Priedas

ANTRASIS OPERATYVINIŲ TARNYBŲ DEPARTAMENTAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

VSD PATRIA ET VERITAS

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

SAUGUS SIGNAL IR KITŲ KOMUNIKACIJOS KANALŲ (PROGRAMĖLIŲ) NAUDOJIMAS: REKOMENDACIJOS

Augant naudotojų poreikiams keistis informacija greitai ir taip, kad būtų užtikrintas didesnis komunikacijų saugumas, privatumas ir turinio konfidencialumas, sparčiai auga šiuos poreikius užtikrinančių komercinių bendravimo platformų (programėlių) naudojimas.

Signal – nuo 70 iki 100 mln. aktyvių naudotojų turinti, patikimumu ir nepriklausomumu pasižyminti komunikacijos platforma, naudojanti ištisinį (angl. *end-to-end*) šifravimą, kuriame tik žinutės siuntėjas ir gavėjas gali ją perskaityti. Dėl šio funkcionalumo *Signal* yra tapusi populiaria priemone tarp institucijų ir privačių naudotojų, norinčių apsaugoti vidinę komunikaciją. Nepaisant patikimo šifravimo, tokie komunikacijos kanalai (programėlės) kaip *Signal* negali būti naudojami įslaptintai informacijai tvarkyti ir perduoti.

Dėl platformos populiarumo ir ja perduodamo turinio, apimančio jautrius duomenis ar tarnybinę informaciją, *Signal* yra tapusi patraukliu taikiniu kibernetiniams piktavaliams. Vėliausiai nuo 2025 m. tuo ypač siekia pasinaudoti Rusijos žvalgybos ir saugumo tarnybos (ŽST) bei jų remiamos kibernetinės grupuotės, piktavaliai.

Siekiama gauti prieigą prie *Signal* paskyrų, priklausančių aukšto rango pareigūnams, kariams ir valstybės tarnautojams Lietuvoje, kitose Vakarų valstybėse ir Ukrainoje. Gauti prieigą gali būti siekiama ir kitų, Rusijos ŽST dominančių, asmenų, pavyzdžiui, žurnalistų, visuomenininkų ar karinės pramonės atstovų. Beveik tikra, kad su Rusijos ŽST siejami piktavaliai yra įgiję prieigą prie neskelbtinos jautrios informacijos, kuria disponavo juos dominantys asmenys, įskaitant ir asmenis iš Lietuvos.

Iki šiol nėra aptikta *Signal* programėlės techninių pažeidžiamumų, kuriuos būtų galima išnaudoti, todėl vykdoma kibernetine kampanija siekiama piktavališkai išnaudoti standartinį programėlės funkcionalumą, t. y. kompromituojama ne pati programėlė, o jos naudotojų paskyros.

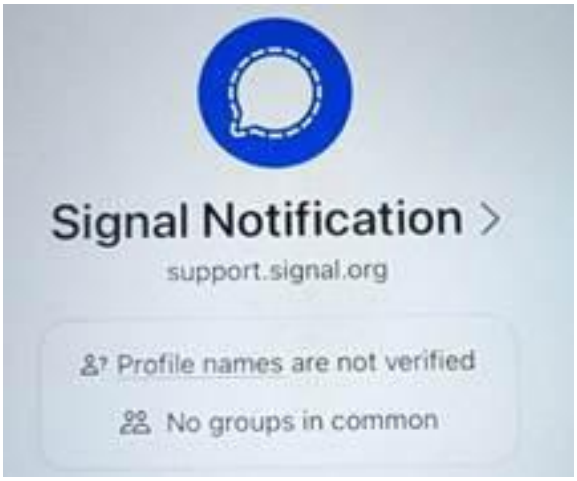
Grėsmė saugioms pranešimų programėlėms neapsiriboja vien tik nuotolinėmis kibernetinėmis operacijomis, bet apima ir fizinės prieigos operacijas, kai piktavalis gali trumpam pasiekti neužrakintą taikinio įrenginį, kuriame tos programėlės įdiegtos.

