Přehled hrozeb pro Android: Chytré telefony v Česku nově ohrožuje trojský kůň, který napadá bankovní aplikace

22.1.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Bezpečnostní experti z ESETu detekovali v prosinci na platformě Android malware Anatsa, který napadá bankovní aplikace. Útočníci malware šíří prostřednictvím škodlivého kódu Spy.Banker.BUL, který vydávají za aplikaci pro čtení dokumentů v PDF. Pokud uživatel stáhne tuto aplikaci do svého chytrého telefonu, po následné aktualizaci se aplikace pokusí stáhnout bankovní malware do zařízení. Malware Anatsa tak závěrem roku doplnil adware Andreed a trojského koně Triada. Podle bezpečnostních expertů bude situace na platformě Android v Česku i v následujícím roce vysoce proměnlivá a uživatelé mohou očekávat nejen adware, ale i závažnější typy škodlivých kódů. Vyplývá to z pravidelné statistiky kybernetických hrozeb pro platformu Android v Česku od společnosti ESET.

Dlouhodobě přítomné zástupce adwaru na platformě Android v Česku doplnil na konci roku 2023 škodlivý kód Spy.Banker.BUL, jehož prostřednictvím útočníci šíří malware Anatsa. Jakmile malware infikuje chytrý telefon, zaměří se na napadení bankovních aplikací.

„Malware Anatsa pozorujeme již několik měsíců, případy napadení bankovních aplikací se již dříve objevily například v Německu, ve Velké Británii či v USA. Z našich dosavadních zjištění víme, že útočníci vydávají nebezpečné aplikace se škodlivým kódem za nástroje pro čtení dokumentů v PDF. Pokud tuto aplikaci stáhnou do svého chytrého telefonu, ta projde po čase aktualizací a pokusí se stáhnout malware Anatsa do zařízení v podobě doplňku pro aplikaci. V prosinci jsme takto objevili doplněk PDF AI: Add on. Uživatel musí stažení doplňku potvrdit. Útočníci tak pravděpodobně obchází samotné zabezpečení obchodu Google Play, kde by bankovní malware jinak odhalily jeho bezpečnostní týmy," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

„Případ trojského koně Spy.Banker.BUL nám opět potvrzuje, že situace na platformě Android v Česku je těžko předvídatelná a stejně tak zůstane i pro následující rok. Útočníci mají tendence měnit velmi rychle strategie a zneužívané aplikace. Jejich hlavním zájmem zůstane i nadále především finanční zisk. Předpokládáme, že stále bude dominovat škodlivý kód z obchodů třetích stran, který do chytrých telefonů stahuje adware, agresivní a obtěžující reklamy. Očekávat bychom ale opět měli i případy škodlivého kódu, který má uživatele špehovat a krást informace," dodává Jirkal.

Spolu se škodlivým kódem Anatsa bezpečnostní specialisté opět detekovali také adware. Ten byl pravidelnou hrozbou pro platformu Android v Česku celý uplynulý rok. Ačkoli je adware méně závažnější než malware určený ke špionáži nebo k napadení bankovních aplikací, i tento typ hrozby může být zdrojem dalšího, daleko závažnějšího malwaru či podvodných reklamních nabídek.

„Adware Andreed, který byl v českém prostředí jedním z nejvíce detekovaných škodlivých kódů loňského roku, se i v prosinci nejvíce vyskytoval v upravených verzích populárních her, jmenovitě například ve hrách Totally Reliable Delivery Service nebo Terraria. Objevil se ale také ve verzi aplikace Magic Fluids nabízené zdarma. Právě nabídkami výhodných balíčků aplikací, ať už zdarma či za zvýhodněnou cenu, lákají útočníci uživatele ke stažení nebezpečných aplikací do jejich zařízení," říká Jirkal.

Mezi nejčastěji detekovanými škodlivými kódy se na konci roku objevil i trojský kůň Triada. Také tento škodlivý kód se může zaměřit na bankovní aplikace. V prosinci ho útočníci šířili ve verzi aplikace FM WhatsApp, která nabízí některé vylepšené funkce oproti základní aplikaci WhatsApp.

„Trojský kůň Triada šíří především nevyžádanou reklamu a spam, může být ale rizikem i pro elektronické platby v aplikacích. Dokáže například modifikovat verifikační SMS zprávy a manipulovat tak finančními transakcemi v legitimních aplikacích. Ty totiž nejsou tak chráněné jako například v internetovém bankovnictví. Peníze za nákupy v aplikacích pak Triada přesměruje přímo k útočníkům," dodává Jirkal.

V případě platformy Android bezpečnostní experti dlouhodobě doporučují především zvýšenou obezřetnost při stahování doplňků a aplikací do chytrého telefonu. Největším rizikem jsou pro uživatele především méně známé obchody třetích stran, internetová úložiště či fóra. Opatrnost je ale na místě i v případě oficiálního obchodu Google Play. Tam mohou uživatelům pomoci například hodnocení jiných uživatelů a recenze, především ty negativní.

„Pokud vím, že nějakou aplikaci využiji jen několikrát a pak už mi zůstane jen v telefonu, zvažoval bych její stažení už úplně na samém začátku. Uživatelé by také neměli dát na pochybné a příliš výhodné nabídky různých aplikací a nástrojů, protože v těchto případech mohou vždy počítat s tím, že do svého chytrého telefonu stáhnou obsah, který tam mít nechtějí. I když se například nebude přímo jednat o malware, i reklamní škodlivý kód může mít negativní vliv na výkon a fungování jejich zařízení a inzerovat odkazy na stránky, na kterých mohou narazit již na závažnější typy malwaru," dodává Jirkal z ESETu.

Před adwarem, malwarem Anatsa a dalšími hrozbami uživatele ochrání kvalitní bezpečnostní software. Ten nabízí nejen účinnou ochranu před spywarem a potenciálně nechtěnými aplikacemi (tzv. PUA), ale nabízí již dnes celou řadu dalších nástrojů, jako je správce hesel pro bezpečné uchovávání našich přihlašovacích údajů, pro které je největším nebezpečím například spyware, nebo virtuální privátní síť (VPN) pro zabezpečené a soukromé prohlížení internetu.

Uživatelé produktů 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 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-chytre-telefony-v-cesku-nove-ohrozuje-trojsky-kun-ktery-napada-bankovni-aplikace