he says.

He adds that Sanoma has since replaced its email system with a more secure one – something he says it would have done in any case.

Another target of the same attempted attack was Veli-Pekka Kivimäki, a Finnish member of Bellingcat, an international group of civic journalists investigating the Ukraine conflict. Pawn Storm sought access to his data by sending him a customised phishing email.

Russian cyber-espionage is the focus of the Yle current affairs programme A-studio beginning at 9pm Monday on Yle TV1.
