Největším rizikem zůstává i závěrem roku adware a škodlivý kód s funkcemi spywaru

13.1.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Také v listopadu zůstal nejčastěji detekovaným škodlivým kódem pro platformu Android v Česku adware Andreed.

Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET. Bezpečnostní experti ho nadále detekují ve zhruba šestině všech zachycených případů pro tento operační systém. Adware v zařízení zobrazuje především škodlivou a agresivní reklamu, která může uživatele potenciálně zavést na nebezpečné webové stránky. Nadále ho doplňuje také malware Spy.SpinOk, který útočníci šíří jako softwarový doplněk pro vývojáře a může být tak ve velkém množství oficiálních i upravených verzí aplikací.

Bezpečnostní specialisté z ESETu odhalili v listopadu řadu neoficiálních verzí aplikací, prostřednictvím kterých útočníci šíří v případě platformy Android škodlivé kódy. Kromě her, které jsou u útočníků dlouhodobě v největší oblibě, byly v listopadu rizikem i aplikace pro stahování hudby či videí nebo dokonce volnočasová aplikace, která má pořízením snímku dlaně uživatelům předpovědět budoucnost.

„Aktuální škodlivé kódy pozorujeme na platformě Android průběžně celý podzim. Uživatelé se mohou setkat s řadou různých aplikací, a to jak s neoficiálními, falešnými verzemi, tak s legitimními aplikacemi, které mohou obsahovat škodlivou knihovnu s nebezpečným kódem. A zatímco adware Andreed pozorujeme stále především v různých hrách, je to právě malware Spy.SpinOk s funkcemi spywaru, který může být ve velkém rozšířený v aplikacích všeho druhu. Autoři škodlivého kódu mohou vývojářům nabízet Spy.SpinOk ve formě modulu jako marketingový doplněk, takzvaný Software Development Kit, SDK. V aplikacích se pak takový doplněk projevuje jako nějaká minihra nebo losování o ceny," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Adware Andreed se v listopadu objevil nejčastěji ve verzích her Tiny Space Program nebo Mini Ninjas, nebo také v modifikaci pro hru Terraria. V aplikaci pro výklad z dlaně pak bezpečnostní specialisté objevili trojského koně Hiddad. Malware Spy.SpinOk se nejčastěji objevoval ve zmíněné aplikaci pro stahování hudby a videí.

Škodlivý kód Spy.SpinOk se v Česku začal na předních místech statistiky pro platformu Android objevovat od letošního června. Vzhledem k tomu, že útočníci šíří tento malware jako doplněk pro vývojáře aplikací, mohou být aplikace s tímto typem hrozby rozšířeny mezi uživateli ve velkém.

„Sami vývojáři si nemusí být škodlivostí doplňku, který použili, vědomi. Proto je v případě stahování aplikací na místě opatrnost. Uživatelé by si v první řadě měli vždy položit otázku, zda danou aplikaci opravdu potřebují a zda ji budou dlouhodobě využívat. Pro stahování bych vždy vybral oficiální obchod, v případě platformy Android tedy Google Play. I tam sice mohou uživatelé narazit na škodlivý kód, riziko je ale s ohledem na bezpečnostní kontroly daleko menší, než na veřejných úložištích nebo v méně známých obchodech," doporučuje Jirkal.

Spy.SpinOk je typem malwaru, který má provádět v zařízeních obětí špionáž. Dokáže shromažďovat informace o souborech v napadeném zařízení a následně je odesílat útočníkům. Jeho prostřednictvím mohou útočníci také zkopírovat či nahradit dočasný obsah uložený ve schránce zařízení.

Kromě bezpečnostního řešení, které je v případě spywaru nejspolehlivější ochranou pro naše data a soukromí na internetu, bezpečnostní experti také doporučují procházet před samotným stahováním uživatelské recenze, které na problém s aplikací většinou spolehlivě upozorní.

„Čísla v našich statistikách nám jasně ukazují, že schovat škodlivý kód do nějaké hry nebo jiné populární aplikace funguje a útočníkům se to vyplácí. Někteří útočníci to dělají i tak, že si již kompletně naprogramovanou hru koupí od samotných vývojářů, kteří je nabízí prakticky komukoliv a jejich cena není vysoká. Útočníci si pak do hry přidají svůj kód, změní její ikonu a prodají ji dál. Samozřejmě si ale hru mohou sehnat i jinou cestou a upravit ji do podoby škodlivé verze bez zdrojových kódů. Na nebezpečnou aplikaci tak opravdu může narazit každý z nás," dodává Jirkal z ESETu.

Bezpečnostní program ochrání mobilní telefon nejen před spywarem a potenciálně nechtěnými aplikacemi (tzv. PUA), ale nabízí již dnes celou řadu dalších nástrojů. Součástí kvalitního bezpečnostního řešení může být také správce hesel pro bezpečné uchovávání našich přihlašovacích údajů, pro které je největším nebezpečím právě spyware, nebo virtuální privátní síť VPN pro zabezpečené a soukromé prohlížení internetu.

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-nejvetsim-rizikem-zustava-i-zaverem-roku-adware-a-skodlivy-kod-s-funkcemi-spywaru