Pandemijos metu ypač suaktyvėja programišiai, siekiantys pakenkti mobiliųjų telefonų vartotojams. Viena dažniausiai naudojamų atakų priemonių – apgaulės programėlės. Jas į įrenginius atsisiuntę žmonės nieko neįtardami gali netekti savo asmens duomenų, privatumo ir net pinigų. Skaičiuojama, kad šių programėlių padaryta žala šiemet sieks daugiau nei milijardą eurų. Kaip jas atpažinti ir nuo pavojaus apsisaugoti tinkamai?

Kas yra apgaulės programėlės?

Apgaulės programėlės (angl. rogue apps) iš pirmo žvilgsnio primena mums įprastas – atrodo taip pat, atlieka kūrėjų žadėtą funkciją. Bet iš tiesų jos sąmoningai sukurtos taip, jog apkrėstų įrenginius, neteisėtai naudotų nieko neįtariančių vartotojų informaciją ar kitaip kenktų vartotojams.

„Į telefoną atsisiuntę smagią programėlę, kuri, pavyzdžiui, gali juokingai iškraipyti ar pakeisti jūsų balsą, net neįtartumėte, kad šiai funkcijai atlikti reikalinga prieiga prie jūsų įrenginio mikrofono gali būti panaudota neteisėtai ir jums nežinant. Būtent taip ir veikia „rogue“ programėlės – vartotojas masinamas jas atsisiųsti dėl smagios ar naudingos funkcijos, tačiau jos, patekusios į įrenginį, šį apkrečia ar gautą prieigą prie telefono funkcijų naudoja neteisėtai“, – aiškina „Huawei Mobile Services“ verslo vystymo ir operacijų vadovas Audrius Granickas.

Įsidiegę šias programėles telefone, vartotojai nieko nežinodami gali netekti savo asmens duomenų, privatumo, prieigos prie kai kurių įrenginio funkcijų, o kartais – net ir pinigų. Pavojų jos kelia ir verslams – žinomą prekės ženklą apgaulei panaudoję programišiai jam gali padaryti neatitaisomą reputacinę žalą.

„Apie apgaulės programėles būtina kalbėti, nes tai nėra tik smulkus pavojus internete – skaičiuojama, kad jų padarytos žalos mastas 2021 m. sieks net 1,38 milijardo eurų. Net 93 proc. mobiliųjų operacijų pernai buvo įvertintos kaip apgaulingos ir dėl to užblokuotos, rodo „Mobile Ad Fraud 2019 Report“ tyrimo duomenys“, – pasakoja A. Granickas.

Kaip jos patenka į įrenginį?

Norint nuo apgaulės programėlių apsisaugoti, pirmiausiai būtina žinoti, kokiais būdais jos patenka į vartotojų mobiliuosius. Dažniausiai taip nutinka tuomet, kai vartotojai jas atsisiunčia iš nepatikimų šaltinių ar paspaudę keistus jų atsisiuntimo adresus.

„Įprastai tuo, kad į telefoną nepatektų kenksmingos programėlės, rūpinasi ir patys gamintojai. Jie testuoja savo oficialias parduotuves, kur kenksmingos programėlės patikrinamos ir akimirksniu užblokuojamos, jei neatitinka saugumo reikalavimų. Bet kartais žmonės dominančias programėles randa kur nors internete, nežinomuose puslapiuose, ar nepažįstamų siuntėjų gautuose laiškuose. Iš tokių vietų atsisiųstos programėlės beveik visada yra apgaulingos, tad rekomenduojama nepatikimų šaltinių vengti“, – sako A. Granickas.

Jei norimos programėlės nerandate oficialioje parduotuvėje, paieškokite jos oficialiame gamintojo puslapyje. Net „Facebook“ visiškai saugiai galima atsisiųsti naudojant naršyklę. Jei produkto nerandate ir šiose vietose, verčiau tokių programėlių iš viso venkite.

„Programėlių parduotuvės siekia maksimaliai užtikrinti vartotojų saugumą, tad taiko įvairias prevencijos priemones. Pavyzdžiui, „AppGallery“ parduotuvėje, pirmiausiai, nustatome ir patikriname kūrėjų tapatybę, tuomet – ar programėlės nėra apgaulingos, kokių duomenų prieigos jos reikalauja, o galiausiai turime vietinius specialistus, kurie rankiniu būdu išbando parduotuvėje esančius produktus. Net ir jau vartotojų naudojamas programėles vis pakartotinai testuojame, atliekame vartotojų naudojimo patirties vertinimą, kad būtume tikri, kad šiuose produktuose niekas nepakito ir vartotojai jais toliau gali sėkmingai naudotis“, – pasakoja A. Granickas.

Eksperto teigimu, „AppGallery“ vien praėjusiais metais atmetė apie 37 proc. programėlių, nes šios neatitiko saugumo reikalavimų.

Ką daryti tokią programėlę atsisiuntus?

Dažnai apgaulės programėlės sukelia bėdų ne tik todėl, kad gali apkrėsti įrenginius, bet ir todėl, kad prašo prieigos prie svarbių telefono funkcijų, kurias vėliau neteisėtai naudoja. Todėl prieš įsirašydami bet kokią išmaniąją programėlę, atidžiai patikrinkite, kokios prieigos ir prie kurių telefono funkcijų prašoma.

„Laikykitės esminės taisyklės – prieigos prašymas turi atitikti programėlės tiesiogines funkcijas. Pavyzdžiui, jei siunčiatės žemėlapių programėlę, jai gali prireikti prieigos prie jūsų vietos nustatymo, kad GPS nuorodos būtų tikslios. Bet jai tikrai nereikės jūsų mikrofono ar kameros valdymo galimybės, nes su tokia prieiga susijusių funkcijų joje tiesiog nėra. Jei tokios prieigos prašoma, tai turėtų kelti įtarimų“, – pataria A. Granickas.

Jei esate tikri, kad apgaulės programėles atpažinti galite, bet įtariate, kad netyčia jau esate įsidiegę vieną tokių, atkreipkite dėmesį, ar nedidėja telefono išnaudojamos energijos kiekis,

ar nesulėtėjusios gamintojo įrašytos programos. Jei telefono veikimas kelia įtarimų, nerizikuokite ir kaip įmanoma greičiau pašalinkite įtartinas programėles.

„Apgaulės programėlės dažniausiai veikia taip, kad neturėtumėte jos įjungti, kad ji atliktų savo neteisėtą funkciją. Todėl paprastas jos išjungimas ir nenaudojimas nuo duomenų vagystės jūsų neapsaugos. Programėlę reikės ištrinti – geriausia tai padaryti naudojant saugųjį telefono režimą (angl. Safe Mode)“, – pasakoja „Huawei“ ekspertas.