Hrozby pro Android: Lidé nechtějí platit za prémiové služby, zneužívají toho hackeři

6.5.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

V březnu se na první příčce statistiky kyberhrozeb pro platformu Android objevil trojský kůň Agent.GKE. Počet jeho detekcí od minulého měsíce výrazněji narostl a podle bezpečnostních expertů máme co do činění s velmi úspěšnou útočnou kampaní. Útočníci jej vydávají za škodlivou modifikaci pro aplikaci Spotify, která slibuje možnost bezplatné aktualizace na prémiovou verzi. Nejvíce se v březnu objevoval ve Španělsku, Polsku a v České republice. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Bezpečnostní experti varují před trojským koněm Agent.GKE již od začátku letošního roku. A jak také potvrdila březnová detekční čísla, stále by uživatelé tuto hrozbu neměli podceňovat.

„Zatímco v lednu a únoru jsme trojského koně Agent.GKE detekovali zhruba ve třech procentech všech zachycených kybernetických hrozeb pro platformu Android, v březnu už počet všech zachycených případů vzrostl na více než 7 procent. Z tohoto pohledu je bohužel patrné, že se jedná o úspěšnou útočnou kampaň, a to i díky posledním změnám ze strany platformy Spotify. Ta v nedávné době upravila svou aplikaci tak, aby placenou verzi nešlo tak snadno obcházet. Pro řadu uživatelů a uživatelek to ale evidentně znamená porozhlédnout se po jiných, neoficiálních možnostech," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce ESET.

Podle bezpečnostních expertů stahují uživatelé z neoficiálních internetových stránek a fór škodlivou modifikaci pro aplikaci Spotify, která slibuje možnost bezplatné aktualizace na prémiovou verzi. Po stažení a spuštění této modifikace ale nakazí svá zařízení zmíněným trojským koněm Agent.GKE. Nejvíce případů zachytili na začátku března, přičemž nejvíce zasaženými evropskými zeměmi bylo Španělsko, Polsko a Česká republika.

„Trojský kůň Agent.GKE je podobně jako ostatní škodlivé kódy na platformě Android rizikem pro naše data, která uchováváme ve svých chytrých telefonech. A ukládáme jich tam čím dál tím více v souvislosti s tím, jak své telefony využíváme ke stále většímu počtu činností a aktivit. Škodlivé kódy mohou často do zařízení stáhnout další malware, jako jsou třeba spyware nebo bankovní trojské koně. I když se na první pohled nemusí toto riziko zdát příliš velké, uživatelé by jej neměli podceňovat. Úspora peněz, která je velmi často motivací k tomu stáhnout nějakou pochybnou verzi aplikace či nějaké doplňky k ní, je opravdu jen zdánlivá. Zaplatíme za to svými daty, která mají nezanedbatelnou cenu například na černém trhu," říká Jirkal.

Ačkoli je dlouhodobě přední hrozbou pro platformu Android, v březnu adware Andreed mírně oslabil. Největším rizikem byl tentokrát především v Německu a Polsku. Nejčastěji jej uživatelé tentokrát stahovali ve falešné verzi hry StudyGe – World Geography Quiz anebo v podobě škodlivých cheatů pro populární hru GTA.

„Právě po herních cheatech je podobně jako po aplikacích mezi uživateli poptávka, protože jim mohou usnadnit hru nebo získat ve hře výhody. Opět tak útočníci velmi dobře předvídají naše chování a mají přehled o tom, co vyhledáváme," doplňuje Martin Jirkal.

Trojský kůň Agent.EQD se v březnu nadále nejčastěji objevoval ve falešné verzi aplikace Swing VPN. Stále zůstává hrozbou především pro naše německé sousedy.

„Uživatelé a uživatelky by se měli vyhnout stažení adwaru i z toho důvodu, že jej není v zařízení úplně snadné odhalit. Váš telefon může ještě dlouho po nakažení fungovat bez větších problémů. Varovné ukazatele, jako jsou například agresivní reklamní okna, která nejde zavřít, nebo pomalé prohlížení webových stránek, si nemusíme hned spojit se škodlivým kódem. Adware ale mezitím může bez našeho vědomí stahovat do zařízení doplňky, instalovat programy a sledovat, co děláme na internetu. Proto bych rozhodně doporučoval zvážit pořízení bezpečnostního softwaru i pro chytrý telefon. Adware v zařízení spolehlivě odhalí, a navíc zařízení ochrání před celou řadou dalších škodlivých kódů," dodává Jirkal z ESETu.

Bezpečnostní software kontroluje stahované aplikace. Program v případě, že nějakou aplikaci nebo soubor rozpozná jako nebezpečný, spustí tzv. rezidentní ochranu souborového systému, která stažení či spuštění aplikace zablokuje a umístí ji do karantény. Uživatelé jsou o tomto postupu vždy informováni samotným bezpečnostním programem.

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.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

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/hrozby-pro-android-lide-nechteji-platit-za-premiove-sluzby-zneuzivaji-toho-hackeri