

RUSSIAN INTELLIGENCE HIJACKS SIGNAL ACCOUNTS VIA DEVICE-LINKING PHISHING ACROSS EUROPE

On 4 September 2026 Czechia's cyber agency NÚKIB published an analysis and recommendations. It warned that actors linked to Russia are taking over Signal accounts by tricking users into linking an attacker's device or revealing their PIN, using fake 'support' messages, malicious links and fraudulent group-invitation QR codes. NÚKIB cited cyber incidents connected with the app in Czechia. Its analysis (dated 11 Aug 2026) says such attacks have hit users in Ukraine, Germany, France and the Netherlands, and that the scope is very likely wider. An English version followed on 13 Oct 2026. Earlier, the Dutch AIVD/MIVD (9 Mar 2026) attributed the campaign to Russian state hackers, and the FBI and CISA (March 2026) to actors associated with the Russian Intelligence Services; the FBI/CISA alert reports unauthorised access to thousands of accounts.

UKRAINE EVIDENCE HUB
BEYOND UKRAINE
AS OF 20 OCT 2026

DEGREE OF PROOF

OFFICIAL ATTRIBUTION

A government, a prosecutor, the EU, NATO or a UN body has formally named Russia, its services or its state-backed forces. This is a position of that authority, not a verdict.

WHO ESTABLISHED IT

NÚKIB analysis 'Ruské zpravodajské služby cílí na uživatele aplikace Signal' (č. j. 21670/2026-NÚKIB-E/630, 11 Aug 2026, TLP:CLEAR): the method was one that 'ruské zpravodajské služby pravděpodobně (55–70 %) poprvé nasadily vůči členům ukrajinské armády' ('Russian intelligence services probably (55–70%) first deployed against members of the Ukrainian army'). NÚKIB notice (4 Sep 2026): 'Tyto aktivity jsou spojovány zejména s aktéry napojenými na Ruskou federaci' ('These activities are mainly linked to actors connected to the Russian Federation'). AIVD/MIVD (9 Mar 2026): 'Russian state hackers are engaged in a large-scale global cyber campaign'; 'targets and victims of the campaign include Dutch government employees'. FBI/CISA PSA I-032026-PSA: 'cyber actors associated with the Russian Intelligence Services (RIS)'; 'This global campaign has resulted in unauthorized access to thousands of individual CMA accounts.'

LATEST

The attacks abuse legitimate Signal features; the encryption is not broken. On 13 Oct 2026 NÚKIB re-issued the warning in English, with the analysis translated (ref. 24019/2026-NÚKIB-E/630, 30 Sep 2026). NÚKIB recommends checking linked devices regularly, enabling Registration Lock, never sharing a PIN or codes, and downloading Signal only from signal.org.

LINK TO THE WAR AGAINST UKRAINE

NÚKIB assesses that Russian intelligence services probably (55–70%) first used the technique against members of Ukraine's armed forces before turning it on European targets.

SOURCES

- B** NÚKIB – Ruští aktéři cílí na uživatele Signalu. NÚKIB vydává analýzu a doporučení, jak si aplikaci zabezpečit · 2026-09-04
<https://nukib.gov.cz/cs/infoservis/aktuality/2456-rusti-akteri-cili-na-uzivatele-signalu-nukib-vydava-analyzu-a-doporuceni-jak-si-aplikaci-zabezpecit>
- B** NÚKIB – Zneužití aplikace Signal pro phishing (analysis, TLP:CLEAR) · 2026-08-11
<https://nukib.gov.cz/download/publikace/analyzy/Zneu%C5%BEit%C3%AD%20aplikace%20Signal%20pro%20phishing.pdf>
- B** NÚKIB – Russian Actors Are Targeting Signal Users. NÚKIB Releases an Analysis and Recommendations on How to Secure the App · 2026-10-13
<https://nukib.gov.cz/en/infoservis-en/news/2465-russian-actors-are-targeting-signal-users-nukib-releases-an-analysis-and-recommendations-on-how-to-secure-the-app>
- B** NÚKIB – Misuse of the Signal app for phishing (English analysis) · 2026-09-30
https://nukib.gov.cz/download/publications_en/Misuse-of-the-Signal-app-for-phishing_ENG.pdf
- B** AIVD – Russia targets Signal and WhatsApp accounts in cyber campaign · 2026-03-09
<https://english.aivd.nl/latest/news/2026/03/09/russia-targets-signal-and-whatsapp-accounts-in-cyber-campaign>
- B** FBI IC3 / CISA – Russian Intelligence Services Target Commercial Messaging Application Accounts (I-032026-PSA) · 2026-03-20
<https://ic3.gov/PSA/2026/PSA260320>

WHAT WE ASK OF MEMBER STATES

- Attribute jointly and raise it in the UN Open-ended Working Group on ICT security.
- Use the EU cyber sanctions regime against the units responsible.
- Share indicators and support the resilience of critical infrastructure.

