

LA INTELIGENCIA RUSA SECUESTRA CUENTAS DE SIGNAL EN EUROPA MEDIANTE PHISHING DE VINCULACIÓN DE DISPOSITIVOS

El 4 de septiembre de 2026, la agencia checa de ciberseguridad NÚKIB publicó un análisis y recomendaciones. Advirtió de que actores vinculados a Rusia se están apoderando de cuentas de Signal engañando a los usuarios para que vinculen el dispositivo de un atacante o revelen su PIN, mediante falsos mensajes de «soporte», enlaces maliciosos y códigos QR fraudulentos de invitación a grupos. NÚKIB mencionó ciberincidentes relacionados con la aplicación en Chequia. Su análisis (de fecha 11 de agosto de 2026) señala que estos ataques han afectado a usuarios en Ucrania, Alemania, Francia y los Países Bajos y que su alcance es muy probablemente mayor. El 13 oct 2026 se publicó una versión en inglés. Anteriormente, los servicios neerlandeses AIVD/MIVD (9 de marzo de 2026) habían atribuido la campaña a piratas informáticos del Estado ruso, y el FBI y la CISA (marzo de 2026), a actores asociados a los servicios de inteligencia rusos; la alerta del FBI y la CISA informa del acceso no autorizado a miles de cuentas.

UKRAINE EVIDENCE HUB
MÁS ALLÁ DE UCRANIA
A 20 OCT 2026

GRADO DE PRUEBA

ATRIBUCIÓN OFICIAL

Un Gobierno, una fiscalía, la UE, la OTAN o un órgano de las Naciones Unidas ha señalado formalmente a Rusia, a sus servicios o a sus fuerzas respaldadas por el Estado. Se trata de una posición de esa autoridad, no de una sentencia.

QUIÉN LO ESTABLECIÓ

Análisis de NÚKIB «Ruské zpravodajské služby cílí na uživatele aplikace Signal» (č. j. 21670/2026-NÚKIB-E/630, 11 ago 2026, TLP:CLEAR): el método era uno que «ruské zpravodajské služby pravděpodobně (55–70 %) poprvé nasadily vůči členům ukrajinské armády» («los servicios de inteligencia rusos probablemente (55–70 %) emplearon por primera vez contra miembros del ejército ucraniano»). Aviso de NÚKIB (4 sept 2026): «Tyto aktivity jsou spojovány zejména s aktéry napojenými na Ruskou federaci» («Estas actividades se vinculan principalmente con actores conectados con la Federación de Rusia»). AIVD/MIVD (9 mar 2026): «Piratas informáticos del Estado ruso llevan a cabo una campaña cibernética mundial a gran escala»; «entre los objetivos y víctimas de la campaña figuran empleados del Gobierno neerlandés». Aviso al público del FBI/CISA I-032026-PSA: «ciberactores asociados a los servicios de inteligencia rusos (RIS)»; «Esta campaña mundial ha dado lugar a un acceso no autorizado a miles de cuentas CMA individuales».

LO MÁS RECIENTE

Los ataques abusan de funciones legítimas de Signal; el cifrado no se ha vulnerado. El 13 oct 2026, NÚKIB volvió a publicar la advertencia en inglés, con la traducción del análisis (ref. 24019/2026-NÚKIB-E/630, 30 sept 2026). NÚKIB recomienda revisar periódicamente los dispositivos vinculados, activar el bloqueo de registro, no compartir nunca PIN ni códigos y descargar Signal únicamente desde signal.org.

VÍNCULO CON LA GUERRA CONTRA UCRANIA

Según NÚKIB, los servicios de inteligencia rusos probablemente (55–70 %) utilizaron la técnica por primera vez contra miembros de las fuerzas armadas de Ucrania antes de dirigirla contra objetivos europeos.

FUENTES

- 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>

QUÉ PEDIMOS A LOS ESTADOS MIEMBROS

- Atribuir conjuntamente y plantearlo en el Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre seguridad de las TIC.
- Aplicar el régimen de sanciones cibernéticas de la UE a las unidades responsables.
- Compartir indicadores y apoyar la resiliencia de las infraestructuras críticas.

