V září na uživatele cílil nejen adware, ale také škodlivé kódy určené ke špionáži

13.1.2024 - Lucie Mudráková | ESET software

Adware Andreed a malware Spy.SpinOk byly v září nejčastěji detekovanými škodlivými kódy na platformě Android v Česku.

Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET. Zatímco adware se dále šíří především prostřednictvím falešných verzí mobilních her, malware Spy.SpinOk se v aplikacích objevuje jako škodlivý doplněk s funkcemi spywaru. Třetím nejčastěji detekovaným škodlivým kódem byl v září downloader Agent.CZB, který stahuje do zařízení další malware. Podle posledních zjištění by mohl i tento škodlivý kód získávat informace ze zařízení nebo převzít nad zařízením kontrolu. S proměnou kyberbezpečnostního prostředí na platformě Android, kdy méně závažný adware aktuálně doplňují škodlivé kódy, které jsou rizikem pro naše data a soukromí, bezpečnostní specialisté doporučují chránit také chytré mobilní telefony bezpečnostním softwarem.

Nejčastějšími škodlivými kódy pro platformu Android v Česku byly v září adware Andreed a malware Spy.SpinOk.

„Adware Andreed je typickým zástupcem adwaru, se kterým se uživatelé na zařízeních s platformou Android setkávají často. Ke svému šíření typicky využívá upravené verze her. V září útočníci takto zneužili například hry PickUp nebo Mini Ninjas," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

„Malware Spy.SpinOk je potom zcela jiným typem škodlivého kódu. Uživatelé v Česku se s ním setkávají již několik měsíců. Jedná se o softwarový modul s funkcemi spywaru, který dokáže shromažďovat informace o souborech v napadeném zařízení a následně je odesílat útočníkům. V září se objevil nejčastěji v napodobeninách aplikace YouTube, uživatelé ale na něj mohli narazit také ve hrách nebo balíčcích s emotikony," dodává Jirkal.

Narozdíl od adwaru, jehož hlavní funkcí je zobrazovat agresivní reklamu a případně může stahovat do zařízení další malware, škodlivý kód Spy.SpinOk již patří mezi přímé hrozby pro naše data a soukromí. Také u třetího nejčastěji detekovaného kódu za září, downloaderu Agent.CZB, měli útočníci testovat funkce k ovládání telefonu a získávání informací o zařízení.

„Konkrétně Spy.SpinOk je typem malwaru, který má provádět v zařízeních obětí špionáž. Útočníci mohou jeho prostřednictvím získávat informace o souborech i zkopírovat či nahradit dočasný obsah uložený ve schránce zařízení. Vývojářům aplikací mohou nabízet tento modul jako marketingový doplněk, takzvaný Software Development Kit, SDK," vysvětluje Jirkal.

„Downloader Agent.CZB poté funguje tak, že stáhne z internetu jiný škodlivý kód a nepozorovaně ho spustí v zařízení. Na základě bližší analýzy jsme zjistili, že jeho autoři testovali právě i funkce jako zobrazování adwaru, převzetí kontroly nad telefonem a získávání informací ze zařízení. Šířili ho například ve velmi podařené verzi aplikace Duolingo. Je tak možné, že upravili legitimní aplikaci, přidali do ní právě tento škodlivý kód, aby ji poté rozdistribuovali mezi uživatele," dodává Jirkal.

Bezpečnostní experti upozorňují, že uživatelé v současnosti čelí velkému množství aplikací, které mohou být upraveny útočníky. Ti mohou aplikace někde odcizit a následně do nich přidat škodlivý

kód, nebo mohou škodlivý doplněk nabízet rovnou vývojářům aplikací.

„Není neobvyklé, že si aplikace s otevřeným zdrojovým kódem upravují různé komunity. Jejich cílem je například zlepšit fungování aplikace, testovat nové funkce nebo najít její zranitelnosti. Z takových fór ale může aplikace uniknout právě do rukou útočníků, kteří ji po úpravách a nyní již se škodlivým kódem nabídnou na různých úložištích nebo obchodech třetích stran za výhodných podmínek uživatelům," říká Jirkal. „Běžný je ale také scénář, kdy útočníci nabídnou vývojářům škodlivý doplněk a vývojáři aplikací si jeho škodlivosti nemusí být ani vědomi. Aplikace, které pak tento škodlivý doplněk obsahují, mohou být mezi uživateli rozšířeny ve velkém," dodává Jirkal z ESETu.

Doporučením pro uživatele je vždy stahovat hry a aplikace z renomovaných zdrojů a obchodů. Zde totiž mají jistotu, že škodlivý obsah v nabídce aplikací je pravidelně vyhledáván a odstraňován. Škodlivý kód v upravených verzích aplikací spolehlivě odhalí také bezpečnostní software. Bezpečnostní specialisté proto apelují na uživatele, aby řádně zabezpečili také své chytré telefony a chránili svá data a soukromí i v těchto zařízeních.

Kvalitní bezpečnostní programy odhalí nejen spyware, ale také celou řadu dalších hrozeb na platformě Android. Chrání uživatele jak před škodlivým softwarem, tak před potenciálně nežádoucími aplikacemi (tzv. PUA) či podvodnými weby.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

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.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/prehled-hrozeb-pro-android-v-zari-na-uzivatele-cilil-nejen-adware-ale-take-skodlive-kody-urcene-ke-spionazi