Přehled hrozeb pro Android: Zdrojem škodlivého kódu byly letos v létě nejčastěji mobilní hry

20.9.2023 - Lucie Mudráková | ESET software

Mobilní hry i v srpnu zůstaly hlavními zdroji škodlivých kódů pro chytré telefony v Česku. Jejich prostřednictvím se tentokrát šířily všechny nejčastěji detekované hrozby, včetně trojského koně Hiddad – jeho detekce v srpnu opět vzrostly, tentokrát téměř na třetinu všech případů. Trojský kůň Hiddad se tak letos v létě stal hlavním představitelem kybernetických hrozeb pro zařízení s operačním systémem Android. Vyplývá to z pravidelné statistiky od společnosti ESET.

Trojský kůň Hiddad v srpnu znovu posílil téměř na třetinu všech detekovaných případů v Česku. Dle očekávání tak útočníci i letos využili letních prázdnin a škodlivé kódy si našly cestu k českým uživatelům v době, kdy trávíme na telefonu nejvíce času.

„Vyšší detekce u trojského koně Hiddad pozorujeme od letošního května. Nejde však o nic neobvyklého. Také srpnová statistika potvrzuje naše dlouhodobé pozorování situace na platformě Android – v létě čeští uživatelé potřebují celou řadu aplikací, od her, se kterými tráví svůj volný čas, až po aplikace k cestování nebo ke sportu. A toho samozřejmě kybernetičtí útočníci rádi využijí," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Na trojského koně Hiddad uživatelé stále nejčastěji narazí v různých hrách, které využívají popularitu Minecraftu, ať už se jedná o hry s jiným jménem, ale stejným principem hry, anebo o zcela jiné hry, které využívají jen fotky s ukázkami hry Minecraft. V srpnu se jednalo například o falešnou verzi hry Craft Rain Fun Castle.

Škodlivý kód se šířil také prostřednictvím upravené verze hry LIMBO, a to konkrétně adware Andreed. Ten se dále objevil i v upravené verzi programu Google Chrome. Adware jako typ kybernetického rizika zobrazuje množství agresivních reklamních oken, má negativní vliv na výkon a výdrž zařízení a v konečném důsledku může uživateli zobrazit odkaz na nebezpečné webové stránky.

V posledních měsících mohou ale uživatelé v Česku narazit také na malware Spin.Ok, který má funkce spywaru. V srpnu se nejvíce šířil prostřednictvím her Tower Raider: FAST & FUN APP nebo Emoji Blox.

Na kybernetické hrozby pro platformu Android narazí čeští uživatelé nejčastěji právě ve falešných verzích populárních aplikací. Společným znakem hrozeb pro tuto platformu je také to, že nebezpečné aplikace si uživatelé většinou stáhnou sami a dobrovolně.

„Na základě našich zkušeností bývá motivem pro stažení nebezpečné aplikace nějaká výhodná nabídka a její popularita mezi uživateli. Právě oblíbené aplikace, které navíc mohou být nějak zpoplatněné, jsou v obchodech třetích stran a na internetových úložištích hledaným zbožím, a to jak pro dospělé fanoušky, tak pro uživatele z řad dětí. Pro ty může být hra zdarma nebo výhodný balíček softwaru obzvlášť velkým lákadlem," říká Jirkal.

Bezpečnostní specialisté uživatelům opakovaně doporučují rizika spojená se stahováním her nepodceňovat. Hrozby pro platformu Android se velmi rychle vyvíjí a útočníci navíc velmi dobře znají

chování uživatelů. Ti by měli zvážit stahování programů a her mimo oficiální obchod Google Play.

„Uživatelé by měli zůstávat ostražití a sledovat aktuální rizika nejen pro své počítače a notebooky, ale i pro své chytré telefony, které počítače již v celé řadě disciplín směle nahradí. Právě i z tohoto důvodu by uživatelé neměli ani v případě smartphonů zapomínat na bezpečnostní program. Zvlášť zvýšenou pozornost bych věnoval zařízením nejmenších uživatelů. Děti totiž nemusí ještě zcela chápat všechny souvislosti rizik na internetu a bezpečnostní program včas zachytí nejen pokročilé hrozby, ale také potenciálně nechtěné aplikace včetně nebezpečného adwaru nebo podvodné webové stránky," dodává Jirkal z ESETu.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/prehled-hrozeb-pro-android-zdrojem-skodliveho-kodu-byly-letos-v-lete-nejcasteji-mobilni-hry