Uus nuhtlusisend: RatHat murrab Androidi sisse ja keeldub lahkumast

16 min tagasi - 20.09.2026 Autor: AM

Zimperiumi küberturbeuurijate värskelt avastatud Androidi pahavara nimega RatHat viib küberkuritegevuse täiesti uuele tasemele. Tõenäoliselt Hiinast pärit küberpättide poolt juhitud ründetarkvara on tehisaru toel tegutsev sissetungija, mis võtab kasutaja telefoni üle ja keeldub lahkumast isegi siis, kui oled kindel, et viskasid selle juba ukse taha.

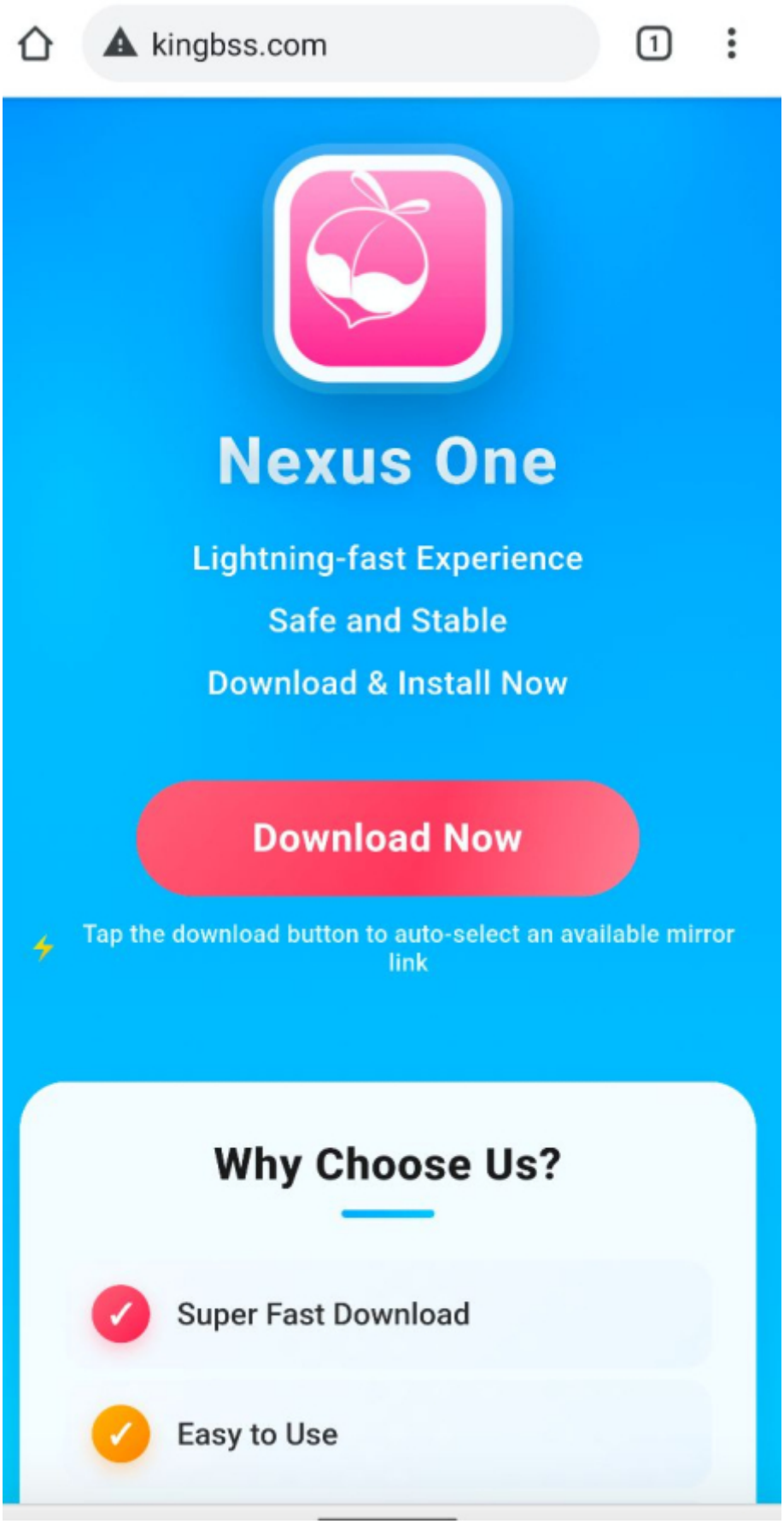
See tüütu rott loeb ekraanilt teksti, saab aru sinu pangarakendustest ja klõpsib puutepinnal nuppe täpselt nii, nagu sa ise seda teeksid. RatHat kasutab seadme juurdepääsetavusteenuseid (*Accessibility Service*), et muuta seadmes toimuv reaalajas XML-koodiks, mille siis söödab ette generatiivsele tehisarule.

