Hlavním rizikem jsou pro mobily v Evropě trojské koně i potenciálně nebezpečná verze aplikace Telegram

24.8.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Největším rizikem na platformě Android v Evropě byly v červenci trojské koně z malware rodiny Hiddad.

- Škodlivé kódy z rodiny Hiddad po napadení zobrazují agresivní reklamy a dokážou dokonce sbírat data o zařízení.
- Bezpečnostní experti v červenci varovali také před škodlivým kódem Agent.FYA v legitimní verzi chatovací aplikace Telegram.
- Upozorňují, že i upravená legitimní aplikace může časem obsahovat malware.

Praha, 24. srpna 2026 – V červenci se škodlivé kódy pro platformu Android sice objevovaly především v Polsku, jednou z nejvíce zasažených zemí byla však i Česká republika. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET. Pozici nejčastěji detekovaných škodlivých kódů opět obsadily trojské koně z malware rodiny Hiddad. Bezpečnostní experti však tentokrát varovali i před škodlivým kódem Agent.FYA v legitimní verzi chatovací aplikace Telegram. I když takto upravená aplikace sleduje především počet stažení nebo zobrazování reklamy a není přímým rizikem pro naše uživatelská data, stává se lehce zneužitelnou do budoucna.

Malware z rodiny Hiddad zůstává dlouhodobě nejrozšířenější hrozbou pro mobilní telefony s platformou Android v Evropě. V čele pravidelné statistiky i v červenci zůstala verze tohoto malwaru Hiddad.BDM, a to stále s podílem pětiny všech zachycených škodlivých kódů v tomto měsíci. Škodlivý kód na druhém místě opět následovala verze Hiddad.BDJ. Obě verze lze zařadit mezi trojské koně, které po napadení zařízení zobrazují agresivní reklamy a dokážou dokonce sbírat data o zařízení.

„V červenci jsme v případě dvou nejčastěji detekovaných typů malwaru viděli především záplavu rozličných her a více či méně užitečných aplikací. Oba typy škodlivých kódů z malware rodiny Hiddad se nejvíce soustředí na Polsko a jejich cílem je vedle řady dalších evropských zemí bohužel i Česká republika. Útočníci je nejvíce využívali v kampaních na začátku července, Hiddad.BDJ se pak objevoval i koncem měsíce," shrnuje červencovou statistiku kybernetických hrozeb Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Kromě falešných her mohli uživatelé a uživatelky na trojského koně Hiddad.BDM narazit také ve škodlivých verzích aplikací pro předpověď počasí nebo se zdravotní tematikou (např. měření tlaku). Hiddad.BDJ pak útočníci šíří prostřednictvím tzv. cracknutých či modovaných aplikací. Kromě her to v červenci byly například i aplikace na úpravu fotografií nebo VPN zdarma.

„Cracknutá hra je neoficiálně upravená verze aplikace, ze které někdo odstranil například placení, kontrolu licence, reklamy nebo jiná omezení. Modovaná hra pak obsahuje změny, například neomezenou herní měnu, odemčené úrovně, výhody nebo herní předměty. Obvykle na takové aplikace narazíme mimo oficiální obchody s aplikacemi," říká Jirkal. „Každá takto upravená aplikace nemusí být zákonitě nebezpečná pro naše data a zařízení. Je to ale veliké riziko, protože uživatelé samozřejmě nevidí do všech změn, které v aplikaci někdo provedl, například zda do ní nepřidal

malware. Infikované aplikace malwarem z rodiny Hiddad se po instalaci navíc skryjí jako systémové, mohou nepozorovaně škodit napříč zařízením a běžní uživatelé je neodhalí. Opět se tak dostáváme k hlavnímu doporučení – stahovat aplikace a hry pouze z oficiálních obchodů a stránek s aplikacemi, které mají vlastní kontrolní mechanismy na odhalení škodlivého kódu," dodává Jirkal.

