Võltsrakendused - mis need on ja kuidas ennast kaitsta?

18. oktoober 2020 - 13:07 Autor: AM

Nutiseadmete kasutamise kasvuga muutuvad üha aktiivsemaks häkkerid, kes kasutavad rünnakuvahendina võltsrakendusi, mille tekitatud kahju sel aastal ületab maailmas ligi miljard eurot. Kuidas selliseid rakendusi ära tunda ja end võimalike ohtude eest kaitsta?

Võltsrakendused näevad välja nagu tavalised äpid, mis on teadlikult programmeeritud seadmete nakatamiseks, heausklike kasutajate andmete näppamiseks või muul viisil pahategudeks.

„Võltsrakendused töötavad üldjuhul nii, et kasutajas tekitatakse kiusatus need alla laadida, pakkudes mingit lõbusat ajaviidet või kasulikku funktsiooni. Kuid peale allalaadimist nakatavad võltsrakendused telefoni või kasutavad ebaseaduslikku juurdepääsu seadme muudele funktsioonidele," ütleb Vitali Donskoi, Huawei Mobile Service äriarenduse juht.

Pahatahtlikke rakendusi oma telefoni installides võivad kasutajad kaotada oma isikuandmed, privaatsuse, juurdepääsu seadme mõnele funktsioonile või isegi raha. Need rakendused kujutavad endast ohtu ka ettevõtetele - häkkerid, kes kasutavad ausat kaubamärki pettuste jaoks, võivad ettevõtte mainele korvamatut kahju teha.

„Petturitest ja võltsrakendustest tuleb rohkem rääkida, sest tegemist pole ainult väikese ohuga internetis - hinnanguliselt ulatub 2021. aastal nende tekitatud kahju lausa 1,38 miljardi euroni. Tundub uskumatu, aga Mobile Ad Fraud 2019 raporti põhjal hinnati 93 protsenti eelmise aasta mobiilsetest tehingutest petlikuks ning blokeeriti," juhib Donskoi tähelepanu olukorra tõsidusele.

Kuidas jõuab võltsrakendus seadmesse?

Pahatahtlike rakenduste eest kaitsmiseks peab eelkõige teadma viise, kuidas need tarbijate mobiiltelefonidesse satuvad. Tavaliselt juhtub see siis, kui kasutaja laadib rakenduse alla ebausaldusväärsest allikatest, klikkides mõnel allalaadimist pakkuval lingil.

„Kõige kindlam on rakendusi alla laadida ametlikest rakenduste poodidest, kus neid kontrollitakse ja blokeeritakse koheselt, kui need ei vasta turvanõuetele. Mõnikord leiavad inimesed siiski huvipakkuva rakenduse kuskilt tundmatult veebilehtelt või võõraste saatjate e-kirjadest. Selliselt alla laaditud rakendused on peaaegu alati pahatahtlikud, mistõttu soovitan tungivalt vältida kõiki ebausaldusväärseid või tundmatuid allikaid," hoiatab Donskoi.

Kui ametlikust poest soovitud rakendust ei leia, tuleks seda otsida tootja veebilehelt. Vitali Donskoi sõnul saab ka näiteks Facebooki rakenduse brauseri abil turvaliselt alla laadida, ent kui soovitud toodet usaldusväärsetelt veebilehtedelt ei leia, tuleks rakenduse allalaadimist vältida.

Ametlikud rakendustepoed püüavad maksimaalselt tagada tarbijate ohutuse, rakendades mitmesuguseid ennetusmeetmeid. „Näiteks Huawei AppGallery's tuvastame ja kontrollime arendajate identiteeti, seejärel analüüsime, kas rakendused on loodud pahatahtlike

toimingute tegemiseks. Järgneb privaatsusanalüüs ja kontroll, millistele andmetele rakendused juurdepääsu vajavad, ning lõpuks testivad meie spetsialistid kõiki poe tooteid käsitsi. Ka juba kasutuses olevate rakenduste puhul testime pidevalt ja hindame kasutajakogemust - veendumaks, et toodetes poleks midagi muutunud," kirjeldab Donskoi Huawei mitmetasandilist turvaprotsessi.

Eksperdi sõnul lükkas AppGallery ainuüksi eelmisel aastal umbes 37 protsenti rakendustest tagasi, kuna need ei vastanud turvanõuetele.

Kuidas võltsrakendust ära tunda?

Võltsrakendused ei tekita probleeme ainult seetõttu, et need võivad seadmeid nakatada, vaid ka seetõttu, et nad paluvad juurdepääsu telefoni olulistele funktsioonidele, mida siis ebaseaduslikult kasutatakse. Enne nutirakenduse allalaadimist tuleb kontrollida, millist juurdepääsu ja milliseid telefoni funktsioone soovib rakendus kasutada.

„Järgige põhireeglit - juurdepääsutaotlus peab olema otseses seoses rakenduse funktsionaalsusega. Näiteks kui laadite alla kaardi- või GPS-rakenduse, võib see täpsete juhiste andmiseks vajada juurdepääsu teie praegusele asukohale. Kuid samal ajal ei pea see olema võimeline juhtima teie mikrofoni ega kaamerat. Kui sellist juurdepääsu taotletakse, peaks see koheselt kahtlusi tekitama," selgitab Donskoi.

Ekspert jagab õpetussõnu: „Kui kahtlustate, et olete pahatahtliku rakenduse siiski tahtmatult installinud, pöörake tähelepanu sellele, kas teie telefoni energiatarve suureneb või teised rakendused muutuvad aeglasemaks. Kahtlane rakendus tuleks telefonist eemaldada esimesel võimalusel."

"Võltsrakendused töötavad tavaliselt nii kavalalt, et kahju põhjustamiseks ei pea rakendust isegi sisse lülitama, see tegutseb vaikselt taustal. Seetõttu ei kaitse teid andmevarguste eest sellise rakenduse välja lülitamine või mitte kasutamine. Ainuke lahendus on rakenduse kustutamine, mida on kõige parem teha turvarežiimis (*Safe Mode*)," ütleb Huawei ekspert.

- Uudised

- Androidiblog
- Tarkvara
- Turvalisus