Svarbu pažymėti, kad tokios pat grėsmės kyla ne tik *Signal*, bet ir kitoms plačiai naudojamoms komunikacijų platformoms, pavyzdžiui, *WhatsApp* ir *Telegram*. Jų naudotojai taip pat yra kibernetinių piktavalių, įskaitant ir priešiškų šalių ŽST, taikiniai.

Signal paskyrų užvaldymo procesas

Piktavaliai, norėdami gauti prieigą prie *Signal* programėlės naudotojų paskyrų, siekia įtikinti naudotojus atskleisti savo saugumo patvirtinimo ir el. pašto kodus. Dažniausiai tai daroma trimis būdais.

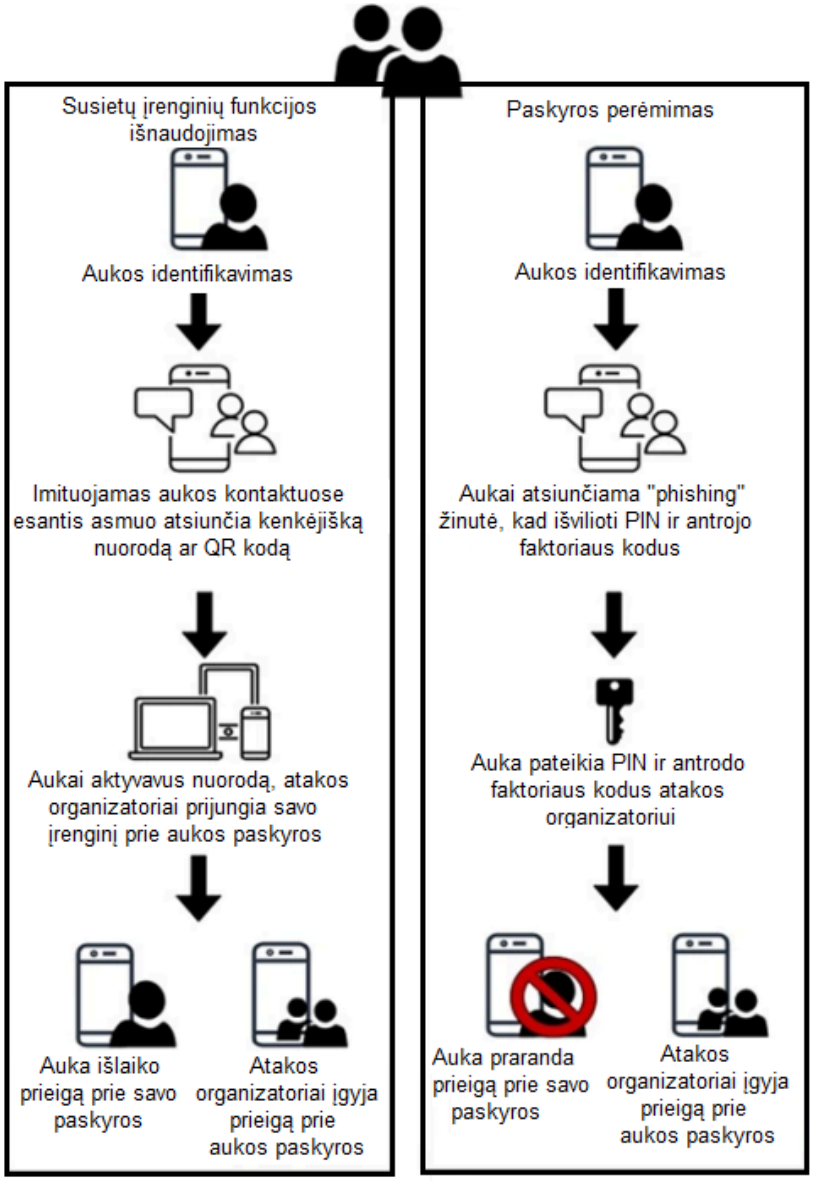
Pirma, apsimetama *Signal* pokalbių robotu (anlg. *Signal Support* arba *Signal Notification*) (1 paveikslas). Dažniausiai auką bandoma paveikti pranešant apie nutekėjusius prisijungimo duomenis ar kitą įtartiną veiklą. Vėliau, pasinaudojant įgytais kodais, perimama naudotojo paskyra (2 paveikslas). Siekiant įtikinti Rusijos ŽST dominantį asmenį, žinutėse gali būti panaudota aktuali, su juo susijusi informacija apie faktines tarnybos, išvykų, šeimines ar kitas asmeniui svarbias aplinkybes. Šiuo atveju svarbu atminti, kad *Signal* niekada nesusisiekia su programėlės naudotojais žinutėmis ir neprašo žinute pateikti PIN ar SMS gaunamų autentifikavimo kodų.



