

ESET: Kyberútočníky v srpnu nejvíce zaujala střední Evropa, své oběti lákali na výhody ve falešných mobilních aplikacích

30.9.2026 - | ESET software spol. s r.o. - Eset.com

Všechny nejčastěji detekované škodlivé kódy pro platformu Android v Evropě se tentokrát zaměřovaly především na země střední Evropy. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET. Stejně jako v předchozích letních měsících si i v srpnu udržely jednoznačnou převahu škodlivé kódy z malware rodiny Hiddad - Hiddad.BDM a Hiddad.BDJ. Opět se také objevila trojanizovaná verze aplikace Telegram, a to v případě škodlivého kódu Agent.FYA. Bezpečnostní experti varují především před stahováním aplikací mimo oficiální obchody, ať už z důvodů získat něco zdarma nebo s dodatečnými výhodami. Jak také upozorňují, škodlivé aplikace mohou figurovat i v pokročilejších útocích.

Malware z rodiny Hiddad byl hlavním škodlivým kódem pro platformu Android po celé léto. Počet srpnových detekcí pak opět potvrdil, že se útočníci prakticky celé léto nemuseli přizpůsobovat chování uživatelů a uživatelek a vystačili si jen s touto malware rodinou. Škodlivé kódy na platformě Android se šíří především prostřednictvím falešných verzí více či méně populárních mobilních aplikací.

„Podobně jako v minulých měsících byli v srpnu falešnými aplikacemi zasaženi především uživatelé a uživatelky ze střední Evropy. Škodlivý kód Hiddad.BDM se nejčastěji objevoval v Německu a Polsku, na třetím místě pak byla Česká republika. Evropské země jsou pro útočníky lákavým cílem – obyvatelstvo široce využívá digitální technologie a je zvyklé si vyhledávat různé nástroje. Stabilní počty zachycených detekcí pak mohou poukazovat také na to, že uživatelé a uživatelky v našem regionu hledají aplikace, za které nechtějí platit v oficiálním obchodě nebo jim jejich stažení poskytuje jiné výhody, například herní úpravy,“ vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Jakmile uživatelé a uživatelky upravenou verzi aplikace s malwarem Hiddad.BDM stáhnou, skryje se v zařízení jako systémová komponenta. Na ploše ji běžní uživatelé nenajdou, upozorněním pak ale může být až enormní množství vyskakujících reklamních oken.

Malware Hiddad.BDM se v srpnu opět nejčastěji skrýval v jednoduchých hrách a drobných nástrojích: skenerech QR kódů, živých mapách, seznamovacích či karetních hrách, měřicích krevního tlaku, nástrojích pro hledání telefonu tlesknutím apod.

Scénář s lákavou, ale falešnou aplikací zachytili bezpečnostní experti z ESETu také u dvou dalších nejčastějších srpnových škodlivých kódů. I v těchto případech byly cílem především země střední Evropy. Jak bezpečnostní experti poukazují, u těchto případů si již lze všimnout jasné motivace ke stažení v podobě nějaké výhody nebo bonusu.

„U druhého nejčastěji zachyceného malwaru, Hiddad.BDJ, se opět nejvíce objevovaly cracknuté nebo modifikované aplikace. Ty se tváří jako plnohodnotné originály, a navíc slibují nějaká vylepšení. Tím ale může být i škodlivý kód. U třetího nejčastěji zachyceného škodlivého kódu, Agent.FYA, byla hlavním rizikem trojanizovaná verze aplikace Telegram – modifikované, beta či premium verze zdarma, které útočníci šíří mimo oficiální obchod,“ říká Jirkal.

V případě malwaru Hiddad.BDJ se pak konkrétně objevovaly falešné verze populárních her jako Geometry Jump a Minecraft nebo aplikací Flightradar či Spotify. V případě detekce Agent.FYA pak bezpečnostní experti upozorňují, že i když se upravená aplikace Telegram zatím pravděpodobně nechová nijak nestandardně, může do ní útočník v budoucnu přidat škodlivý kód. Nahrává tomu i skutečnost, že distributor upravené aplikace je neznámý.

Bezpečnostní odborníci se často setkávají s tím, že mnoho lidí nepovažuje falešné verze mobilních aplikací za dostatečně reálnou hrozbu. Přispívá k tomu i skutečnost, že mnoho těchto aplikací obsahuje adware, který není ve srovnání s jinými škodlivými kódy, ať už ransomwarem či infostealery, stejně závažným rizikem. Neplatí to ale vždy. I adware totiž může obsahovat odkazy na nebezpečné webové stránky a falešné formuláře nebo sbírat naše údaje o chování online.

„Falešné aplikace mohou dokonce figurovat v pokročilých útocích. Příkladem je malware NGate. Útočníci ho šíří prostřednictvím falešných aplikací mimo oficiální obchody a využívají ho ke zneužití NFC technologie,“ vysvětluje Jirkal. „Scénář takového útoku začíná podvodným hovorem. Útočník oběť navede ke stažení aplikace mimo oficiální obchod s aplikacemi, která napodobuje stránky nějaké banky. Útočník ji vyzve, aby přiložila kartu k mobilu a zadala PIN. Škodlivá aplikace následně slouží jako ‚NFC přenos‘ – v okamžiku přiložení karty přenesení přečtená data do zařízení útočníka. Ten musí být ve stejný okamžik fyzicky u bankomatu nebo platebního terminálu, aby transakci provedl. Doporučení k obraně je tak jasné – nikdy neinstalujte aplikace mimo oficiální obchody. Dalším krokem by mělo být pořízení bezpečnostního softwaru i pro mobilní telefon, který kontroluje stahované aplikace a v případě rozpoznání hrozby zamezí jejímu stažení a spuštění,“ dodává Jirkal z ESETu.

Před pokročilými podvody varuje ESET společně s Českou bankovní asociací také v rámci kyberkampaně #nePINdej!, která běží od září do konce roku a dlouhodobě upozorňuje na kyberpodvody namířené na klienty tuzemských bank. Bezpečnostní experti z ESETu se podíleli také na obsahu letošního Kybertestu. Navrhli testové otázky, vysvětlení odpovědí i příklady podvodných scénářů, které vycházejí z vlastního výzkumu hrozeb.

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

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 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.

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

<https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-kyberutocniky-v-srpnu-nejvice-zaujal-a-stredni-evropa-sve-obeti-lakali-na-vyhody-ve-falesnych-mobilnich-aplikacich>