Dutch teens arrested for trying to spy on Europol for Russia

Data: 2025-09-27 20:51:24

Autor: Inteligência Against Invaders

Two Dutch teenage boysaged 17, reportedly used hacking devices to spy for Russia,have been

arrested by the Politie on Monday.

According to De Telegraaf, the two used a WiFi sniffer device near Europol and Eurojust offices, as well as the Canadian embassy in The Hague.

BleepingComputer has contacted Europol to confirm the reports, and a spokesperson acknowledged the incident, noting there are no signs of a compromise on the agency's systems.

"We are in close contact with the Dutch authorities regarding this case. Europol has a robust security infrastructure in place, and there is no indication that our systems have been compromised. We take the security of our operations and staff extremely seriously and continue to work closely with our partners to address any potential risks." – Europol spokesperson.

The boys were recruited over Telegram and were arrested following a tip from the country's intelligence service, the General Intelligence and Security Service (AIVD).

De Telegraaf reports that one of the boys was arrested as he was finishing his homework at home, with parents being completely unaware of their son's espionage activities.

"We raise our children to prepare them for dangers in life: smoking, vaping, alcohol, and drugs. But not for something like this. Who would ever consider this a risk?" stated the father of one of thearrested 17-year-old.

Due to the severity of the charges, the twoboys will have to stay in custody for at least two weeks as the investigation continues.

This case marks an escalation to lower-level recruitment cases seen elsewhere in Europe, like in Germany, where youngsters were paid by Russian agents to perform acts of vandalism and sabotage on critical infrastructure.

WiFi sniffers are devices that can identify wireless networks by listening to radio signals on WiFi channels, and intercept traffic. The devices are typically be used in the reconnaissance stage of an attack.

Russian hackers have demonstrated their ability to exploit WiFi networks remotely, as reported by Volexity in a 2024 report.

In that case, APT28 state hackers used the "nearest neighbor attack" to breach aU.S. firm through its

enterprise WiFi network by leveraging a nearby organization within WiFi range.

H/T – @IntCyberDigest

[IMAGEM REMOVIDA]