Ve škodlivou se může proměnit i legitimní aplikace

V popředí pravidelné statistiky kyberhrozeb pro platformu Android se v červenci nově objevil škodlivý kód Agent.FYA. Útoky se opět nejčastěji objevovaly na začátku měsíce, přičemž nejpostiženějšími zeměmi byly Německo, Česká republika a Polsko. Jak bezpečnostní experti upozorňují, situace je v tomto případě složitější než u malware rodiny Hiddad.

„V tomto případě došlo k pozměnění legitimní aplikace Telegram. Její autoři ji upravili tak, aby dokázala sledovat počet instalací, zobrazovaní reklam apod. Nejedná se o nijak neobvyklou aktivitu a takové chování se může objevit i v případě jiných aplikací. V tomto případě byla ale aplikace ještě upravena, aby provedené změny nešlo poznat," vysvětluje Jirkal. „V tuto chvíli aplikace nedělá nic škodlivého. Je tu však několik varovných ukazatelů. Autoři upravené aplikace jsou na rozdíl od oficiálních vývojářů platformy Telegram neznámí. Také je tato verze pro účely šíření zabalena do ochranné vrstvy, které útočníci s oblibou využívají i u škodlivých aplikací. Z našich zkušeností víme o případech, kdy útočníci přidali do takto upravených aplikací škodlivý kód až časem, typicky poté, co dosáhly nějakého počtu stažení. A protože se v tomto případě jedná o dost známou aplikaci, bude se rozhodně jednat o více než stovky stažení. S naším bezpečnostním softwarem budou ale uživatelé i před touto verzí aplikace vždy včas varováni," říká Jirkal z ESETu.

Bezpečnostní software kontroluje stahované aplikace. Program v případě, že nějakou aplikaci nebo soubor rozpozná jako nebezpečný, spustí tzv. rezidentní ochranu souborového systému, která stažení či spuštění aplikace zablokuje a umístí ji do karantény. Uživatelé jsou o tomto postupu vždy informováni samotným bezpečnostním programem.

Nejčastější kybernetické hrozby pro platformu Android v zemích EU za červenec 2026:

1. Android/Hiddad.BDM trojan (19,96 %)
2. Android/Hiddad.BDJ trojan (7,35 %)
3. Android/Spy.Agent.FYA trojan (5,86 %)
4. Android/Agent.FNM trojan (2,54 %)
5. Android/TrojanDropper.Agent.NAM trojan (2,52 %)
6. Android/Agent.FJL trojan (2,20 %)
7. Android/TrojanDownloader.Agent.BHB trojan (2,16 %)
8. Android/Agent.FTH trojan (1,78 %)
9. Android/Agent.FPB trojan (1,48 %)
10. Android/Triada trojan (1,45 %)

Uživatelé a uživatelky řešení ESET jsou před výše uvedenými typy hrozeb automaticky chráněni.

O společnosti ESET®

Společnost ESET® chrání organizace, kritickou infrastrukturu i jednotlivce a pomáhá jim budovat digitální odolnost ve světě, který stále více využívá umělou inteligenci. Díky více než 35 letům zkušeností v oblasti kybernetické bezpečnosti, více než 25 letům inovací v oblasti umělé inteligence

a 11 globálním výzkumným a vývojovým centrům vyvíjí ESET vlastní technologie určené k ochraně před kybernetickými hrozbami a k zabezpečení širšího ekosystému umělé inteligence. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně.

Na základě vědecké odbornosti a proaktivního přístupu k bezpečnosti poskytuje ESET špičkovou ochranu, která zůstává pod odborným lidským dohledem. Se sídlem v Evropské unii (Bratislava) a v soukromém vlastnictví chrání miliony uživatelů a více než 500 000 organizací ve 178 zemích světa. Společnost ESET je zavázána k odpovědnému využívání umělé inteligence a budování důvěry zákazníků. Chrání pokrok, který technologie umožňují.

Více informací

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Kontakt pro media:

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hlavnim-rizikem-jsou-pro-mobily-v-evrope-trojske-kone-i-potencialne-nebezpecna-verze-aplikace-telegram