Přehled hrozeb pro Android: Na chytré telefony se opět nejvíce zaměřil adware

23.2.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Nejčastěji detekovaným škodlivým kódem na platformě Android v Česku byl v lednu adware Andreed.

Doplnily ho tentokrát trojské koně rodin Hiddad a Triada, které útočníci podobně jako adware šíří prostřednictvím falešných verzí oblíbených volnočasových aplikací. V lednu se mezi takovými aplikacemi objevila nejen populární hra, ale také fitness tracker nebo aplikace určená ke čtení z dlaně. Vyplývá to z pravidelné statistiky kybernetických hrozeb pro platformu Android v Česku od společnosti ESET.

V lednu na platformě Android v Česku převládala rizika v podobě adwaru a trojských koní, které mohou do zařízení stahovat další škodlivý obsah. Nejčastěji detekovanou hrozbou byl pak opět adware Andreed. Ačkoli se jedná o škodlivý kód, který zobrazuje především nevyžádanou agresivní reklamu, kliknutím na inzerovaný obsah se uživatel může dostat na daleko nebezpečnější webové stránky obsahující malware nebo podvodná sdělení.

„Adware Andreed se v lednu objevoval nejvíce ve falešné verzi populární hry My City: Star Horse Stable. Uživatelé na něj narazí nejčastěji v neoficiálním obchodě třetí strany. Doporučoval bych jim tak stahovat hry i aplikace pouze z Google Play a pokud mají děti, rozhodně je také poučit o nástrahách a rizicích stahování mimo oficiální obchody. Právě populární hry zdarma nebo za jiných výhodných podmínek mohou být velkým lákadlem i pro nejmenší uživatele," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Bezpečnostní specialisté detekovali v minulých týdnech v Česku také malware Anatsa, který se ale v nejnovější statistice znovu neobjevil. Podle bezpečnostních expertů ale není vyloučené, že se škodlivý kód na Česko opět zaměří.

V lednu doplnily adware Andreed trojské koně rodin Hiddad či Triada, které útočníci také šíří především mimo oficiální distribuční místa a obchody. Ukrývají je v různých volnočasových aplikacích, které velmi často mění – reagují tak nejen na bezpečnostní opatření, ale také na uživatele a trendy, které pozorně sledují.

„Na případu trojského koně Hiddad vidíme, že i na první pohled bezvýznamnou aplikaci si mohou útočníci vyhodnotit jako ideální k ukrytí škodlivého kódu. Trojský kůň Hiddad se v lednu opět objevil ve škodlivé verzi aplikace Life Palmistry – Palm&Gender, která nabízí uživatelům čtení z dlaně. Stejnou aplikaci využívali útočníci přitom již v listopadu, a tato strategie je tak evidentně stále úspěšná. I v případě trojského koně Triada útočníci v několik případech vsadili na to, co uživatele baví – škodlivý kód ukrývali ve falešné fitness aplikaci," říká Jirkal.

Na konci loňského roku se trojský kůň Triada objevil například ve škodlivé verzi aplikace FM WhatsApp, která oproti klasické aplikaci WhatsApp měla nabízet některé vylepšené funkce. Ačkoli trojský kůň Triada dále šíří především nevyžádanou reklamu a spam, může být rizikem i pro platby v aplikacích.

Na přelomu roku se hrozby na platformě Android v Česku proměňovaly velmi rychle. Kromě adwaru se uživatelé mohli setkat také s již zmíněným bankovním malwarem a pravidelně se na přední místa

statistiky vrací i škodlivý kód, který má funkce spywaru.

„Hrozby na platformě Android se vyvíjejí a proměňují daleko rychleji, než je tomu v případě jiných operačních systémů v Česku. Chytré telefony se totiž stávají plnohodnotnou alternativou k počítačům, především pro mladší generace. Útočníci, kteří v první řadě sledují finanční zisk, se na ně orientují právě i z tohoto důvodu. Telefon navíc vlastní už i děti a jsou tím pádem další zranitelnou skupinou uživatelů, na které cílí škodlivý kód," dodává Jirkal z ESETu.

Moderní bezpečnostní řešení pohodlně zabezpečí zařízení všech členů domácnosti – ochrání uživatele nejen před závažným malwarem, potenciálně nechtěnými aplikacemi (tzv. PUA) či nebezpečnými webovými stránkami, ale díky celé řadě nástrojů jim dokáže usnadnit jejich online životy – správce hesel jim pomůže s bezpečným uchováváním přihlašovacích údajů a virtuální privátní síť (VPN) pak zajistí 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-na-chytre-telefony-se-opet-nejvice-zameril-adware