Tehisintellekt omakorda suudab selle põhjal iseseisvalt seadmes navigeerida ja menüüdes edasi "kerida".

Zimperiumi uurijad Gianluca Braga, Vishnu Pratapagiri ja Fernando Ortega selgitasid oma lehel olukorra tõsidust tehnilises keeles: "Pärast paigaldamist ühendab see juurdepääsetavusteenuste kuritarvitamise autonoomse lokaalse ADB enesesidumise funktsiooniga, et murda välja standardsest Androidi rakenduste liivakastist, käivitades iseseisvad süsteemsed taustaprogrammid, mis töötavad kerneli taseme õigustega."

Kuidas pahalane seadmesse jõuab?

Pahavara ei hüppa Sinu seadmesse iseenesest. See poeb sisse petlike SMS-õngitsuste (*smishing*), pahatahtlike reklaamide ja kolmandate osapoolte allalaadimisportaalide kaudu.



Alguses tundub kõik legaalne – laadid alla justkui tavalise äpi. Kuid tegemist on Trooja hobusega. *Dropper* peidab endas mitut kavalat kihti (näiteks *Manifest*

bomb ja *DEX bytecode poisoning*), mis ajavad automaatsed turvaanalüüsid segadusse ja jooksutavad süsteemid kokku, võimaldades pahavaral märkamatult tegutseda.

Tüütu külaline teeb endale ise tagaukse võtme

Kui avastad, et midagi on valesti ja proovid pahatahtliku äpi kustutada, manab RatHat Sinu nutitelefoni ekraanile Google Play poe veateate, mis blokeerib kustutamise. Aga isegi kui sul õnnestub see eemaldada, on RatHat juba astunud sammu edasi.

Rakendusega koos paigaldati nimelt seadmesse Go Agent – iseseisev taustaprogramm, mis töötab edasi isegi siis, kui peaäpp on kadunud. Kui agent märkab, et peremees on eemaldatud, laeb selle vaikselt ja automaatselt tagasi.

Teadlased selgitavad tagaukse loogikat nii: "Go agent hangib juhtserverist FRP-tunneli seadistused, võimaldades FRP-kliendil luua operaatoriga püsiva ja aktiivse pöördtunneli."

Teab sinu PIN-koode pimesi

RatHati üks hirmuäratavamaid omadusi on selle riistvaratasemel klahvinuhk (*keylogger*). Erinevalt tavapärastest pahavaradest, mis püüavad lugeda sisestatud teksti, salvestab RatHat füüsilised puuted ekraanilehk X ja Y koordinaadid koos ajatempliga. Kuna pahavara teab täpselt, milline on telefoni klaviatuuri või mustriluku geomeetria, suudab see paljaste puutekoordinaatide põhjal PIN-koodid ja salasõnad edukalt taastada.

Mida siis teha? Ole oma nuhvliga ettevaatlik ja laadi äppe alla vaid ametlikest poodidest. Küberkurjategijate uued tööriistad on nutikamad kui kunagi varem ja traditsioonilistest turvameetmetest enam alati ei piisa.

See tehisaruga varustatud äpp vajab ekspertide sõnul omaette tähelepanu ja võib sisse juhatada uue ajastu pahavara loomises.

PLUSSID

- Erakordne püsivus: suudab end pärast kustutamist ise uuesti paigaldada.
- Geniaalne tehisaru kasutamine: navigeerib seadmes nagu päris inimene.
- Riistvaratasemel klahvinuhk: loeb paroole ekraanipuudutuste koordinaatide kaudu.

MIINUSED

- Võib tekitada kasutajatele tohutut rahalist kahju.
- Nõuab paigaldamiseks kasutaja esialgset õngeminemist.

- Uudised

- Turvalisus
- Androidiblog

Pilt