ESET: V červnu vzrostl počet zachycených falešných her s trojským koněm

28.7.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejčastějším škodlivým kódem na platformě Android v zemích EU zůstal v červnu trojský kůň Hiddad.BDM. Objevil se tentokrát ve více než pětině všech detekcí škodlivého kódu ve sledovaném regionu.

- Již druhý měsíc ho útočníci šířili prostřednictvím velmi jednoduchých a barevných mobilních her, které zároveň slouží jako domovská obrazovka telefonu – tzv. launcherů.
- Mírně vzrostly také detekce dalšího trojského koně Hiddad.BDJ. Útočníci ho nově schovali do falešné verze nástroje k úpravě fotek pomocí AI.
- Kyberbezpečnostní experti uživatelům a uživatelkám doporučují, aby ani v letních měsících nerezignovali na základy kyberbezpečnosti a pečlivě si kontrolovali, odkud aplikace stahují.

Praha, 28. července 2026 – Kybernetičtí útočníci i v červnu pokračovali v šíření trojských koní na platformě Android prostřednictvím jednoduchých mobilních her a populárních nástrojů. Počet detekcí trojského koně Hiddad.BDM, před kterým bezpečnostní experti varovali již minulý měsíc, tvořil v červnu více než pětinu všech zachycených případů škodlivého kódu. Útočné kampaně zatím také stále míří na střední Evropu – nejvíce do Polska, Německa a České republiky. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Data z letošního června potvrdila pokračující strategii útočníků na platformě Android – pro letošní letní sezonu se na uživatele a uživatelky zaměřili s novou várkou falešných her, které obsahují škodlivé kódy. Již v květnu také bezpečnostní experti nově pozorovali škodlivé verze tzv. launcherů – mobilních her, které zároveň slouží jako domovská obrazovka telefonu. V červnu jejich počet ještě narostl.

„Červnová statistika nejčastějších hrozeb pro platformu Android nám zatím potvrzuje naše očekávání, že v létě se bude škodlivý kód nejvíce šířit přes mobilní hry. Již v květnu jsme byli svědky toho, jak útočníci zapojili kromě falešných verzí klasických her i launchery, velmi jednoduché a barevné hry jako například Pillow Chase Home App či Candy Race Launcher. Útočníci je šířili především prostřednictvím trojského koně Hiddad.BDM. Podíl jeho detekcí oproti předešlému měsíci vzrostl v červnu na více než pětinu všech zachycených případů škodlivého kódu v rámci sledovaných zemí. Jeho nejčastějšími cílovými zeměmi zůstaly Polsko, Česká republika a Německo," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

V červnu rostl počet detekcí také u dalšího malwaru z rodiny Hiddad, trojského koně Hiddad.BDJ. V květnu ho útočníci ukryli do celé řady falešných aplikací – her jako Geometry Dash či Minecraft, falešných verzí populárních AI nástrojů ChatGPT či Grok nebo streamovací aplikace Spotify. V červnu se na tomto seznamu objevila i aplikace Photoroom: AI Photo Editor. Také v tomto případě mířily útočné kampaně nejvíce na Polsko, Německo a Českou republiku. Trojské koně po napadení zařízení zobrazují agresivní reklamy a dokážou dokonce sbírat data o zařízení. Ty mohou útočníci následně využít pro zacílení dalších útočných kampaní.

„Jak můžeme vidět, jakmile si nějaká legitimní aplikace či hra získá určitou popularitu mezi uživateli a uživatelkami, je pravděpodobné, že její jméno se nevyhne zneužití ve prospěch šíření škodlivých kódů. V otázce obrany pak platí pořád to stejné – stahovat nové aplikace pouze z oficiálních obchodů.

Pokud nějakou aplikaci vyhledáváme v mobilních prohlížečích, můžeme narazit na nabídky v obchodech třetích stran, kde bohužel nemáme takovou garanci bezpečnostní kontroly jako v případě oficiálních distribučních míst," dodává Jirkal.

Letní minimum digitálních návyků pro váš telefon

Letní měsíce pro nás bývají příležitostí k většímu odpočinku i cestování. Většina z nás se alespoň na chvíli nechce starat o nastavení telefonu a chce si od neustálé ostražitosti odpočinout. Úplně rezignovat na kyberbezpečnostní návyky ale experti nedoporučují.

„Vedle opravdu škodlivých aplikací můžeme narazit na řadu her a nástrojů, které sbírají o našem chování a zvycích víc dat, než doopravdy potřebují, přestože nejsou vyloženě nebezpečné a nepomáhají šířit malware. Vždy se snažíme uživatelům a uživatelkám vysvětlovat, že osobní data jsou jejich majetkem podobně jako peníze nebo úspory. Když si toto uvědomíme, úplně nám to změní pohled na to, jak s nimi zacházíme. Jedním z kroků, který může významně pomoci k ochraně našich dat, je zamyslet se, jestli opravdu nějakou aplikaci potřebuji do svého telefonu stahovat a povolit jí tak přístup k dalším položkám v našem zařízení, včetně dokumentů, fotek a videí. Kolik aplikací máme v telefonu, a přitom jsme je stáhli jen ze zvědavosti a použili jen párkrát? Pokud opravdu nějakou aplikaci chcete nebo potřebujete, povolte jí jen nezbytná oprávnění pro její fungování. Pokud ji delší dobu už nepoužíváte, odinstalujte ji," radí Jirkal z ESETu.

Aby uživatelé a uživatelky nemuseli v létě řešit nepříjemnosti spojené s kyberbezpečnostními hrozbami, doporučují experti kromě stahování aplikací z oficiálních zdrojů provést například i zálohu obsahu telefonu pro případ, že bychom jej ztratili nebo nám ho někdo odcizil. Základem je také telefon co nejpravidelněji aktualizovat, a to jak operační systém, tak jednotlivé aplikace.

Bezpečnostní software je pak dalším krokem, který nám s řadou kontrol pomůže. Moderní bezpečnostní řešení dnes obsahují také například virtuální privátní síť VPN pro zajištění většího soukromí při procházení internetu, nebo funkci Anti-Theft, která telefon v případě ztráty či odcizení pomůže lokalizovat a v krajním případě i na dálku vymazat.

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

1. Android/Hiddad.BDM trojan (21,19 %)
2. Android/Hiddad.BDJ trojan (8,82 %)
3. Android/Spy.Agent.FYA trojan (7,34 %)
4. Android/Agent.FNM trojan (6,15 %)
5. Android/TrojanDropper.Agent.JHA trojan (1,99 %)
6. Android/Agent.FJL trojan (1,65 %)
7. Android/TrojanDownloader.Agent.BHB trojan (1,59 %)
8. Android/Triada trojan (1,51 %)
9. Android/Andreed trojan (1,48 %)
10. Android/TrojanDropper.Agent.NAM trojan (1,47 %)

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

O společnosti ESET

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení digitální bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé

inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

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, v podcastu RESET 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/eset-v-cervnu-vzrostl-pocet-zachycenych-falesnych-her-s-trojskym-konem