

Tisíce lacných androidov majú malvér už z výroby. Odinštalovať sa nedá

Datum 9.10.2026
Subjekt Zajtra studio spol.
Autor Lenka Ivančíková
Region Slowakei
Kategorie Elektronikindustrie, IT und Kommunikation, Sicherheit

V tisíckach lacných telefónov s Androidom je malvér už od výroby. Výskumníci rumunskej firmy Bitdefender opísali kampaň Midnight Mimosa, pri ktorej je škodlivý kód priamo súčasťou firmvéru. Podľa analýzy Bitdefender Labs je v zariadení skôr, než ho majiteľ prvý raz zapne.

Kampaň sa týka telefónov viacerých značiek postavených na čipoch MediaTek. Škodlivý komponent sa tvári ako súčasť systému, nesie všeobecný názov System a nemá ikonu. Beží so **systémovými oprávneniami**, takže bez vedomia majiteľa inštaluje a odstraňuje aplikácie, udeľuje im povolenia a spúšťa kód, ktorý mu pošle vzdialený server. Výskumníci ho našli pod názvami balíkov ako com.android.system.lite alebo com.android.sys.prot.

Zdroj: security.bloggoogle.com

Zarába na reklame, ktorú nikto nevidí

Cieľom je podľa výskumníkov najmä zárobok. Samotný komponent reklamy nezobrazuje, do telefónu však potichu nasadí krycie aplikácie, ktoré vyzerajú ako počasie, zámok aplikácií, poznámky alebo rozpoznávanie textu. Tie podľa portálu *The Record* zobrazujú skutočné reklamy v **neviditeľných oknách** nad inými aplikáciami a vedú vytvárať aj automatické kliky. Takých maskovaných aplikácií napočítali **najmenej 32**.

Aby inštaláciu nič nezachytilo, malvér pred ňou dočasne vypne Obchod Play, v ktorom beží skener Play Protect, a potom ho znova zapne. Záznam vie upraviť tak, akoby aplikácia prišla z oficiálneho obchodu. Telefóny zároveň premieňa na **uzly proxy siete**, teda na súčasť botnetu. Komponent si navyše sám zapína služby dostupnosti aj prístup k upozorneniam a žiada povolenia na SMS. Ich zneužitie výskumníci nepozorovali, operátor ho však môže spustiť na dialku.

Ktorých telefónov sa to týka

Za približne dva roky zaznamenal Bitdefender kampaň na tisíckach zariadení vo **viac než 150 krajinách**. Najviac nálezov pripadá na Mexiko, Francúzsko a Taliansko, nasledujú USA, Nemecko, Brazília a Španielsko. Slovensko medzi menovanými krajinami nie je, to ale neznamená, že sa zariadenia na náš trh dovozom zo zahraničia nedostali. Také rozloženie podľa firmy zodpovedá tovaru z **medzinárodných internetových trhovísk**, nie predaju cez operátora či národného predajcu. Jeden zo skúmaných kusov stál približne 180 dolárov.

Dva najčastejšie modely patria skutočným značkám. Označenie S200 X sa spája so značkou **Doogee** a KINGKONG X so značkou **Cubot**. Veľkú časť však tvoria neznačkové telefóny a napodobeniny, ktoré sa hlásia názvami ako S24 Ultra, S25 Ultra alebo S26 Ultra. **Skutočných telefónov Samsung**

sa to netýka, cudzie zariadenia ich názvy len kopírujú.

Stopy vedú aj do Obchodu Play

Kampaň nemá len jeden kanál. Bitdefender našiel aj **13 aplikácií v Obchode Play**, ktoré komunikujú s tými istými servermi a nesú ten istý kód na reklamné podvody. Systémové oprávnenia nemajú a ponúkajú skutočné funkcie, napríklad počasie alebo čítačku QR kódov. Reklamy však vedia zobrazovať aj mimo seba, dokonca vtedy, keď majiteľ telefón práve nepoužíva. Odstránenie jedného kanála tak nechá druhý nedotknutý.

Nemali by ste prehliadnuť:

- **Falošný AI model Plus 5.6 na stránke ChatGPT šíri malvér. Takto útok funguje**
- **Používate lacné smart okuliare? Dajú ovládnuť cez Bluetooth a útočník sa dostane k fotkám**
- **Nový malvér zneužije vašu platobnú kartu v reálnom čase. Stačí jeden telefonát**

Kto a v ktorom bode dodávateľského reťazca malvér do firmvéru vložil, Bitdefender nezistil. Časť firmvéru je podpísaná certifikátmi s menom čínskej firmy Shenzhen Zediel, podľa výskumníkov to však nedokazuje, že firma malvér vytvorila alebo o ňom vedela.

Pre majiteľov je podstatné, že **odinštalovanie nepomôže**. Vyčistenie vyžaduje zásah do firmvéru alebo vypnutie komponentu cez ADB, čo je pre väčšinu ľudí nereálne. Trvalá náprava je podľa firmy na výrobcoch a trhoviskách, ktoré takéto telefóny dodávajú a predávajú. Aj tento prípad potvrdzuje, že je dôležité kupovať telefóny z oficiálnej distribúcie a od overených výrobcov. A nie sa nechať lákať nízkou cenou a papierovými parametrami od no name značky.

Čo medzitým chystá konkurencia

Streamovacia služba Spotify už nebude len o hudbe. Do konca roka chce sprístupniť audioknihy na ďalších trhoch a novinka mieri aj k slovenským používateľom. Katalógy kníh majú pribudnúť vo vyše stovke jazykov.

Aplikácia Google Fotky dostáva vítané vylepšenie v mobilnej verzii pre Android. Videá sa po novom dajú upraviť tesne pred odoslaním, čo má pri ich zdieľaní ušetriť čas. Ide o ďalšie z radu praktických vylepšení, ktoré služba dostáva.

Xiaomi rozšírilo jazykovú podporu čínskej verzie HyperOS 4 o európske jazyky. Stalo sa tak krátko po predstavení nového systému. Zaujíma to najmä tých, ktorí si telefóny značky kupujú v zahraničí, slovenčina však medzi pridanými jazykmi chýba.

<https://www.mojandroid.sk/tisice-lacnych-androidov-maju-malver-uz-z-vyroby-odinstalovat-sa-neda>