Přehled hrozeb pro Android: V dubnu na české telefony cílil adware, bankovní malware i spyware

23.5.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

V čele pravidelné statistiky kybernetických hrozeb pro platformu Android v Česku byl i v dubnu adware Andreed. Doplnily ho tentokrát dva škodlivé kódy, se kterými se čeští uživatelé a uživatelky již v minulosti pravidelně setkávali – bankovní trojský kůň Cerberus a škodlivý kód s prvky spywaru, Spy.SpinOk. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET. Malware se i v dubnu šířil především prostřednictvím falešných verzí her pro chytré telefony. Bezpečnostní experti proto varují před neuváženým stahováním aplikací mimo oficiální distribuční místa.

Ačkoli v čele statistiky pro platformu Android v Česku stále figuruje adware Andreed, i v dubnu na sebe upozornil bankovní malware Cerberus, který se po delší době opět vyšplhal na přední místa pravidelných detekcí malwaru v Česku.

„Platforma Android je v kontextu kybernetických hrozeb v České republice poměrně dost proměnlivá a každý měsíc tak vidíme, jak se škodlivé kódy střídají. Návrat bankovního trojského koně Cerberus je tak poměrně překvapivý, protože tento škodlivý kód nebyl v Česku dlouho výrazněji aktivní," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „Podobně, jako jiné bankovní trojské koně, i Cerberus dokáže v napadeném zařízení kontrolovat SMS zprávy nebo zaznamenávat stisky kláves na klávesnici. Dokáže také sbírat informace o kontaktech, poloze, aplikacích a další údaje přímo ze zařízení. Na základě našich dat můžeme říct, že v dubnu již byl v českém kontextu i cíleněji zaměřený – objevili jsme ho hlavně ve falešné verzi hry Fast Car Driving - Street City," dodává Jirkal.

Hry pro chytré telefony jsou dlouhodobě na straně kybernetických útočníků využívané k šíření škodlivých kódů. Zdrojem malwaru jsou pak jejich falešné verze, které útočníci nabízejí v menších obchodech třetích stran či na internetových úložištích. Jejich prostřednictvím se v dubnu opět šířil také adware Andreed – objevil se například ve verzích her Car Factory Simulator nebo ve hře Power Girls – Fantastic Heroes.

„Aktuálně sledujeme situaci, kdy adware, který můžeme považovat za hlavní škodlivý kód pro české uživatele chytrých telefonů s platformou Android, doplňují závažnější typy škodlivých kódů. Bankovní trojský kůň Cerberus je rizikem zejména pro internetové bankovnictví," říká Jirkal, ale dodává: „Rozhodně to však neznamená, že adware je v tomto srovnání bez rizika, přestože ho někteří uživatelé mají tendenci podceňovat. Nevyžádaná agresivní reklama může fungovat jako prostředník mezi námi a závažnějšími typy škodlivých kódů. Reklamní odkazy nás totiž mohou odvést na webové stránky, na kterých můžeme do zařízení stáhnout nebezpečnější malware."

Poprvé od začátku letošního roku se na přední místa statistiky vyšplhal také škodlivý kód Spy.SpinOk. Jedná se o softwarový modul, který má však funkce spywaru. Jeho autoři ho mohou nabízet vývojářům jako marketingový doplněk, tzv. Software Development Kit (SDK). Proto můžeme na tento škodlivý kód narazit ve velkém množství aplikací, například ve hrách, které obsahují nějaké losování o ceny, a také v aplikacích pro přehrávání videí.

„Škodlivý kód Spy.SpinOk dokáže shromažďovat informace o souborech v napadeném zařízení a

následně je odesílat útočníkům. Ti mohou jeho prostřednictvím získávat informace o souborech i zkopírovat či nahradit dočasný obsah uložený ve schránce zařízení. Sami vývojáři si škodlivosti doplňku nemusí být vědomi, a tak může být rozšířený opravdu ve velkém množství různých aplikací," vysvětluje Jirkal.

V případě spywaru bezpečnostní experti doporučují již pokročilejší ochranu moderním bezpečnostním řešením. Spyware je v Česku hrozbou nejen v případě platformy Android a jeho cílem jsou naše hodnotná osobní data, se kterými mohou útočníci poté dále nakládat – prodat je na černém trhu nebo využívat k dalším typům útoků.

Kromě využívání spolehlivého kyberbezpečnostního řešení bychom měli zvažovat, odkud stahujeme aplikace pro chytré mobilní telefony. Ačkoli může být pro některé rozhodujícím kritériem to, že někde můžeme stáhnout jinak placenou aplikaci zdarma, nebo sehnat aplikaci, jejíž oficiální distribuce již byla ukončena, v konečném důsledku se nám tyto zdánlivé výhody vyplatit nemusí.

„Důležité je si uvědomit, že v současnosti se můžeme setkat s velkým množstvím aplikací, které mohou být útočníky nějak upraveny. Mohou aplikace někde odcizit a následně do nich přidat škodlivý kód, nebo mohou škodlivý doplněk nabízet rovnou vývojářům. Není také neobvyklé, že si aplikace upravují různé komunity, jejichž cílem je například zlepšit fungování aplikace, testovat nové funkce nebo najít její zranitelnosti. Z fór ale může aplikace uniknout opět do rukou útočníků, kteří ji po svých úpravách, a po vložení škodlivého kódu potom nabízejí za výhodných podmínek uživatelům," říká Martin Jirkal z ESETu.

Ačkoli ani v případě oficiálního obchodu pro platformu Android, Google Play, nemají uživatelé nikdy jistotu, že nenarazí na aplikaci obsahující malware, přesto je zde větší pravděpodobnost, že jeho bezpečnostní týmy škodlivé aplikace včas odhalí a odstraní. Právě stahování pouze z oficiálních distribučních míst významně sníží dle bezpečnostních expertů pravděpodobnost, že vpustíme škodlivý kód do našeho zařízení.

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.

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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/prehled-hrozeb-pro-android-v-dubnu-na-ceske-telefony-cilil-adware-bankovni-malware-i-spyware