1 paveikslas (viršuje). *Apsimetėlių naudojama paskyra*

2 paveikslas (dešinėje). Apsimetėlių susirašinėjimas su auka

Antras Rusijos piktavalių naudojamas būdas – susietų įrenginių funkcijos išnaudojimas *Signal* programėlėje, kai tos pačios paskyros naudojimas įgalinamas iš skirtingų įrenginių (pvz., planšetinio ar stacionaraus kompiuterio). Sėkmingai kompromitavus paskyrą, įsilaužėliai gali skaityti gaunamus pranešimus, įskaitant pranešimus aukos pokalbių grupėse. Schema (žr. 3 paveikslą) iliustruoja, kaip veikiama abiem būdais.



3 paveikslas. *Atakos organizatorių naudojamų metodų schema*
Šaltinis: *https://www.ic3.gov/PSA/2026/PSA260320*

Trečiuoju būdu kibernetiniai piktavaliai per *Signal* programėlę vykdo tikslinės „gaudyklės“ kibernetines atakas ir siekia perimti paskyros kontrolę. Atakų vykdytojai siekia socialinės inžinerijos principais paveikti taikinius, apsimeta kitais asmenimis, pavyzdžiui, kitų valstybių aukšto rango politikais ar pareigūnais, ir, išnaudodami aktualią arba intriguojančią tematiką, siunčia pasirinktiems adresatams privačias žinutes. Jose gali būti įterpiamos ir kenksmingos nuorodos, kuriose gali būti prašoma įvesti prisijungimo duomenis.

Saugumo rekomendacijos

Bendrosios rekomendacijos

- Visuose mobiliuosiuose įrenginiuose įjunkite ekrano užraktą. Užraktui pasirinkite ilgą (ne trumpesnį nei 15 simbolių), sudėtingą slaptažodį su didžiosiomis bei mažosiomis raidėmis, skaičiais ir simboliais. *Android* įrenginiai palaiko raidinius ir skaitmeninius slaptažodžius, kurie suteikia daugiau saugumo nei tik skaitmeniniai PIN kodai ar

