Šiais metais interneto sukčių pradėta ataka, kuria bandoma išvilioti gyventojų pinigus pasinaudojant žinomų portalų, žmonių vardais ir „Ignitis“ pavadinimu, toliau plinta ir jau tapo masiškiausia iki šiol vykdyta dezinformacijos bei finansinio sukčiavimo ataka Lietuvoje. Dezinformacijos analizės centas „Debunk.org“ skaičiuoja, kad iki spalio vidurio socialiniuose tinkluose nusikaltėlių žinutės buvo ištransliuotos daugiau kaip 7,5 mln. kartų ir perspėja gyventojus likti atsargiems.

„Tai – iki šiol didžiausio masto mums žinoma dezinformacinė ir finansinio sukčiavimo ataka. Apgauti gyventojus sukčiai siekia kurdami netikras naujienų svetaines ir kviesdami žmones greitai pralobti investavus į iš tiesų neegzistuojančias investavimo platformas, kurias pristato neva kaip „Ignitis grupės“ ar kitos įmonės. Šis atvejis – sudėtingos atakos pavyzdys, kai apgaulės schemose taikomi socialinės inžinerijos, dezinformacijos ir manipuliacijos metodai, tačiau šiuo atveju neramina jos agresyvumas ir rekordiniai mastai“, – sako „Debunk.org“ vadovas ir dezinformacijos analizės ekspertas Viktoras Daukšas.

Kaip veikia sukčiai?

Šios atakos tyrimą atlikę „Debunk.org“ aptiko net 93 netikras paskyras „Facebook“ socialiniame tinkle, kurias sukčiai naudojo dezinformacijai ir klaidinančiam turiniui skleisti. Dauguma jų bando apsimesti žiniasklaidos kanalais „LRT“, „LNK“, „Delfi“, „InfoTV“ arba „Ignitis“ ar „Orlen Lietuva“ įmonėmis.

Per sukurtus apsimetėliškus profilius sukčiai skelbia ir intensyviai reklamuoja netikras naujienas su skandalingomis antraštėmis. Kad sudomintų vartotoją, remiamasi rezonansiniais įvykiais. Pavyzdžiui, istorijomis kai Neryje, kaip įtariama, motina nuskandino dvi dukras arba kai sostinėje dingo penkiolikmetis. Taip pat naudojamasi gerai žinomų žmonių vardais ir įmonių pavadinimais – nuo LR Prezidento, Andriaus Tapino ir Marijono Mikutavičiaus iki „Ignitis grupės“ ir jos vadovo Dariaus Maikštėno.

Nieko neįtariantys vartotojai, susidomėję įraše pateikiama „naujiena“, nukreipiami į svetainę, kuri atrodo it „Delfi“, „LRT“, „LNK“ ar kitas žinomas naujienų kanalas, bet iš tiesų yra tik jo klastotė. Čia pateikiamame straipsnyje aprašomas neva lengvas būdas gyventojui užsidirbti pinigų investuojant. Suvilioti vartotojai galiausiai nukreipiami į „Ignitis“ svetainės imitaciją, kurioje pateikiamas melagingas pasiūlymas investavus nedidelę sumą uždirbti po 200 tūkst. Eur per metus. Svetainėje vartotojo prašoma įvesti savo banko duomenis ir tokiu būdu sukčiai įgauna prieigą prie gyventojo sąskaitų bei gali pasisavinti lėšas.

Gyventojų klaidinimui mestos didelės pajėgos

Ekspertų vertinimu, ši sukčių ataka yra gerai suplanuota ir parengta, buvo įdėta daug pastangų, sukurtos identiškos naujienų portalų kopijos. Taip pat veikiama smūginiu būdu – greitai ir intensyviai reklamuojami klaidinantys, melagingi įrašai.

„Debunk.org“ tyrimas atskleidė, kad iki spalio vidurio socialiniuose įrašuose buvo paleisti daugiau kaip 568 reklamuojami įrašai, kurie transliuoti milijonus kartų ne tik „Facebook“ socialiniame tinkle, bet ir per „Instagram“ bei „Messenger“ platformas.

Vien apgaulingai pasinaudojant „Ignitis“ vardu, buvo sukurta mažiausiai 14 netikrų paskyrų „Facebook“, iš kurių buvo leidžiamos 22 melagingos reklamos, o bendrai su „Ignitis“ vardu buvo ištransliuotos net 122 reklamos, kurios parodytos 1,33 mln. kartų. Debunk.org duomenimis, šias reklamas jau pamatė apie pusė Lietuvos „Facebook“ vartotojų, o vienam žmogui jos vidutiniškai buvo parodytos apie tris kartus.

