Metų pradžioje prasidėjusi masiškiausia dezinformacinė ataka su vieninteliu tikslu – vilioti pinigus iš patiklių gyventojų – toliau plinta Baltijos šalyse ir Lenkijoje, rodo „Debunk.org“ tyrimas. Savo veiklai sukčiai pasitelkia vis platesnį žinomų visuomenės veidų ratą – nuo pramogų pasaulio žvaigždžių, iki sportininkų ir Lietuvos, Latvijos, Estijos ir Lenkijos prezidentų bei premjerų.

„Tai, kad į dezinformacijos ir diskreditavimo kampaniją įtraukiami pirmieji valstybių asmenys, tampa ir nacionalinio saugumo bei tarptautinio valstybių reputacijos klausimais, – sako „Debunk“ vadovas Viktoras Daukšas. – Socialinių tinklų platformos neturi jokių saugiklių, kurie neleistų nusikaltėliams apsimetinėti dideliais prekės ženklais, tokiais kaip „Ignitis“, „Orlen Lietuva”, ar išnaudoti valstybės vadovų nuotraukas ar video. Turint omenyje kitąmet artėjančius trejus rinkimus, tai yra didelė grėsmė, kuria gali pasinaudoti Lietuvai nedraugiški veikėjai“.

„Debunk“ fiksuoja, kad socialiniuose tinkluose vykdomoje sukčių atakoje neteisėtai buvo pasinaudota LR prezidento Gitano Nausėdos ir premjerės Ingridos Šimonytės, Latvijos prezidento Edgar Rinkēvičs, Estijos prezidento Alaras Karis ir premjerės Kaja Kallas, taip pat Lenkijos vadovų ir buvusio Europos Tarybos prezidento Donaldo Tusko atvaizdais.

Pasak eksperto, sukčiai tampa vis išradingesni, manipuliuojama ne tik nuotraukomis, bet ir vaizdo įrašais – pavyzdžiui, naudojant dirbtiniu intelektu paremtą „deepfake“ video technologiją, sukčiai „įdėjo“ fiktyvios investavimo schemos reklamą į Lenkijos ministro pirmininko Mateuszo Morawieckio lūpas. Lietuvoje sukčiai jau panaudojo daugiau kaip 20 šalies vadovų, politikų, žurnalistų ir įtakingų visuomenės veidų – nuo futbolininko Deivido Šembero ar dainininko Vido Bareikio iki nuomonės formuotojos Viktorijos Siegel ar „Ignitis grupės“ vadovo Dariaus Maikštėno.

Atakos mastai išaugo

Lapkričio mėnesio duomenimis, sukčių veiksmų apimtys dar labiau išaugo. Jie jau panaudojo mažiausiai 124 profilius ir 119 netikrų svetainių adresų. Per šias paskyras parodytos net 1144 netikros „Facebook“ reklamos, o jų pasiekta auditorija – beveik 10 milijonų vartotojų. „Debunk“ neabejoja, kad ši dezinformacinė kampanija prisidėjo prie liūdnos Lietuvos bankų asociacijos paskelbtos statistikos, kad trečiąjį šių metų ketvirtį iš lietuvių sukčiai pavogė du milijonus eurų.

„Naudodamiesi netikrais žiniasklaidų priemonių ir visuomenės veikėjų profiliais sukčiai

skelbia ir intensyviai reklamuoja netikras naujienas. Nieko neįtariantys vartotojai nukreipiami į svetainę, kuri atrodo kaip tikra, o straipsnyje aprašomas neva lengvas būdas užsidirbti pinigų investuojant. Suvilioti vartotojai galiausiai nukreipiami į svetainę, kurioje sukčiai prašo pervesti pinigus“, – apie sukčių taikomą pinigų viliojimo schemą pasakoja V. Daukšas.

Didžioji dalis netikrų profilių bando apsimesti Lietuvos žiniasklaidos kanalais LRT, LNK, „Delfi“ „InfoTV“, ar „Ignitis“ bei „Orlen Lietuva“ įmonėmis. Kitose šalyse naudojami tų šalių populiarūs portalai.

Sukčiavimo atakų nepavyksta nutraukti nepaisant to, kad į „Facebook“ savininkę „Meta“ kreipėsi LR Vyriausybės atstovai. Ekspertai pastebi, kad nepaisant „Meta“ deklaruojamų pastangų kovoti su sukčiavimo schemomis, dezinformacija ir „botais“, matome, Facebook“ savininkų dėmesys problemai spręsti nėra pakankamas, o sukčių paskyros blokuojamos vangiai.

Kaip apsisaugoti nuo sukčių?

„Debunk“ vadovas aiškina, kad norėdami apsisaugoti nuo dezinformacijos ir sukčių atakų, gyventojai turėtų kritiškai vertinti socialiniuose tinkluose skaitomą turinį ir nuolat tikrinti, ar tai nėra klastotė. Susidūrus su klastote „Debunk“ visuomet rekomenduoja kreiptis į e. policiją.

Siekiant atskirti tikrą svetainę nuo fiktyvios, rekomenduojama atkreipti į dėmesį į interneto svetainės adresą, kuris dažniausiai skiriasi nuo tikrojo (pvz., egzistuojančios žiniasklaidos priemonės). Nors svetainės pavadinimas ir panašus, dažnai būna pridurta nereikalingų simbolių ir žodžių. Netikros svetainės taip pat kopijuoja atpažįstamų portalų dizainus, tačiau jose pasitaiko aibė klaidų ir neatitikimų.

Susidūrus su „deepfake“ technologija, dera prisiminti, kad dirbtinis intelektas šiandien jau gali imituoti ne tik žmogaus veidą, bet ir vaizdo įrašą, o taip pat – įdėti į lūpas tuos žodžius ir tas mintis, kurių kalbėtojas niekada nesakė. Pagrindinis patarimas norintiems neapsigauti – tikrinti informaciją kituose šaltiniuose.

Socialinių tinklų vartotojams taip pat patariama analizuoti skandalingas naujienas skleidžiančių autorių profilius. Paprastai jie būna šviežiai sukurti, neturi sekėjų, įrašų istorijos – ir tai jau yra rimtas signalas, kad profilis yra netikras ir sukurtas sukčiavimo ar dezinformacijos skleidimo tikslais. Pastebėjus tokius profilius, gyventojai taip pat gali apie juos pranešti Debunk.org.