Baltijos šalyse tebesitęsiant masiškiausiai sukčiavimo ir dezinformacijos atakai, dezinformacijos analizės centro „Debunk.org“ ekspertai ištyrė nusikaltėlių taikomą schemą. Analitikai akcentuoja sukčių naudojamų metodų kompleksiškumą ir pastebi, kad sustabdyti tokių atakų institucijoms nepavyksta ir dėl vangaus „Facebook“ socialinį tinklą valdančios įmonės „Meta“ bendradarbiavimo, mat jai sukčių veikla neša pelną.

„Didžiausią atakos intensyvumą stebėjome šių metų rugsėjo-spalio mėnesiais. Matome, kad aktyvus viešinimas, kartu su policijos ir valdžios institucijų veiksmais, padarė įtakos. Vis tik, bandymai apgauti tebetęsiami, nors ir mažesniu masteliu“, – sako „Debunk.org“ vadovas Viktoras Daukšas.

Šioje masiškiausioje dezinformacijos ir sukčiavimo atakoje nusikaltėliai, pasinaudodami įvairių politikų, žinomų žmonių, įmonių ir naujienų portalų vardais bei rezonansiniais įvykiais, siekia suvilioti gyventojus „pelningai investuoti“ į iš tiesų neegzistuojančias platformas. Žinoma, visus „investuotus“ pinigus susivilioję gyventojai praranda.

Naudoja labai pažangias maskuotės technologijas

V.Daukšas teigia, kad sukčiai šiai atakai naudojo technologiškai pažangias schemas. Tarp tokių – vadinamoji maskuotės technologija. Jos esmė – sukurti daugybę įvairių svetainių ar puslapių ir, atsižvelgiant į tam tikrus kriterijus, skirtingiems vartotojams rodyti skirtingą turinį. Pavyzdžiui, potencialioms aukoms rodoma apgavikiška svetainė bei netikra investavimo platforma, o „Meta“ moderatoriai ar tyrėjai nukreipiami į visai nesusijusius tikrus tinklalapius ar jų kopijas.

Be to, apgavikiškose svetainėse sukčiai automatiškai atvaizduoja turinį ta kalba ir apie tokias aktualijas, iš kurios šalies yra vartotojas. Pavyzdžiui, vartotojai iš Lietuvos nukreipiami į svetainę, kuri apsimeta „Delfi“ ar kita žinoma žiniasklaidos priemone, netikrame straipsnyje naudojami žinomų žmonių (G. Nausėdos, I. Šimonytės, M. Mikutavičiaus ar kt.) atvaizdai ir netikros citatos, o investuoti siūloma į neegzistuojančias platformas su „Ignitis“ pavadinimu. Tuo tarpu Latvijoje, Estijoje ar Lenkijoje vartotojams buvo rodomos vietinės „naujienos“, įžymybės ir įvykiai.

„Visi šie procesai vykdomi sukčiams automatiškai identifikuojant vartotoją pagal įvairius kriterijus: šalį, IP adresą, naršyklę, paspaudimų skaičių, praleistą laiką ir kitus elgsenos sekimo parametrus. Nusikaltėliai, vengdami būti susekti, taip pat slepia bet kokius savo

pėdsakus – netikrų svetainių domenus registruoja per lengvatinio apmokestinimo bendroves tokiose šalyse kaip Panama, Sent Kitsas ir Nevis, naudojosi ir buvusio populiarios *torentų* svetainės „Pirate Bay“ įkūrėjo Peter Sunde sukurta paslauga, leidžiančią domenus registruoti anonimiškai“, – aiškina V. Daukšas.

Gyventojai prarado šimtus tūkstančių eurų

„Debunk.org“ skaičiuoja, kad masiškiausiai kada nors užfiksuotai dezinformacijos ir sukčiavimo atakai nusikaltėliai panaudojo mažiausiai 119 netikrų svetainių adresų ir 124 profilius „Facebook“ socialiniame tinkle. Per šias paskyras parodytos net 1144 netikros reklamos, o jų pasiekta auditorija – beveik 10 milijonų vartotojų.

Kad sukčių investicijos „atsipirko“ rodo ir „Eesti Ekspress“ gautos istorijos iš nukentėjusių vartotojų. Pavyzdžiui, vien pamatę reklamą su Elonu Musku ir „Tesla“, šeši nukentėjusieji Estijoje prarado nuo 2 tūkst. iki 46 tūkst. eurų. O reklama su buvusia Estijos prezidente Kersti Kaljulaid paskatino bent vieną asmenį investuoti ir dėl to prarasti virš 9 tūkst. eurų.

„Nemažai žmonių prarado didesnes ar mažesnes pinigų sumas, tačiau savo atvejų neviešina. Tad spėju, kad per šią ataką iš gyventojų išviliota keli šimtai tūkstančių eurų“, – sako V. Daukšas.

Ryšių reguliavimo tarnyba kreipsis į EK

„Debunk.org“ atstovas teigia, kad kibernetinių nusikaltėlių veiklos ribojimas yra nelengvas uždavinys, tačiau „Meta“ akivaizdžiai skiria nepakankamai dėmesio ir resursų. Organizacija kreipėsi į Ryšių reguliavimo tarnybą (RRT) dėl šios sukčiavimo schemos. RRT nustatė, kad „Ignitis“ apsimetančios „Facebook“ paskyros kelia potencialią riziką ir kreipėsi į „Meta“ dėl jų pašalinimo. Dalis jų buvo ištrintos, tačiau viena „Ignitis“ pasivadinusi netikra paskyra liko veikti, nes pasak „Meta“, nepažeidžia taisyklių.

„Nors „Facebook“ teigia pašalinęs netikrus puslapius, apgaulingus skelbimus ir nuorodas, daugelis jų vis dar veikia, o socialinius tinklus kasdien užplūsta nauji. Didžiausia problema – bendradarbiavimo iš „Meta“ pusės trūkumas. Deja, bet „Meta“ sukčių platinama reklama iš dalies yra naudinga, nes įmonė už jos platinimą gauna pajamų“, – pastebi V. Daukšas.

Ryšių reguliavimo tarnyba bei Seimo kultūros komitetas pareiškė rengiantys kreipimąsi į Europos Komisiją dėl įvertinimo ar tai yra Skaitmeninių paslaugų akto pažeidimas. Vieningai sutariama, kad EK turėtų paskatinti „Meta“ įmonę tobulinti kovos su nusikalstamumu politiką ir prisiimti atsakomybę už sukčių blokavimą, nes per socialinius tinklus nusikaltėliai

pasiekia didelę auditoriją ir toliau daro žalą naujoms aukoms.

Vartotojams saugumo ekspertai primena internete būti atsargiems – visus „itin gerus“ pasiūlymus reikia vertinti labai kritiškai. Taip pat svarbu atpažinti netikras svetaines ir profilius: paprastai jie būna šviežiai sukurti, neturi sekėjų, įrašų istorijos, o netikros interneto svetainės pastebimiausias ženklas – internetinio adreso eilutė. Sukčiai dažnai bando sukurti adresą, kuris primintų tikrą, tačiau iš tiesų būtų sukeistos raidės, pridėta kita galūnė ar pan. Pastebėjus sukčiavimo atvejus, gyventojai apie juos kviečiami pranešti „Debunk.org“.

Nuoroda į pilną „Debunk.org“ tyrimo ataskaitą:
https://www.debunk.org/lt/apt-weredirect-didelio-masto-sukciavimo-ataka