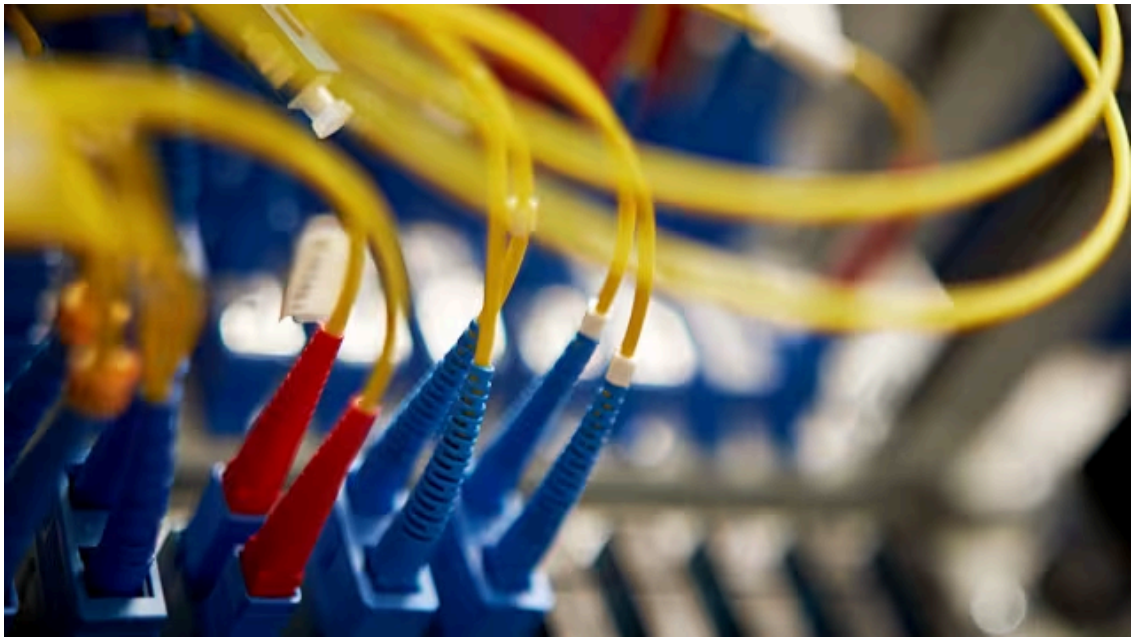
Russian group behind 2013 Foreign Ministry hack

Published: 2016-01-13 · Archived: 2026-04-05 13:29:21 UTC

The article is more than 10 years old

The 2013 data hack at the Finnish Foreign Ministry was perpetrated by a group of Russian hackers, and was part of a wider campaign against targets in nearly fifty countries. Experts contacted by Yle have confirmed that the attack was perpetrated by the Turla group.



Tietoturvayritys arvioi, että Turla on iskenyt yhteensä satoihin kohteisiin lähes viidessäkymmenessä maassa. Image: Jyrki Lyytikkä / Yle

13.1.2016 13:21Updated 14.1.2016 7:58

In 2013 Finland’s Foreign Ministry had its systems hacked by what investigators described as ‘a state actor’. Now Yle's sources have confirmed who was behind the attack: the Turla group of Russian-speaking hackers who perpetrated attacks on targets in more than 50 countries worldwide during the same period.

Stefan Tanase of Kaspersky security says that the Turla group is the premier Russian hacker organization—and it targets ministries, embassies and militaries in Russia’s neighbours.

"We believe that the Turla group is a nation state-sponsored attacker," said Tanase. "We have seen traces in their malware and their servers, which we analyse, that point to the fact that the authors are Russian speaking and they definitely seem to have lot of resources to their cyber-espionage operation."

Yle has confirmed from several European sources that the 2013 attacks on the Foreign Ministry were perpetrated by the Turla group. The Foreign Ministry says that it has investigated the attacks in the light of similar actions targeting other nation states around Russia.

"The typical signs in these attack tools can be observed once you get to the stage where you know what you're looking for and can check to see if there's anything like that, and if there have been any changes in their tools," said Ari Uusikartano of the Foreign Ministry.

Uusikartano says that the attack by Turla hit most countries in western Europe. Kaspersky, which published a report on the methods and targets of Turla (which did not at the time mention Finland) last autumn, has outlined the methods used by the attackers.

First, cyber spies start by gathering information about the target via sources like social media, public websites and internal phone directories.

Second, they choose a few employees to whom they send emails which include a link to an apparently interesting website, which appears to be connected somehow to the targets everyday life or area of specialization. The hackers have however embedded malware in the site concerned.

Third, when the employee visits the site, the malware ends up on his or her computer.

That allows in the attacker, as happened to the Finnish Foreign Ministry in 2013. The ministry says it's learned it's lessons from this attack--but the hackers may already have moved on to a new method.
