



NEMZETI
KIBERBIZTONSÁGI
INTÉZET

CÉLKERESZTBEN AZ ÜZENETKÜLDŐ ALKALMAZÁSOK

ÓVATOSAN A MEGHÍVÓKKAL!



Az utóbbi időben Intézetünkhöz több megkeresés is érkezett üzenetküldő alkalmazások ellen irányuló, **felhasználói fiókok megszerzését célzó** támadásokkal kapcsolatban. A kampány célpontjai **magas beosztású állami és gazdasági szereplők, vezetők**.

A támadások során QR kódok kerülnek kiküldésre, amelyeket signal csoportokhoz történő meghívónak álcáznak, és amelyek beolvasásával a támadók átvehetik az irányítást az áldozatok fiókjai felett. A kampányban **más üzenetküldő alkalmazások**, például a **WhatsApp** is érintett.

A TÁMADÁS MENETE

A támadók általában egy káros QR-kódot tartalmazó megtévesztő üzenetet küldenek áldozataiknak. Amennyiben az áldozat beolvassa a QR-kódot, a **Signal alkalmazás eszköztársító funkcióját** (*“Linked Devices”*) kihasználva, a támadók képesek lesznek hozzáférni az áldozatok beszélgetéseihez azáltal, hogy **a felhasználói fiókhoz a támadók eszköze is társításra kerül.**

Jellemzően egy adott felhasználói kört megszólító **Signal csoport meghívójának álcázzák** az üzeneteket, de olyan esetről is beszámoltak, amelyben az elkövetők egy **valós Signal csoport meghívó linkjét írták át** úgy, hogy az egy **kártékony URL-re** irányítson és létrehozza a kapcsolódást az elkövetők eszköze és az áldozat fiókja között. Mivel a támadást magát nehéz észlelni, az elkövetők sokáig észrevétlenek maradnak a céleszközökön.

Más üzenetküldő alkalmazások is érintettek a támadási sorozatban, például az elmúlt hónapokban zajló *„Coldriver”* elnevezésű kampány során **WhatsApp** alkalmazást használó diplomatákat vettek célba az elkövetők.

Az ilyen és ehhez hasonló támadások elkerülése érdekében javasolt az alábbiak betartása:

- **Soha ne olvassunk be ismeretlen forrásból származó QR-kódokat!**
- Alkalmazzunk hosszú, és összetett feloldó kódokat!
- **Rendszeresen ellenőrizzük a társított eszközök listáját!** Amennyiben ismeretlen eszközt észlelünk a listában, mielőbb töröljük!
- Üzenetküldő alkalmazásainkat is tartsuk naprakészen!
- Ahol csak módunkban áll, alkalmazzunk kétlépcsős azonosítást!

VÉDELMI JAVASLATOK

