Přehled hrozeb pro Android: Falešné hry Českem stále šíří adware a bankovní malware

24.7.2024 - Lucie Mudráková | ESET software

Statistika kybernetických hrozeb pro platformu Android v Česku i v červnu zůstala neměnná. Největším rizikem je nadále adware Andreed, který v minulém měsíci znovu o něco posílil.

Také v případě bankovního malwaru Cerberus, který se v Česku znovu začal objevovat od letošního jara, zůstávají detekce stabilní. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET. Falešné verze mobilních her jsou i nadále oblíbeným nástrojem kybernetických útočníků při šíření škodlivých kódů nejen v Česku. Bezpečnostní experti proto opakovaně varují před stahováním aplikací a her mimo oficiální obchody s aplikacemi pro chytré telefony.

Ani v červenci se pravidelný přehled kybernetických hrozeb pro platformu Android nezměnil a na předních místech statistiky se stále drží adware Andreed a bankovního malware Cerberus. Adware navíc oproti předchozímu období v červnu zase o něco posílil. Ačkoli se neřadí mezi vysoce nebezpečné škodlivé kódy, jako je například ransomware nebo spyware, i adware může sledovat naše chování na internetu a prostřednictvím velkého množství zobrazované reklamy nás přesměrovat na nebezpečné webové stránky se škodlivým či podvodným obsahem.

„Adware Andreed zatím neochvějně zůstává největším kybernetickým rizikem pro chytré telefony s platformou Android. Každý měsíc se šíří prostřednictvím jiných mobilních her. Na tyto aplikace uživatelé a uživatelky narazí nejčastěji v obchodech třetích stran a jedná se zpravidla o falešné a nelegitimní verze známých předloh, které jsou na těchto místech nabízeny za výhodných podmínek či zcela zdarma. Hra může fungovat bez problémů, její součástí je ale adware. Ten pak může zobrazovat agresivní reklamu, zpomalovat chytrý telefon nebo stahovat další škodlivé kódy," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

V červnu bezpečnostní specialisté objevili adware Andreed nejčastěji ve verzi hry Flower Girls Tamagotchi Anime. Častými zdroji adwaru mohou být i verze her se závodní tématikou či strategické hry.

Již před několika měsíci se do Česka znovu vrátil bankovní trojský kůň Cerberus. Mezi detekcemi se objevil také v červnu. I tento malware útočníci šíří prostřednictvím různých verzí herních aplikací. V červnu to byla již dříve detekovaná hra Fast Car Driving - Street City nebo verze kulečníkové hry Pool Stars.

„Uživatelé a uživatelky mohou být někdy v případě varování před adwarem lehkovážnější, protože ho nepovažují za vážnou kybernetickou hrozbu. Rozhodně by ale neměli podceňovat riziko stahování her mimo oficiální obchody s aplikacemi. Jak můžeme totiž vidět, falešné verze her útočníci využívají i v případě šíření bankovního malwaru. A ten již rozhodně nechcete mít ve svém zařízení," říká Jirkal.

Bankovní malware i adware doplnil v červnu trojský kůň Agent.HQS, který se ve větším počtu detekcí objevil již letos v březnu. Stále se vydává především za pirátskou kopii aplikace MX Player. Šíří se v podobě tzv. dropperu, škodlivého kódu, který funguje jako obálka a škodlivý obsah tak skrytě doručí do cílového zařízení. Podle posledních zjištění bezpečnostních specialistů existuje možnost, že se šíří prostřednictvím sítě Telegram.

Návrat bankovního malwaru do Česka a jeho několikaměsíční stabilní přítomnost svědčí podle bezpečnostních expertů o tom, že zvolené strategie útočníků jsou zatím úspěšné. Bankovní trojský kůň je rizikem především pro internetové bankovnictví, nikoli pro samotné bankovní aplikace. I ty by měli uživatelé stahovat ale výhradně z oficiálního obchodu Google Play.

„Bankovní malware Cerberus má několik funkcionalit typických pro tento typ hrozby. V napadeném zařízení dokáže kontrolovat SMS zprávy a zaznamenávat stisky kláves na klávesnici. Sbírá informace o kontaktech, poloze, aplikacích a další údaje z chytrého telefonu. S ohledem na to, že se jedná o již pokročilejší typ hrozby, bych uživatelům rozhodně doporučil využívat bezpečnostní software, který dokáže bankovní malware včas rozpoznat a funguje také jako včasná prevence před jeho různými variantami," dodává Jirkal z ESETu.

Moderní bezpečnostní řešení dnes uživatelům nabízejí mimo zabezpečení před škodlivými kódy i řadu dalších praktických nástrojů. Jedním z nich je například správce hesel, který poskytuje bezpečné a šifrované uchovávání přihlašovacích údajů a automaticky hesla doplňuje při přihlášení do našich online účtů. Uživatelé a uživatelky mají možnost využívat také virtuální privátní síť, VPN, která pomůže zajistit zabezpečené a soukromé prohlížení internetu.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete 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.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

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 řešení od 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-falesne-hry-ceskem-stale-siri-adware-a-bankovni-malware