Dutch teens arrested for spying on behalf of pro-Russian hackers

Data: 2025-09-29 06:00:53

Autor: Inteligência Against Invaders

Dutch teens arrested for spying on behalf of pro-Russian hackers

Dutch police arrested two 17-year-olds for spying for pro-Russian hackers; one jailed, the other placed on home bail.

Dutch police arrested two 17-year-olds suspected of spying for pro-Russian hackers. One of the suspects remains in custody, while the other is released on home bail. According the NL times, the arrests followed a tip from Dutch intelligence (AIVD) Monday.

Dutch prosecutors say two 17-year-olds were recruited via Telegram by pro-Russian hackers to carry a Wi-Fi sniffer near EU buildings in The Hague.

“They were arrested on suspicions that are linked to government-sponsored interference,” prosecution spokesperson Brechtje van de Moosdijk said*.*

One boy’s father confirmed they were allegedly recruited to spy in The Hague near Europol, Eurojust, and embassies using a data-sniffing device. PM Dick Schoof called the activity part of Russia’s hybrid attacks on Europe and warned it was alarming that children were being exploited in such operations.

Two Dutch teens faced an examining judge Thursday, with a closed-door follow-up hearing scheduled in two weeks.

This case is a stark warning about how easily adolescents can be drawn into risky hacking activities, especially through social networks and instant messaging platforms like Telegram. The recruitment of teens to conduct technical espionage near critical EU institutions highlights the growing danger: not only are these children vulnerable to manipulation by state-sponsored actors, but their actions could unintentionally trigger national security incidents or even attacks on critical infrastructure. Protecting young people from such exploitation—and educating them on the real-world consequences of hacking—is now essential.

There is a significant risk that Russia may utilize non-state actors, such as NoName(057)16 and Killnet, to conduct cyber attacks while masking direct state involvement and evading international sanctions. These hacktivist and cybercriminal groups often operate with varying degrees of coordination or tacit approval from Russian intelligence services. By leveraging the proxy actions of such actors, Russia can achieve strategic disruption—especially against Western critical infrastructure or government targets—while maintaining plausible deniability. This approach complicates attribution, reduces political costs, and exploits legal and enforcement gaps in the global response to state-sponsored cyber aggression.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,pro-Russian hackers)