# Přehled hrozeb pro Android: Adware doplnil v listopadu dropper v podobě falešné modifikace pro Roblox

**7.1.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software**

**Ačkoli ještě v říjnu bezpečnostní experti zaznamenali v Česku větší příliv falešných verzí her různých žánrů, v listopadu evidovali na platformě Android v Česku výraznější útlum v počtu škodlivých kódů. Dlouhodobě přítomný adware Andreed se objevil pouze v desetině všech zachycených případů. Tentokrát na sebe spíše upozornil škodlivý kód typu dropper, který útočníci vydávali za herní modifikaci pro platformu Roblox. Ukrýval trojského koně Agent.GKE. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v České republice od společnosti ESET.**

Bezpečnostní experti v listopadu zaznamenali pokles aktivity u nejčastěji detekovaného škodlivého kódu pro platformu Android v Česku, adwaru Andreed. Z téměř pětiny všech případů klesly v listopadu detekce na desetinu. Naposledy se této hranici adware Andreed přiblížil letos v srpnu.

„Zatímco v říjnu jsme pozorovali celou paletu různých falešných her, kterými se šířily hrozby pro platformu Android, v listopadu se počet detekcí znatelně snížil, především v případě adwaru Andreed. Takové kolísání jsme pozorovali již během roku. Většinou to značí, že útočníci věnují čas zvážení dalších strategií anebo že se setkáme s nějakým novým typem hrozby, který uživatelé ještě neznají," komentuje poslední výsledky pravidelné statistiky Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Co se prozatím v listopadu nezměnilo, je způsob šíření malwaru – stále jsou to převážně falešné hry nebo falešné herní modifikace, a to nejen v případě adwaru Andreed. Bezpečnostní experti v listopadu takto odhalili především falešné verze her Bad Piggies nebo Bike Race Pro. Ve falešné herní modifikaci pro populární platformu Roblox se pak ukrýval trojský kůň Agent.GKE.

„Také v listopadu se opět setkáváme s velmi běžnou hrozbou na platformě Android, kterým je škodlivý kód typu dropper. Ten ukrýval již zmíněného trojského koně Agent.GKE. Droppery útočníci využívají proto, že jedním škodlivým kódem vlastně zamaskují další. Dropper si můžete představit jako obálku, která v sobě schová další malware. Právě proto na sebe droppery často berou podobu her. Útočníci vědí, že uživatelé hry, které jsou navíc nějak finančně výhodnější, zcela zdarma nebo jinde nedostupné, rádi stáhnou. Rizikem jsou především v méně známých obchodech třetích stran. Proto bych uživatelům rozhodně doporučil stahovat aplikace pouze z důvěryhodných a oficiálních zdrojů, například z obchodu Google Play," vysvětluje Jirkal.

Kromě her nebo aplikací známých a zvučných značek útočníci zneužívají i bankovní aplikace nebo řadu zábavných nástrojů. V listopadu byly mezi takovými aplikacemi například tzv. word blender, nástroj k zamíchání existujícího textu a tvorbě nového obsahu, aplikace pro počítání slov v textu, rozmazávání obrázků nebo encyklopedie pokojových rostlin. Všechny tyto škodlivé verze aplikací přitom byly propojeny se zařízením útočníka a čekaly na jeho příkazy, jakmile by si je uživatelé stáhli do svých zařízení. Ukrývaly škodlivý kód FakeApp.AHS.

„Všechny hrozby pro platformu Android se nemusí jevit jako zvlášť závažné, když se nejedná o ransomware nebo špionážní program. I adware přitom může sledovat, co na internetu děláme nebo co vyhledáváme. Kromě zabezpečení pomocí profesionálního programu, který odhalí celou řadu

potenciálně škodlivých aplikací i webových stránek, bych pak uživatelům rozhodně doporučoval, aby vždy zvážili, zda aplikaci, kterou si vyhlídli ke stažení, skutečně potřebují. Kromě toho, že tak sníží riziko nákazy malwarem, se mohou vyhnout i nadměrnému sběru dat ze strany aplikací. Před stažením by také měli věnovat pozornost hodnocení aplikace, důvěryhodnosti a renomé jejího vývojáře nebo zda neměla v poslední době nějaké bezpečnostní problémy. Právě na to, že tohle všechno ve spěchu před stažením aplikace neuděláme, útočníci sází," dodává Jirkal z ESETu.

Pokud je webová stránka, na kterou se adware snaží uživatele přesměrovat, na seznamu podvodných a nebezpečných stránek, bezpečnostní program k ní zablokuje přístup. Uživatelům se pak objeví varování s informacemi, proč je webová stránka blokována. Program také v případě, že nějakou aplikaci nebo soubor detekuje jako nebezpečné, zapne při jejich stažení či spuštění detekci rezidentní ochranou souborového systému. Tato funkce stažení nebo spuštění zablokuje a přesune nebezpečný objekt do karantény, o čemž je uživatel opět informován.

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.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/prehled-hrozeb-pro-android-adware-doplnil-v-listopadu-dropper-v-podobe-falesne-modifikace-pro-roblox