Přehled hrozeb pro Android: Neoficiální verze her mohou ohrozit bankovní účty v Česku

29.8.2024 - | ESET software

Statistiku kybernetických hrozeb pro platformu Android v Česku v červenci vedl opět adware Andreed, který se dlouhodobě šíří prostřednictvím falešných mobilních her.

Objem jeho detekcí ale mírně klesl. Na předních příčkách zůstává také nebezpečný spyware. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET. Bezpečnostní experti varují před stahováním aplikací a her mimo oficiální obchody s aplikacemi.

Nejčastěji detekovanou hrozbou v Česku zůstává malware Andreed. Jedná se o adware, který v zařízení uživatele zobrazuje nevyžádanou reklamu. Na druhé a třetí příčce se umístily spyware Cerberus a malware Agent.HQS, který dokáže šířit další škodlivé kódy. Uživatelé si škodlivý kód nejčastěji stáhli nevědomky sami, a to v aplikacích z neoficiálních zdrojů.

„Adware uživatelé často nepovažují za příliš závažný problém. Já bych jej ale nepodceňoval. Malware jako je Andreed zahltí váš telefon nevyžádanou reklamou. Telefon bude pomalý a prakticky nepoužitelný. Navíc inzeráty, které adware zobrazuje, často odkazují na phishingové stránky nebo ke stažení dalšího, mnohem nebezpečnějšího škodlivého kódu," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Detekce adwaru Andreed v červenci oproti předchozímu období mírně oslabily. Podle expertů to není překvapivé. Reklamní škodlivý kód se držel na předních příčkách od začátku roku, je tedy pravděpodobné, že už je pro jeho tvůrce velmi složité obcházet se současnou verzí adawaru bezpečností aplikace. Ještě v červnu byl tento adware přitom na svém maximu. Důvodem může být i to, že si uživatelé před prázdninami stahovali hry na dovolené. Nejčastěji se šíří v neoficiálních verzích her, především pak ve hře Car Factory Simulator.

V červenci vzrostl objem detekcí v případě malwaru Agent.HQS. Na začátku roku byl přitom detekován v menším počtu případů, větší aktivitu zachytili analytici až v březnu, a také předešlý měsíc. Útočníci jej šíří v pirátské kopii aplikace MX Player, a to pravděpodobně prostřednictvím sociálních platformy Telegram. Jedná se o tzv. dropper. Tento typ malwaru funguje jako obálka: když si uživatelé nainstalují infikovanou aplikaci, obálka se rozbalí a s ní se nainstaluje i nějaký další škodlivý kód.

Podoba dropperů se rychle proměňuje a útočníci mohou škodlivý kód vydávat prakticky za jakoukoli aplikaci. Běžné jsou například škodlivé kódy, které z telefonu sbírají přihlašovací údaje, které je možné na černém trhu velmi lukrativně prodat.

Dlouhodobě patří mezi nejvážnější rizika pro mobilní zařízení s platformou Android bankovní malware Cerberus. V detekční datech se co do počtu případů stabilně drží na stálých hodnotách. Objem jeho detekcí nicméně od června mírně slábne.

„Menší počet detekcí bankovního trojského koně Cerberus nemusí být dobrá zpráva. Je zcela běžné, že během letních měsíců se pozornost útočníků zaměří na jiný typ malwaru, zkoušejí nové kampaně a postupy, jak obcházet bezpečnostní aplikace. Situaci monitorujeme a vývoj tohoto škodlivého kódu ukáží další měsíce," dodává Jirkal.

Trojský kůň Cerberus se v červenci šířil prostřednictvím falešných mobilních her, například v

závodním simulátoru Fast Car Driving – Street City. Představuje riziko především pro internetové bankovnictví, nikoli pro samotné bankovní aplikace. 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.

Všechny uvedené hrozby si většinou do zařízení stáhne uživatel nevědomky sám. Zdrojem malwaru jsou totiž převážně aplikace z neoficiálních zdrojů, typicky ze sociálních sítí, fór nebo z neoficiálních a pochybných internetových obchodů s aplikacemi. Často si je ale stáhneme i my sami po kliknutí na nějakou reklamu.

„Uživatelům bych na tomto místě poradil, aby si své aplikace vybírali pečlivě a stahovali je jen na Google Play. To je totiž pro platformu Android jediný oficiální zdroj. Tento obchod všechny aplikace kontroluje a aktivně v nich škodlivé prvky vyhledává, to se samozřejmě o diskuzních fórech nebo veřejných úložištích nedá říct. Nenechte se zlákat tím, že je drahá aplikace někde ke stažení zdarma nebo že je na internetu v beta verzi nová hra. To vše bývají triky podvodníků, jak vás ke stažení infikované aplikace nalákat," radí Jirkal z ESETu.

Přítomnost malwaru v chytrém telefonu nemusíme na první pohled poznat. Někdy falešná hra skutečně funguje, jen v pozadí běží škodlivý kód, který například začne s odstupem času zobrazovat reklamu nebo sbírat vaše hesla. Proto bezpečnostní experti doporučují nainstalovat si i do chytrého telefonu bezpečnostní program, který podezřelé chování odhalí. Moderní řešení nabízejí i řadu dalších funkcí, které v důsledku chrání vaše data. 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 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 výzkumná a 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-neoficialni-verze-her-mohou-ohrozit-bankovni-ucty-v-cesku