Šios atakos mastai, anot ekspertų, rodo, kad nusikaltėliams pavyksta apgauti dalį gyventojų – antraip pastangos jau būtų nuslopusios. Be to, „Debunk.org“ pastebi, kad ataka ne tik tęsiama, bet jau peržengė ir Lietuvos ribas – žinutės rengiamos ir rusų, latvių, lenkų, čekų, vokiečių ir olandų kalbomis, imituojami ir kitų šalių žiniasklaidos kanalai, pvz. Estijos nacionalinio transliuotojo ERR ar laikraščio „Eesti Päevaleht“.

Nepakankamas kompanijos „Meta“ dėmesys problemai

Šiuo metu „Debunk.org“ neturi žinių apie nuo šios sukčių atakos nukentėjusius asmenis. Tačiau jeigu tokių yra, V. Daukšas ragina nedelsiant imtis veiksmų – kreiptis į policiją arba užpildyti formą puslapyje Debunk.org/pranesti, kurie perduos visą informaciją pareigūnams.

Dezinformacijos ekspertas taip pat teigia, jog apie neteisėtus nusikaltėlių veiksmus buvo pranešta institucijoms, tačiau kovoti su tokiomis atakomis – sudėtinga.

„Pirmieji netikri profiliai „Facebook“ socialiniame tinkle buvo sukurti paskutinėmis gegužės dienomis. Liepos ir spalio mėnesiais LR Vyriausybės atstovai kreipėsi į „Meta“ atstovus dėl šių netikrų puslapių ir reklamų pašalinimo, tačiau socialinio tinklo atstovai nesiima reikiamų veiksmų. „Facebook“ valdančios bendrovės „Meta“ aplaidumas leidžia toliau kurti naujus netikrus profilius ir platinti dezinformaciją bei vilioti pinigus iš Lietuvos piliečių. Todėl raginame gyventojus būti budriais, neiti į nesaugias svetaines ir jokiu būdu jose nesuvedinėti savo asmeninių, finansinių duomenų“, – sako V. Daukšas.

Kompanijos „Meta“ atstovams LRVK Nacionalinis krizių valdymo centras yra pateikęs 3 oficialius pranešimus pagal „Debunk.org“ atliktus tyrimus, tačiau „Facebook“ savininkų dėmesys problemai spręsti nėra pakankamas, o sukčių paskyros blokuojamos vangiai.

„Nepaisant vykstančio dialogo su kompanija „Meta“ bei jų deklaruojamų pastangų kovoti su sukčiavimo schemomis, dezinformacija ir „botais“, matome, kad reikalingas papildomas institucijų indėlis ir teisinis reglamentavimas, padedant Lietuvos gyventojams išvengti nuostolių bei apsisaugoti nuo nepatikimos informacijos. Nacionalinis kibernetinio saugumo centras jau susitarė su Internetinės žiniasklaidos asociacija, kad vartotojai bus informuojami specialiais užrašais apie naujienų portalų dublikatus, o jų adresai perduodami Lietuvos policijai, Lietuvos radijo ir televizijos komisijai, Žurnalistų etikos inspektoriui, kad būtų kuo skubiau blokuojami. Taip pat Vyriausybė pritarė bei šiuo metu Seime svarstomos Visuomenės informavimo įstatymo bei Baudžiamojo kodekso pataisos dėl „botų“ naudojimo socialiniuose tinkluose uždraudimo prisidės sprendžiant nepatikimos informacijos ar dezinformacijos dirbtinio amplifikavimo problemą“, – pažymi Ministrės pirmininkės patarėjas Rimantas Žylius.

Į ką atkreipti dėmesį gyventojams

Siekdami apsisaugoti nuo dezinformacijos ir finansinių sukčių atakų gyventojai turėtų atidžiai vertinti socialiniuose tinkluose matomą turinį, bei pasitikrinti ar jis nėra klastotė.

Norint atskirti tikrą svetainę nuo fiktyvios, pirmiausia ekspertai rekomenduoja atkreipti dėmesį į interneto svetainės adresą: sukčiai labai dažnai bando sukurti tokius adresus, kurie atrodytų panašūs į tikrus. Pavyzdžiui, adrese naudojamas žinomos svetainės pavadinimas, bet yra padaroma sunkiai pastebima klaida, pakeičiama galūnė, prirašomi papildomi žodžiai. Tai išduoda, kad svetainė iš tiesų yra klastotė ir gali būti naudojama dezinformacijos ar finansinio sukčiavimo tikslais.

Socialiniuose tinkluose ekspertai vartotojams taip pat pataria paanalizuoti 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.