



ALERTĂ
08.03.2022

UNCLASSIFIED / NECLASIFICAT

Utilizarea aplicației de mesagerie Signal



În contextul escaladării conflictului militar din **Ucraina**, Directoratului Național de Securitate Cibernetică (DNSC) a primit notificări recente din partea unor autorități cyber competente din Uniunea Europeană, și a unor experți ce ne semnalează faptul că utilizatorii aplicației de mesagerie Signal ar putea întâmpina o serie de amenințări și riscuri de securitate cibernetică.

Acestea pot afecta utilizatori din organizații guvernamentale sau private, factori de decizie, personal tehnic dar și utilizatori obișnuiți.

- **Infiltrarea chat-ului de grup în Signal.** Uneori, utilizatorii platformelor de mesagerie formează grupuri mari de chat pe Signal (colegi de serviciu, familie, prieteni, etc.), unde se vehiculează informații importante și uneori sensibile. Nu toți membrii grupului sunt însă verificați, ceea ce poate permite unor intruși să folosească numele unui membru al grupului, prin impersonare. Infiltrarea poate permite intrușilor să devină membri ai grupului și să urmărească mesajele, comunicarea, și să obțină acces neautorizat la documentele și fișierele transmise.
- **SIM swapping.** Utilizatorii platformelor de mesagerie sunt identificați deseori prin numărul lor de telefon mobil. Un utilizator malițios poate fura identitatea victimei și poate cere furnizorului de telefonie mobilă să emită o nouă cartelă SIM, cu numărul de telefon al victimei. Dacă opțiunea „blocarea înregistrării” nu este activată pe telefonul victimei, un nou telefon mobil poate fi introdus în chat-ul de grup în Signal.
- **Impersonarea.** Actorul malițios poate fura identitatea unei persoane pe care victima o cunoaște și poate cere să devină un contact Signal al acesteia. Aceasta tehnică poate deschide și alte posibilități de acțiune, cum ar fi infiltrarea grupurilor pe Signal în care victima participă, trimiterea unor link-uri periculoase, a unor programe malware etc.

RECOMANDĂRI

Cum te poți proteja mai bine ca utilizator al platformei Signal, luând în considerare cele prezentate mai sus?

- Când primiți o nouă solicitare de contact pe Signal, **utilizați un alt canal sigur** pentru a verifica dacă solicitarea este autentică și dacă provine în fapt de la persoana de la care se pretinde că provine.
- **Verificați contactele dvs. existente**, comparând numărul dumneavoastră de siguranță cu al lor pe un alt canal de comunicare sigur (atingeți pictograma de profil a contactului dumneavoastră > Vizualizați numărul de siguranță).
- Dacă un contact al dumneavoastră își schimbă dispozitivul (semnalul va alerta în acest sens), este recomandat să **verificați din nou numărul de siguranță** al persoanei respective.
- **Activați actualizările automate** (în App Store sau Play Store) pentru a vă menține telefonul și aplicația Signal actualizate în orice moment.

- **Activați accesul PIN** la aplicația Signal (via pictograma profilului > Cont > Mementouri PIN).
- **Blocați funcția de înregistrare a altor dispozitive** pentru a preveni atacurile de tip SIM swap (via pictograma profilului > Cont > Blocare înregistrare).
- **Activați funcția de ștergere a mesajelor** pentru a preveni scurgerile mai mari de date în caz de compromis (via pictograma profilului > Cont > Confidențialitate > Mesaje care dispar).
- Deși mesajele în Signal pot fi setate să dispară după o anumită perioadă de timp, așa cum este definită în setările conversației, este posibil să nu oprească captarea sau reținerea mesajului prin capturi de ecran. **Activați funcția Screen Security** (via Setări -> Meniul confidențialitate) ce va dezactiva capacitatea oricui primește mesaje de la dumneavoastră, de a putea face o captură de ecran a conversației.
- Dacă utilizați Signal pe mai multe dispozitive, asigurați-vă că acestea sunt **configurate corect**.
- **Reporniți dispozitivul (smartphone) în mod periodic**, cel puțin o dată la câteva zile, pentru a înlătura orice infecție potențială cu malware nepersistent.
- **Nu ezitați să contactați Directoratul**, în cazul în care suspectați că grupul sau contul dumneavoastră de Signal a fost compromis sau a fost subiectul unui atac.

alerts@dnsc.ro

Telefon 1911

#DNSC #alert #cybersecurity #awareness