Přehled hrozeb pro Android: Falešné hry v březnu ukrývaly adware i bankovní malware

25.4.2024 - | ESET software

Adware Andreed, přední kybernetická hrozba pro platformu Android v Česku, se i nadále drží v čele pravidelné statistiky od společnosti ESET.

V březnu však bezpečnostní specialisté zaznamenali také návrat trojského koně Cerberus, bankovního malwaru, který útočníci využívají k napadení internetového bankovnictví. Zdrojem šíření škodlivých kódů nadále zůstávají především hry pro chytré mobilní telefony.

Nejvíce aktivním škodlivým kódem na platformě Android byl v březnu opět adware Andreed. Na předních místech statistiky se pravidelně objevuje již několikátým rokem a stal se tak dlouhodobou hrozbou pro uživatele v Česku – kromě zátěže pro operační systém zařízení a nepříjemného vyskakování agresivních reklamních oken mohou útočníci jeho prostřednictvím inzerovat webové stránky, které obsahují závažnější malware nebo podvodné nabídky. Útočníci šíří adware Andreed prostřednictvím falešných verzí známých her, které každý měsíc mění. V březnu se adware nejčastěji skrýval ve falešné verzi hry Interstellar Pilot 2.

„To, že je adware Andreed tak dlouho v čele naší pravidelné statistiky, svědčí především o tom, že se útočníkům stále vyplácí – tedy že ho uživatelé a uživatelky v Česku stále stahují," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „Útočníci se nás opakovaně snaží v případě adwaru Andreed nalákat na hry zdarma, na které narazíme zpravidla v obchodech třetích stran a na internetových úložištích. Nadále však platí, že stahování mimo oficiální obchody a distribuční místa je dnes prakticky vždy zárukou, že kromě hry nebo různých nástrojů stáhneme i škodlivý kód," dodává Jirkal.

V letošním březnu se do popředí statistiky dostal po delší odmlce také bankovní malware Cerberus. Ten býval velmi aktivním typem škodlivého kódu naposledy v zimě roku 2022. Stejně, jako adware Andreed, i trojský kůň Cerberus se nejčastěji vyskytoval ve falešných verzích závodních her.

„Bankovní malware na platformě Android v Česku na delší dobu vystřídal především adware, nicméně březnová čísla nám ukázala, že malware Cerberus rozhodně není minulostí. Šíří se často prostřednictvím tzv. dropperů, škodlivého kódu, který napodobuje známé nástroje a služby. Rizikem je zejména pro internetové bankovnictví," vysvětluje Jirkal a dodává: „Podobně jako jiné bankovní trojské koně, i Cerberus dokáže v napadeném zařízení kontrolovat SMS zprávy nebo zaznamenávat stisky kláves na klávesnici. Dokáže ale také sbírat informace o kontaktech, poloze, aplikacích a další údaje přímo ze zařízení."

Podobně, jako v případě trojského koně Cerberus, se v březnu jako dropper šířil i malware Agent.HQS. Vydával se za pirátské kopie aplikací MX Player anebo Ultimate USB. Podle posledních zjištění bezpečnostních specialistů existuje možnost, že se takové aplikace šíří i prostřednictvím sítě Telegram.

V případě obrany před malwarem Cerberus bezpečnostní experti doporučují využívat vždy oficiální aplikace bank a ověřovat všechny operace v aplikaci ideálně pomocí otisků prstů či snímkem obličeje.

„Biometrické způsoby ověřování, jako je otisk prstu nebo snímek obličeje, využívání oficiálních

bankovních aplikací a nainstalování bezpečnostní aplikace do chytrého mobilního telefonu jsou spolehlivou zárukou toho, že naše přihlašovací i platební údaje zůstanou v bezpečí. Bezpečnostní software nás navíc ochrání i před dalšími kybernetickými hrozbami, včetně adwaru, který občas bývá nesprávně označován za méně škodlivý kód. I reklama vytvořená útočníky nás může odvést na nebezpečné webové stránky, které mohou být zdrojem dalších rizik," říká Jirkal z ESETu.

Kromě bezpečnostního softwaru experti doporučují také pravidelně aktualizovat operační systém i všechny aplikace zařízení a maximálně se vyvarovat stahování programů a her mimo obchod Google Play.

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 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 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/prehled-hrozeb-pro-android-falesne-hry-v-breznu-ukryvaly-adware-i-bankovni-malware