Hrozby pro Android: Útočníci ví, že se chceme bavit – koncem roku vsadili na falešné Spotify a Amazon Prime Video

30.1.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Prosincová statistika nejčastějších kybernetických hrozeb nepřinesla žádné větší zvraty a s největším počtem detekcí bezpečnostní experti opět zachytili adware Andreed. Od listopadu pak mírně posílil trojský kůň Agent.GKE a do třetice se v Česku nejvíce vyskytoval škodlivý kód FakeApp.AHS. Škodlivé kódy tentokrát nejvíce šířily hry doplněné falešnou aplikací Spotify a Amazon Prime Video. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v České republice od společnosti ESET.

Loňský rok skončil opět prvenstvím adwaru Andreed jako nejčastější hrozby pro české uživatele platformy Android. Co do počtu detekcí si v prosinci udržel prakticky stejná čísla jako v předchozím sledovaném období. Závěrem roku pak mírně posílil trojský kůň Agent.GKE, který se na předních místech pravidelné statistiky objevuje od listopadu 2024. Podle bezpečnostních expertů nedošlo na platformě Android koncem roku k žádnému většímu překvapení. Může to dle nich být ale předzvěst přípravy nových typů útoků.

„V prosinci se kromě her, jejichž prostřednictvím se adware na platformě Android šíří nejčastěji, objevovala i falešná aplikace Spotify pro přehrávání hudby nebo aplikace Prime Video od společnosti Amazon pro sledování filmů a seriálů. Domníváme se, že útočníci se snažili maximálně vytěžit volný čas uživatelů během prázdnin a dovolených," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Aplikace Spotify posloužila tentokrát útočníkům k tomu, aby ji vydávali za trojského koně Agent.GKE. Útočníci jej šíří nepozorovaně jako tzv. dropper a následně jim slouží k šíření dalších škodlivých kódů. Za aplikaci Prime Video pak vydávali škodlivý kód FakeApp.AHS, který po stažení do zařízení oběti zprostředkoval komunikaci se servery útočníků. V případě adwaru Andreed byly hlavním zdrojem škodlivého kódu opět hry. Bezpečnostní experti nejčastěji zachytili falešnou verzi hry Car Factory Simulator a Heroes of Might and Magic III.

„Hry ani aplikace určené k zábavě útočníky stále neomrzely a může to být z jediného důvodu – stále se najde dostatečný počet obětí, které se do této pasti chytí. Adware i dropper jsou rizikem především kvůli tomu, že na první pohled nemusí být hrozba, kterou představují, pro uživatele viditelná. Adware se v zařízení může dlouho skrývat, sledovat co děláme na internetu a pomoct útočníkům odvést uživatele například na nebezpečné webové stránky. Dropper pak funguje jako obálka, která nepozorovaně doručí do zařízení další škodlivý kód. Útočníci takto mohou šířit i závažné škodlivé kódy určené k odcizení našich dat a financí. Uživatelé mohou pro svou obranu určitě udělat to, že si i do chytrého telefonu pořídí kvalitní bezpečnostní software a významně zvýší svou obezřetnost při stahování mobilních aplikací z internetových obchodů," radí Jirkal.

V minulém roce se bezpečnostní experti setkávali na platformě Android s novým způsobem útoků na chytré telefony, a to nejen s platformou Android. Jejich cílem se stala také platforma iOS. Útočníci v rámci těchto útoků využívali technologii progresivních webových aplikací (PWA) a tzv. WebAPK.

„Případy z loňského roku nám bohužel ukazují, že k instalaci škodlivé aplikace mohou útočníci přimět uživatele i tak, aby nepojali podezření, že stahují do svého zařízení něco škodlivého. Škodlivé

aplikace v těchto případech kradly bankovní přihlašovací údaje. Napodobovaly legitimní bankovní aplikace a umožnily útočníkům získat přihlašovací údaje, hesla a dvoufaktorové autentizační kódy k získání neoprávněného přístupu k účtům obětí. Multiplatformní povaha PWA také umožňuje útočníkům cílit na širší publikum, díky čemuž jsou tyto typy útoků univerzálnější a je možné je škálovat. Tyto technologie poskytují útočníkům pohodlný a účinný prostředek k šíření podvodných aplikací, aniž by potřebovali schválení v oficiálních obchodech s aplikacemi. Očekáváme, že s využitím PWA a WebAPK se setkáme i v letošním roce," říká Jirkal z ESETu.

Před škodlivými kódy, které jsou určené ke krádeži našich dat a následně i financí, uživatele ochrání kvalitní bezpečnostní software. Bezpečnostní experti však doporučují věnovat pozornost všemu, co na internetu děláme. Zdrojem kybernetických hrozeb mohou být totiž i škodlivé webové stránky, phishingové útoky, nebezpečné přílohy e-mailů, taktiky sociálního inženýrství a škodlivé reklamy umístěné ve vyhledávačích, na sociálních sítích a na webových stránkách. Právě obezřetnost v kombinaci s účinnými moderními způsoby ochrany našich dat je dle expertů správným přístupem k bezpečnosti na internetu.

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-utocnici-vi-ze-se-chceme-bavit-koncem-roku-vsadili-na-falesne-spotify-a-amazon-prime-video