

Taip lengviau: greitis skaitymas

- **Telefonai - itin patrauklus kėsnis programišiams, nes čia vis dar nėra nusistovėjusių saugumo tradicijų, o jų savininkai į saugumą dažnai žvelgia atsainiai**
- **Kenkėjiškos programos telefonams gali savintis įvairius prisijungimo duomenis, perduoti kameros vaizdą ir garsą, apkrauti įrenginį įvairiomis reklamomis ar net užšifruoti visus duomenis ir už jų atrakinimą reikalauti išpirkos**
- **Tiesiausias kelias įsilaužėliui - neatnaujinta operacinė sistema ir programėlės bei neapsaugotų viešų bevielio interneto („WiFi“) tinklų naudojimas**
- **„Nulaužta“ telefoną gali išduoti sulėtėjęs veikimas, greičiau išsikraunanti baterija, staiga išaugęs matomų reklamų skaičius ar net padidėję sąskaitos už mobiliųjų ryši**

Kompiuteriams skirti virusai ir tai, kad nuo jų būtina saugotis - nieko nestebina, tačiau dažnai pamirštame, jog išmanieji telefonai reikalauja tokių pačių apsaugos priemonių. Perskaityta speciali SMS žinutė ar prisijungimas prie neapsaugoto bevielio interneto („WiFi“) tinklo gali atverti programišiams duris į jūsų asmeninius duomenis, pridaryti finansinių nuostolių ar paversti telefoną įsilaužimo raktu į darbovietės vidinį tinklą. „Bitės Profai“ kartu su kibernetinio saugumo bendrovės „NRD Cyber Security“ ekspertu apžvelgia, kaip į mūsų telefonus atkeliauja kenksmingos programos ir kaip nuo jų apsisaugoti.

„Išmanieji telefonai šiuo metu yra bene populiariausia platforma su kuria dirba praktiškai visas pasaulis. Čia kaupiame begalę jautrių asmeninių duomenų, naudojamės elektronine bankininkyste, jungiamės prie savo darbovietės „WiFi“ tinklo. Kol kas, priešingai nei kompiuterių pasaulyje, nėra nusistovėjusios praktikos ir tradicijų kaip tokius įrenginius saugoti, todėl išmanusis telefonas – itin patrauklus kėsnis programišiams“, – sako Marius Urkis, „NRD Cyber Security“ kibernetinio saugumo incidentų valdymo ir tyrimo ekspertas.

Išmaniesiems telefonams skirtų kenkėjų yra itin įvairių. Vieni gali apsimesti tikromis programėlėmis ir tuo pačiu kažkam siųsti jūsų asmeninius duomenis. Pavyzdžiui, šį mėnesį „Google“ iš savo programėlių parduotuvės „Play Store“ pašalino 25 programėles, kurios be savo pirminės funkcijos – sekti žingsnių kiekį, redaguoti vaizdo įrašus ir pan. – programišiams perduodavo ir telefono naudotojo „Facebook“ prisijungimo duomenis.

„Kiti kenkėjai gali jūsų telefone dirbtinai rodyti daugiau reklaminių skydelių, netgi perduoti vaizdą iš įrenginio kameros ar garsą iš jo mikrofonų, užšifruoti visus telefono duomenis ir už

jų atrakinimą paprašyti išpirkos. Kiti gali tyliai laukti, kol prisijungsite prie savo darbovietės bevielio tinklo ir tuomet suteikti programišiui tiesioginę prieigą prie įvairių vidinių dokumentų ar sistemų. Galimybės čia neribotos ir beveik niekuo nesiskiria nuo saugumo grėsmių įprastiems kompiuteriams“, – teigia „Bitės Profas“ Andrius Archangelkis.

Durys į telefoną - ir nesaugus „WiFi“

Turbūt nerasime nė vieno telefono savininko, kuris išvydęs išpėjimą, kad reikia atnaujinti operacinę sistemą ar programėles, pagalvojo „kada nors kitą kartą“.

„Taip elgtis nederėtų, nes šie atnaujinimai ištaiso naujai atrastas saugumo spragas, kurios programišiams leidžia be didelių pastangų į neatnaujintus telefonus įdiegti kenkėjiškas programėles be mūsų žinios. Įdomu tai, kad „iPhone“ savininkai yra kiek pareigingesni – „StatCounter“ duomenimis pačią naujausią „iOS“ versiją birželio pabaigoje pasaulyje naudojo per 35 proc. „iPhone“ ir „iPad“ savininkų. „Android“ stovykloje pačią naujausią šios operacinės versiją turėjo tik kas penktas, o beveik pusėje „Android“ įrenginių veikė tris ar net dar daugiau metų neatnaujintos operacinės sistemos versijos. Taip pat labai svarbu nepamiršti atnaujinti ir pačių telefone veikiančių programėlių“, – pastebi A. Archangelkis.