šablonai. Papildomai naudokite biometrinių duomenų apsaugos sprendimus (angl. *Face ID*, *Face Recognition*).
- Bet kokioms el. paslaugoms, esant galimybei, įjunkite dviejų faktorių saugumo nustatymus (MFA), pvz., pirštų atspaudus, veido atpažinimą, saugos raktą ar vienkartinį kodą.
- Įdiekite įrenginio operacinės sistemos atnaujinimus, kai tik jie tampa prieinami, ir visada naudokite naujausias *Signal* bei kitų komunikacijos kanalų programėlių versijas.
- Įsitikinkite, kad *Android* įrenginiuose įjungta *Google Play Protect* funkcija. Ji tikrina jūsų programas ir įrenginius, ar juose nevykdoma kenkėjiška veikla, ir gali įspėti arba blokuoti programas, kurios ją vykdo, net jei šios programos yra iš šaltinių, esančių ne iš *Google Play*.
- Reguliariai tikrinkite *Signal* ir kitų komunikacijos kanalų programėlių susietus įrenginius, siekdami įsitikinti, ar nėra neteisėtai susietų įrenginių. Tai atlikti galima programėlės nustatymuose pasirenkant skyrių *Susieti įrenginiai* (angl. *Linked Devices*).
- Kritiškai vertinkite nepažįstamų ar naujai prie jūsų *Signal* kontaktų prašančių prisijungti asmenų žinutes ir nespauskite jums siunčiamų nežinomų nuorodų.
- Visada būkite atsargūs naudodami QR kodus ir žiniatinklio išteklius, kurie yra tariamai programinės įrangos atnaujinimai, grupių kvietimai ar kiti pranešimai, net jei jie atrodo teisėti ir ragina nedelsiant imtis veiksmų. Pasitikrinkite informacijos tikrumą kitais komunikacijos kanalais (el. paštu, skambučiu telefonu). QR kodus su *Signa*l ar *WhatsApp* programėle nuskaitykite tik tada, kai patys siejate naują įrenginį su savo paskyra.
- *iOS* naudotojai, siekdami sumažinti kibernetinio saugumo grėsmių galimą poveikį, gali įsijungti *Lockdown* režimą, kuris dėl saugumo gali apriboti tam tikrų įrenginio funkcijų veikimą.
- Įjunkite automatinio žinučių išnykimo (angl. *disappearing messages*) funkciją pokalbiuose, kuriuose gali būti pateikta svarbi informacija ir kurios atskleidimas gali turėti neigiamų pasekmių. Jei jūsų įrenginys ar paskyra būtų pažeisti, ši funkcija sumažintų riziką, kad tretieji asmenys galėtų pasiekti visą susirašinėjimo istoriją

Papildomos rekomendacijos dėl *Signal* nustatymų

Signal pokalbių grupių saugumas

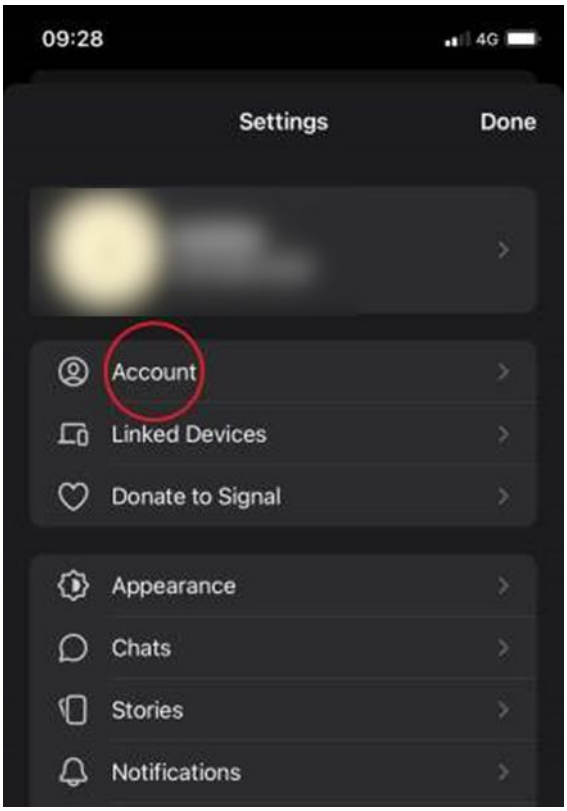
- Pasitikrinkite, ar jūsų grupės pokalbiuose nėra potencialiai „pažeistų“ kontaktų – jei grupės narių sąraše matote asmenų, kurie rodomi daugiau nei kartą (tuo pačiu arba šiek tiek pakeistu vardu), tai gali indikuoti, kad jų paskyros buvo pažeistos ir aukos susikūrė sau naują paskyrą. Kilus įtarimui, patikrinkite, ar atitinkamos paskyros pokalbių grupės kontaktų sąraše esančio asmens paskyra yra tikra. Tai padarykite pasinaudodami kita komunikacijos priemone (pvz., parašykite el. laišką ar paskambinkite). Jei paskyra netikra, paprašykite grupės administratoriaus pašalinti abi paskyras iš grupės pokalbio, o vėliau teisėtą paskyros savininką vėl prijungti prie grupės.
- Būkite budrūs dėl grupės narių, kurių neatpažįsta likusi grupės dalis – kad liktų nepastebėtas pokalbių grupėse, paskyrą perėmęs apsimetėlis gali pakeisti perimtos paskyros rodomą vardą, pvz., į tokį pavadinimą kaip „paskyra pašalinta“ (angl. *account deleted*). Jei grupės nario rodomas vardas pasikeičia, grupė apie tai gaus pranešimą. Kai paskyra iš tikrųjų pašalinama, į grupę pranešimas nesiunčiamas.
- Apsimetėlio kontroliuojamos paskyros gali patekti į grupę ir per gautą grupės nuorodą (angl. *Group Link*). Apie tokį prisijungimą grupė visada gauna pranešimą. Pastebėję

