

LE RENSEIGNEMENT RUSSE DÉTOURNE DES COMPTES SIGNAL EN EUROPE PAR HAMEÇONNAGE À L'ASSOCIATION D'APPAREILS

Le 4 septembre 2026, l'agence tchèque de cybersécurité NÚKIB a publié une analyse et des recommandations. Elle a averti que des acteurs liés à la Russie prennent le contrôle de comptes Signal en incitant les utilisateurs à associer l'appareil d'un attaquant ou à révéler leur code PIN, au moyen de faux messages du « support », de liens malveillants et de codes QR frauduleux d'invitation à des groupes. NÚKIB a fait état de cyberincidents liés à l'application en Tchéquie. Son analyse (datée du 11 août 2026) indique que ces attaques ont touché des utilisateurs en Ukraine, en Allemagne, en France et aux Pays-Bas et que leur portée est très probablement plus large. Une version anglaise a suivi le 13 oct. 2026. Auparavant, les services néerlandais AIVD/MIVD (9 mars 2026) avaient attribué la campagne à des pirates informatiques de l'État russe, et le FBI et la CISA (mars 2026) à des acteurs associés aux services de renseignement russes ; l'alerte du FBI et de la CISA fait état d'un accès non autorisé à des milliers de comptes.

UKRAINE EVIDENCE HUB
AU-DELÀ DE L'UKRAINE
AU 20 OCT. 2026

DEGRÉ DE PREUVE

ATTRIBUTION OFFICIELLE

Un gouvernement, un procureur, l'UE, l'OTAN ou un organe de l'ONU a formellement désigné la Russie, ses services ou ses forces soutenues par l'État. Il s'agit d'une position de cette autorité, non d'un jugement.

QUI L'A ÉTABLI

Analyse de NÚKIB « Ruské zpravodajské služby cílí na uživatele aplikace Signal » (č. j. 21670/2026-NÚKIB-E/630, 11 août 2026, TLP:CLEAR) : la méthode serait celle que « ruské zpravodajské služby pravděpodobně (55–70 %) poprvé nasadily vůči členům ukrajinské armády » (« les services de renseignement russes ont probablement (55–70 %) déployée pour la première fois contre des membres de l'armée ukrainienne »). Avis de NÚKIB (4 sept. 2026) : « Tyto aktivity jsou spojovány zejména s aktéry napojenými na Ruskou federaci » (« Ces activités sont principalement liées à des acteurs rattachés à la Fédération de Russie »). AIVD/MIVD (9 mars 2026) : « Des pirates informatiques de l'État russe mènent une cybercampagne mondiale de grande ampleur » ; « parmi les cibles et les victimes de la campagne figurent des agents de l'administration néerlandaise ». Avis au public du FBI/de la CISA I-032026-PSA : « cyberacteurs associés aux services de renseignement russes (RIS) » ; « Cette campagne mondiale a permis un accès non autorisé à des milliers de comptes CMA individuels. »

DERNIÈRES NOUVELLES

Les attaques détournent des fonctionnalités légitimes de Signal ; le chiffrement n'est pas compromis. Le 13 oct. 2026, NÚKIB a publié de nouveau l'avertissement en anglais, accompagné de la traduction de l'analyse (réf. 24019/2026-NÚKIB-E/630, 30 sept. 2026). NÚKIB recommande de vérifier régulièrement les appareils associés, d'activer le verrouillage de l'enregistrement, de ne jamais communiquer de code PIN ou de code de vérification et de ne télécharger Signal que sur signal.org.

LIEN AVEC LA GUERRE CONTRE L'UKRAINE

Selon NÚKIB, les services de renseignement russes ont probablement (55–70 %) utilisé la technique d'abord contre des membres des forces armées ukrainiennes avant de la retourner contre des cibles européennes.

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>

CE QUE NOUS DEMANDONS DES ÉTATS MEMBRES

- Attribuer conjointement et porter la question devant le Groupe de travail à composition non limitée des Nations Unies sur la sécurité du numérique.
- Appliquer le régime de sanctions cyber de l'UE aux unités responsables.
- Partager les indicateurs et renforcer la résilience des infrastructures critiques.

