# Hrozby pro Android: V únoru útočníci lákali své oběti na získání prémiové verze Spotify

**26.3.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software**

**Praha, 19. března 2025 – Také únorová statistika kybernetických hrozeb potvrdila, že adware Andreed má zatím dobře nakročeno stát se i letos hlavním kybernetickým rizikem pro platformu Android. Vyplývá to z pravidelné analýzy detekčních dat pro tuto platformu v zemích EU od společnosti ESET. Skladba a pořadí nejčastěji detekovaných škodlivých kódů se zatím nemění, útočníci se však v případě trojského koně Agent.GKE rozhodli vyzkoušet novou strategii. Škodlivý kód v únoru maskovali za falešnou modifikaci k získání placené služby Spotify Premium. Desetina všech zachycených případů v Evropě se týkala také České republiky. Bezpečnostní experti varují, že s tím, jak uživatelé a uživatelky hledají cesty k úspoře svých peněz a poohlížejí se po možnostech jak obcházet standardní poplatky u aplikací, může počet případů škodlivého kódu dále růst.**

Adware Andreed oproti lednu mírně posílil a v rámci České republiky se v únoru objevil v 5 procentech všech zachycených detekcí v zemích EU. Nejvíce ho uživatelé ve falešných verzích her stahovali v Německu a Polsku. Oproti lednu, kdy ho bezpečnostní experti pozorovali ve výraznějším zastoupení také ve Švédsku, byl v únoru nejsilnější právě hlavně ve střední Evropě. Pořadí ostatních škodlivých kódů pro platformu Android se pak v únoru neměnilo – i tento měsíc mohli evropští uživatelé a uživatelky narazit na trojské koně Agent.EQD a Agent.GKE.

„Také v únoru nalíčili útočníci pasti především do škodlivých verzí her a populárních aplikací. Adware Andreed se nejčastěji objevil standardně v mobilních hrách. V únoru jej uživatelé nejvíce stahovali v cracknutých verzích her Vector Classic a Jewels Legend - Match 3 Puzzle. Parkurová hra Vector se přitom objevovala na našem seznamu již v lednu. Útočníkům se evidentně toto maskování škodlivého kódu vyplácí a na místě je tak ostražitost," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce ESET.

Trojský kůň Agent.EQD se i v únoru nejčastěji objevil ve falešné verzi aplikace Swing VPN. Také tento škodlivý kód v počtu detekcí oproti lednu mírně posílil. Dominantní zůstává v Německu, několik případů však bezpečnostní experti objevili v lednu také v Česku. Téměř na stejných hodnotách zůstal trojský kůň Agent.GKE. Pro něj však útočníci v únoru přichystali novou strategii. K jeho šíření zvolili škodlivou modifikaci pro upgrade aplikace Spotify na Premium verzi.

„Způsob, pro který se útočníci rozhodli v případě trojského koně Agent.GKE, považujeme za nebezpečný. Platforma Spotify v nedávné době upravila svou aplikaci tak, aby jejich placenou verzi nešlo tak snadno obcházet. Uživatelé tak více hledají možnosti, jak placení přesto obejít, a to na různých internetových fórech. A útočníci to dobře vědí," vysvětluje Jirkal. „Trojského koně Agent.GKE jsme detekovali nejvíce ve Španělsku a Polsku. Ze všech detekcí se v desetině případů objevil také v České republice. Jak můžeme vidět, tak uživatelé a uživatelky v Česku hledají možnosti, jak ušetřit na zpoplatněných službách populárních aplikací. Vždy nicméně varujeme před tím, že taková výhoda v podobě úspory peněz může být jen iluzí. Adware i další škodlivé kódy pro platformu Android jsou rizikem pro naše data. Právě na různých fórech a úložištích máte velkou šanci, že spolu s aplikací stáhnete nějaký malware," dodává Jirkal.

Adware, neboli advertising-supported software, se v zařízení obvykle chová tak, že otevře nové vyskakovací okno s reklamou v prohlížeči. Agresivní zobrazování reklamy má hlavně negativní vliv na výkon našeho mobilního telefonu a snižuje nám uživatelský komfort při prohlížení webových stránek.

S adwarem se ale pojí i další rizika.

„Ne každá reklama je adware. Řada vývojářů využívá legitimní formy reklamy k tomu, aby se jim vrátily náklady na vývoj jejich aplikace, kterou nabízejí bezplatně. Bohužel to platí i opačně a reklama může být podvodná a nebezpečná. Reklamní banner nás může odvést na nebezpečné webové stránky a na nich již můžeme narazit na škodlivý kód, který infikuje naše zařízení. Adware může také sbírat naše osobní údaje, například zaznamenávat naše chování na internetu. V neposlední řadě může být adware také prostředníkem pro různé podvodné nabídky, tedy scam. S ohledem na celou škálu kybernetických rizik, které představuje, bych i v tomto případě doporučoval pořízení kvalitního bezpečnostního softwaru, který adware včas rozpozná a najde jej, pokud už je v zařízení přítomný," říká 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.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-android-v-unoru-utocnici-lakali-sve-obeti-na-ziskani-premiove-verze-spotify