ESET: S příchodem léta zaplavují Česko falešné mobilní hry

24.6.2026 - Lucie Mudráková | ESET software

Praha, 24. června 2026 – Nejčastějšími typy nebezpečných aplikací, kterými se šíří škodlivé kódy na platformě Android, byly v květnu opět především mobilní hry. Vyplývá to z analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET. Útočníci tentokrát zvolili falešné verze tzv. launcherů, aplikací a her, které zároveň plní funkci domovské stránky na vašem telefonu. Bezpečnostní experti také upozorňují, že útočníci nově volili jednoduché a velmi barevné hry, pravděpodobně s účelem co nejvíce přilákat nejmladší uživatele a uživatelky. Před odjezdem na dovolenou proto doporučují věnovat náležitou pozornost zabezpečení telefonu a základy kyberbezpečnosti předat také dětem.

Nejrozšířenějšími typy škodlivých kódů pro platformu Android byly v květnu trojské koně z malware rodiny Hiddad. Jsou například známé tím, že po napadení zobrazují agresivní reklamy, a dokážou dokonce sbírat data o zařízení. Ty mohou útočníci následně využít pro zacílení dalších útočných kampaní.

„V květnu jsme na platformě Android opět pozorovali nárůst detekcí škodlivých kódů, které útočníci maskují za různé hry a populární aplikace. Stojíme přitom před letní, prázdninovou sezonou, kdy útočníci počítají s tím, že budeme hledat nějaké aplikace k odreagování, které nám zkrátí čekání na letišti nebo zabaví děti," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „Trojské koně z rodiny Hiddad se v květnu zaměřily na střední Evropu, včetně České republiky. Zejména v případě škodlivého kódu Hiddad.BDM jsme viděli, jak útočníci zneužívali jednoduché, barevné hry, aby pravděpodobně přilákali právě děti. S nadcházejícím létem bych je proto doporučoval seznámit se základy kybernetické bezpečnosti a vysvětlit jim, na co mohou narazit při stahování aplikací," dodává Jirkal.

Trojský kůň Hiddad.BDM útočníci v květnu nejčastěji vydávali za tzv. launcher, typ mobilní hry, která zároveň slouží jako domovská obrazovka telefonu. Jednalo se například o aplikace Yoga Flex Home App, Pillow Chase Home App či Candy Race Launcher. Hlavním cílem útočníků bylo v tomto případě Polsko, následováno Českem a Slovenskem. V případě trojského koně Hiddad.BDJ útočníci zvolili cracknuté populární hry jako Geometry Dash či Minecraft, sáhli tentokrát ale také po falešných verzích populárních AI nástrojů jako ChatGPT či Grok nebo streamovací aplikace Spotify. I v tomto případě bylo cílem především Polsko, které následovalo Německo a opět Česká republika.

Bezpečný chytrý telefon o prázdninách

Ať už vezmeme v létě mobilní telefon na deku k rybníku, k moři, pod stan nebo na festival, kyberbezpečnostní experti doporučují věnovat ochraně dat speciální pozornost. Útočníci s touto sezonou při přípravě svých kampaní počítají a své strategie jí přizpůsobují. Moc dobře vědí, že budeme mít víc času na oddychové aktivity a možná budeme chtít také zahnat nudu.

„Kromě svých obvyklých doporučení bych v tomto období častějšího cestování a volnočasových aktivit telefon co nejpravidelněji aktualizoval a provedl zálohu dat. Telefon můžeme ztratit, nebo nám ho může někdo odcizit. Nejen z tohoto důvodu bych si pak také zkontroloval, zda máte u všech účtů, kde to jde, zapnuté dvoufázové ověření, které přihlášení chrání i v případě, že útočník získá vaše heslo. Doporučil bych tady pořízení bezpečnostního softwaru, protože řada těchto moderních řešení má například už i funkci Anti-Theft. V případě, že o telefon přijdete, jej pomůže lokalizovat a v

krajním případě i telefon na dálku vymazat," říká Jirkal.

Bezpečnostní experti také dále radí příliš se nespoléhat na veřejné Wi-Fi sítě. Nejen na letištích, ale také v hotelech či kavárnách nebývá internetové připojení dostatečně šifrované, a proto bychom se v těchto případech měli omezit pouze na prohlížení nedůležitých informací. Naopak bychom se měli vyhnout přihlašování do našich účtů či zadávání údajů z platební karty.

„Větším dětem, které mají třeba už svůj první mobilní telefon, bych vysvětlil, na co si dávat pozor při stahování aplikací. Zásadní je stahovat aplikace pouze z oficiálního obchodu, i tam je ale zapotřebí určitá obezřetnost. Můžete si to projít s nimi, a zároveň jim u toho ukázat, čeho si všímat. Za zvážení stojí i nástroje rodičovské kontroly, které vám pomohou ohlídat, co děti do telefonu stahují. Přesto bych doporučoval se s dětmi na pravidlech vzájemně domluvit. U nás doma například platí, že se nebudou stahovat hry, které mají málo recenzí a špatná hodnocení. Právě škodlivé launchery, které jsme sledovali u trojského koně Hiddad.BDM, podmiňovaly dohrání hry udělením dobrých recenzí. Ve slovním hodnocení se ale můžete setkat s informacemi od uživatelů, že je k tomu hra donutila. Rozhodně je proto důležité číst celé recenze a neřídit se jen počtem hvězdiček," dodává Jirkal z ESETu.

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

1. Android/Hiddad.BDM trojan (12,55 %)
2. Android/Hiddad.BDJ trojan (12,21 %)
3. Android/Agent.FNM trojan (7,77 %)
4. Android/TrojanDropper.Agent.NAM trojan (3,02 %)
5. Android/TrojanDownloader.Agent.BHB trojan (2,81 %)
6. Android/Triada trojan (2,18 %)
7. Android/Andreed trojan (1,89 %)
8. Android/TrojanSMS.FakeInst trojan (1,57 %)
9. Android/Spy.Banker.BGB trojan (1,55 %)
10. Android/TrojanDropper.Agent.NEH trojan (1,44 %)

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-s-prichodem-leta-zaplavuji-cesko-falesne-mobilni-hry