



**TLP: CLEAR**

**Szabadon terjeszthető!**

## Tájékoztató üzenetküldő alkalmazások elleni támadásokról (2025. február 25.)

Tisztelt Ügyfelünk!

**A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet tájékoztatót ad ki az orosz eredetű kiberbűnözői csoportokhoz köthető destruktív, üzenetküldő alkalmazásokat célzó támadásokkal kapcsolatban.**

A Google Threat Intelligence Group (GTIG) 2025. február 19-én kiadott [jelentése](#) szerint megnövekedett a Signal felhasználói fiókok megszerzésére irányuló kampányok száma az Oroszországhoz köthető kiberbűnözői csoportok körében.

Az utóbbi időben egy olyan támadási módszer terjedt el, amely a **Signal üzenetküldő alkalmazás eszköztársító („Linked Devices”) funkcióját használja ki**. A támadók jellemzően egy kártékony **QR-kódot juttatnak el az áldozatokhoz**, megtévesztő szöveges üzenet kíséretében. Amennyiben az érintett beolvassa a QR-kódot, **a támadók eszköze automatikusan társításra kerül az áldozat Signal-fiókjához**, ezáltal teljes hozzáférést szerezve az üzenetváltásokhoz, amelyek tartalmát akadálytalanul megfigyelhetik.

A módszer különösen kockázatos, mivel a támadók célzott kampányokat alkalmaznak, amelyek során a megtévesztő üzeneteket úgy állítják össze, hogy azok hitelesnek tűnjenek a célcsoport számára. Egyes esetekben **a fertőzött linket tartalmazó QR-kódot egy Signal-csoport meghívójának álcázva küldik el**, ezzel növelve az áldozatok megtévesztésének valószínűségét. Továbbá előfordult, hogy a csalók egy **eredeti Signal-csoport meghívó linkjét módosították** oly módon, hogy a manipulált hivatkozás egy kártékony URL-re irányítsa a felhasználót, amely létrehozta a **kapcsolatot a támadók eszköze és az érintett fiókja között**.

Az **ukrán CSIRT** egy, a Signalos esethez hasonló kampányt [figyelt meg](#), amelyben a támadók a **WhatsApp** alkalmazás felhasználói fiókjaihoz fértek hozzá. A GTIG jelentése szintén azt hangsúlyozza, hogy nem csak a Signal áll az orosz hackercsoportok fókuszában. Például az elmúlt hónapokban zajló „Coldriver” elnevezésű kampány célpontjai magas beosztású, WhatsAppot használó diplomaták voltak.

Nemzetbiztonsági Szakszolgálat  
Nemzeti Kibervédelmi Intézet  
Telefon: +36-1-336-4833  
Incidentsbejelentés: [csirt@nki.gov.hu](mailto:csirt@nki.gov.hu)

**TLP: CLEAR**