neteisėtus prisijungimo prie pokalbių grupės atvejus, paprašykite grupės administratoriaus pašalinti atitinkamas paskyras iš grupės.

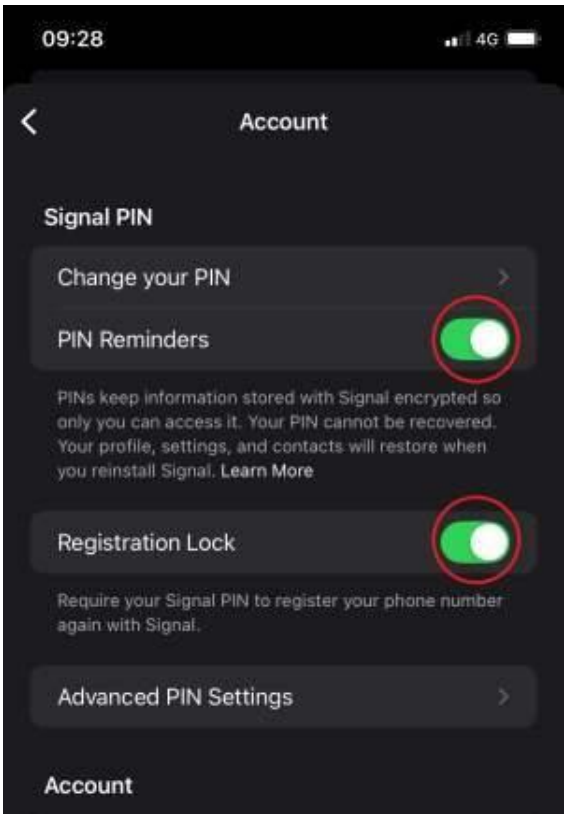
- Jei kompromituota paskyra atlieka ir pokalbių grupės administratoriaus rolę, patartina visiems nariams išeiti iš grupės ir sukurti naują.

Signal profilio saugumas

- Siekdami užtikrinti *Signal* profilio saugumą, įgalinkite programėlės PIN saugumo nustatymus: *Signal* programėlėje spauskite ant savo profilio ikonėlės (viršutiniame kairiajame kampe) ir pasirinkite *Nustatymai* (angl. *Settings*), atsidariusiame meniu spauskite *Paskyra* (angl. *Account*) (žr. 4 paveikslą) ir įsitikinkite, ar yra įgalintas *Registracijos užraktas* (angl. *Registration Lock*) (žr. 5 paveikslą). Šis parametras yra antrasis faktorius registruojant *Signal* profilį kitame telefone. Jei jis neįgalintas – įgalinkite jį. Taip pat papildomai rekomenduojama įgalinti ir *PIN priminimą* (angl. *PIN Reminders*), kuris *Signal* reguliariai prašys suvesti PIN kodą (žr. 5 paveikslą).



4 paveikslas. *Paskyra*



5 paveikslas. *Registracijos užraktas*