Nemokami vieši ir slaptažodžiais neapsaugoti bevielio interneto („WiFi“) tinklai – dar vienas kelias į mūsų įrenginius. „Programišiai gali sukurti dirbtinius „WiFi“ tinklus, kurie veiks ir atrodys lyg tikri, bet tuo pačiu leis surasti telefonuose esančias saugumo spragas, stebėti kokius portalus aplanko vartotojas ar net perimti įvairius prisijungimo duomenis. Tokiu atveju visada geriau naudoti mobilių internetą, o neturint kitos galimybės – nesijungti prie el. pašto, soc. tinklų ar bankininkystės platformų ir tuo pačiu užtikrinti, kad įrenginys turi naujausią operacinę versiją, o programėlės – atnaujintos“, – sako M. Urkis.

Taip pat reikėtų stengtis programėles siųsti tik iš oficialių jų parduotuvių: „Apple“ įrenginiams – „App Store“, „Android“ – „Google Play Store“. Kitu atveju iškyla didelė rizika, kad kartu su programėle į telefoną atkeliaus ir pasislėpusi kenksminga programa.

„Tai nėra vieninteliai būdai, kaip kenkėjai patenka į telefonus. Jei šie yra pilni saugumo spragų, programišiui gali pakakti atsiųsti SMS žinutę su specialiu tekstu – ją atidarius telefonas taps pažeidžiamu. Taip pat čia galioja ir tradiciniai, kompiuterių pasaulyje įprasti būdai, kaip žinutės ar el. laišakai su kenksmingomis nuorodomis ir failais“, – įspėja M. Urkis.

Požymiai išduodantys „užkrėstą“ telefoną

Kenksmingas programą aptikti gali būti nelengva, nes programišiai dažnai stengiasi, kad

jos veikų kuo mažiau pastebimai ir atneštų kuo daugiau naudos.

„Kenkėją telefone gali išduoti staigiai išaugęs matomų reklaminių skydelių kiekis, netikėtai sulėtėjęs įrenginys arba greičiau išsikraunanti baterija. Telefone gali atsirasti anksčiau nematytų programėlių, išaugti sąskaitos už mobilųjį ryšį arba adresų knygelėje esantys kontaktai gali pradėti gauti įvairias žinutes iš jūsų“, – teigia M. Urkis.

Pastebėjus tokius simptomus rekomenduojama parsisiųsti patikimo gamintojo (pvz., „Avast“, „AVG“, „Bitdefender“) antivirusinę programėlę ir leisti jai nuskanuoti telefoną. Situacijai nepasikeitus gali tekti ištrinti visą telefone esančią informaciją ir atstatyti telefono gamyklinius parametrus. Taip pat labai svarbu bet kuriuo atveju pasikeisti visus pagrindinius slaptažodžius.

Auksinės saugaus telefono taisyklės:

- Kuo greičiau atnaujinti telefono operacinę sistemą ir jame esančias programėles
- Vengti viešų, slaptažodžiais neapsaugotų bevielio interneto („WiFi“) tinklų
- Programėles diegti tik iš oficialių programėlių parduotuvių
- Įvertinti, kokių teisių prašo diegiama programėlė: jei vaizdo klipų redagavimo programėlė reikalauja prieigos prie adresų knygelės kontaktų, vertėtų paieškoti vartotojų atsiliepimų ar ji išties patikima
- Neatidarinėti įtartinų SMS žinučių, nepatikimai atrodančių nuorodų el. laiškuose ar draugų žinutėse socialiniuose tinkluose

Daugiau informacijos apie išmaniųjų įrenginių priežiūrą ir saugumą galite sužinoti iš didžiųjų miestų „Bitės“ salonuose įsikūrusių „Bitės Profų“. Išmaniųjų technologijų ekspertai konsultuoja nemokamai nepriklausomai nuo to, kokio tinklo paslaugomis naudojats.

Daugiau naudingų patarimų ir įdomių naujienų ieškokite „Bitės Profų“

puslapyje <https://www.bite.lt/profai>.

