

РОССИЙСКАЯ РАЗВЕДКА ЗАХВАТЫВАЕТ АККАУНТЫ SIGNAL ЧЕРЕЗ ФИШИНГ С ПРИВЯЗКОЙ УСТРОЙСТВ ПО ВСЕЙ ЕВРОПЕ

4 сентября 2026 года агентство кибербезопасности Чехии NÚKIB опубликовало аналитический материал и рекомендации. Агентство предупредило, что связанные с Россией субъекты захватывают аккаунты Signal, обманом вынуждая пользователей привязать устройство злоумышленника или раскрыть свой PIN-код, с помощью поддельных сообщений «службы поддержки», вредоносных ссылок и мошеннических QR-кодов с приглашениями в группы. NÚKIB сослалось на киберинциденты, связанные с этим приложением, в Чехии. В его аналитическом материале (от 11 авг. 2026) говорится, что такие атаки затронули пользователей в Украине, Германии, Франции и Нидерландах и что их масштаб весьма вероятно шире. Английская версия была опубликована 13 окт. 2026. Ранее нидерландские AIVD/MIVD (9 марта 2026) атрибутировали кампанию российским государственным хакерам, а ФБР и CISA (март 2026) — субъектам, связанным с российскими спецслужбами; в предупреждении ФБР/CISA сообщается о несанкционированном доступе к тысячам аккаунтов.

UKRAINE EVIDENCE HUB
ЗА ПРЕДЕЛАМИ
УКРАИНЫ
ПО СОСТОЯНИЮ НА 20
ОКТ. 2026 Г.

СТЕПЕНЬ ДОКАЗАННОСТИ

ОФИЦИАЛЬНАЯ АТРИБУЦИЯ

Правительство, прокуратура, ЕС, НАТО или орган ООН официально назвали Россию, её спецслужбы или поддерживаемые ею государственные формирования. Это позиция соответствующего органа, а не приговор.

КЕМ УСТАНОВЛЕНО

Аналитический материал NÚKIB «Ruské zpravodajské služby cílí na uživatele aplikace Signal» (č. j. 21670/2026-NÚKIB-E/630, 11 авг. 2026, TLP:CLEAR): речь идёт о методе, который «ruské zpravodajské služby pravděpodobně (55–70 %) poprvé nasadily vůči členům ukrajinské armády» («российские спецслужбы, вероятно (55–70 %), впервые применили против военнослужащих украинской армии»). Уведомление NÚKIB (4 сент. 2026): «Tyto aktivity jsou spojovány zejména s aktéry napojenými na Ruskou federaci» («Эта деятельность связывается прежде всего с субъектами, связанными с Российской Федерацией»). AIVD/MIVD (9 марта 2026): «российские государственные хакеры ведут масштабную глобальную киберкампанию»; «в число целей и жертв кампании входят служащие правительства Нидерландов». ФБР/CISA, PSA I-032026-PSA: «киберсубъекты, связанные с российскими спецслужбами (RIS)»; «Эта глобальная кампания привела к несанкционированному доступу к тысячам индивидуальных аккаунтов CMA».

ПОСЛЕДНЕЕ

Атаки используют легитимные функции Signal; шифрование не взломано. 13 окт. 2026 NÚKIB повторно опубликовало предупреждение на английском языке вместе с переводом аналитического материала (исх. 24019/2026-NÚKIB-E/630, 30 сент. 2026). NÚKIB рекомендует регулярно проверять привязанные устройства, включить блокировку регистрации (Registration Lock), никогда не сообщать PIN-коды и коды подтверждения и загружать Signal только с signal.org.

СВЯЗЬ С ВОЙНОЙ ПРОТИВ УКРАИНЫ

По оценке NÚKIB, российские спецслужбы, вероятно (55–70 %), впервые применили этот метод против военнослужащих Вооружённых сил Украины, прежде чем обратить его против европейских целей.

ИСТОЧНИКИ

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%B8it%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>

С КАКИМ ПРИЗЫВОМ МЫ ОБРАЩАЕМСЯ

К ГОСУДАРСТВАМ-ЧЛЕНАМ

- Совместно атрибутировать и поднять вопрос в Рабочей группе открытого состава ООН по безопасности ИКТ.
- Применить режим киберсанкций ЕС к ответственным подразделениям.
- Обмениваться индикаторами и укреплять устойчивость критической инфраструктуры.

