Přehled hrozeb pro Android: V říjnu byl škodlivý kód nejčastěji ve falešných hrách, útočníci opět cílí na děti

27.11.2023 - Rita Gabrielová, Lucie Mudráková | ESET software

Rizikem pro platformu Android v Česku byl i v říjnu Adware Andreed, a to spolu se škodlivým kódem Spy.SpinOk a downloaderem Agent.CZB.

Bezpečnostní specialisté z ESETu objevili všechny tři nejčastější hrozby ve falešných verzích mobilních her. Upozorňují tak na to, že se může opět jednat o hlavní strategii útočníků, kterou cílí na širokou uživatelskou veřejnost, včetně nejmenších uživatelů z řad dětí. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Bezpečnostní experti z ESETu pozorovali v říjnu na platformě Android celou řadu falešných aplikací a her, prostřednictvím kterých útočníci v Česku dlouhodobě šíří adware a škodlivé kódy. Především falešné a upravené verze známých her jsou častou strategií, ke které se útočníci uchylují v období blížících se svátků a prázdnin.

„Nejčastěji jsme v říjnu na platformě Android opět detekovali adware Andreed. Dlouhodobě v jeho případě pozorujeme, že ho útočníci šíří primárně přes různé verze her, které nabízejí v obchodech třetích stran, a to za výhodných podmínek nebo zcela zdarma. V říjnu se jednalo například o hry Tasty Planet Forever, Geometry Jump nebo My Singing Monsters Composer," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „S větším počtem falešných her jsme se naposledy setkávali v letošním létě. Je tak pravděpodobné, že s blížícím se koncem roku a s tím souvisejícími prázdninami a nákupy technologií pod stromeček budou útočníci opět cílit na širokou veřejnost, a to včetně dětských uživatelů, kteří patří již v nízkém věku také mezi fanoušky mobilních her," dodává Jirkal.

Další škodlivé kódy, které se v říjnu objevily na předních místech pravidelné statistiky, objevili bezpečnostní specialisté také v některých hrách. Downloader Agent.CZB se například objevil v upravené verzi populární hry Roblox, škodlivý kód Spy.SpinOk, který má funkce spywaru, pak kromě her také v upravených aplikacích pro stahování hudby a videí z internetu nebo v aplikacích pro přenos souborů.

Právě mobilní hry jsou pro útočníky většinou spolehlivým způsobem, jak škodlivý kód nepozorovaně doručit uživatelům do jejich chytrých telefonů. Kvůli ochranným krokům kyberbezpečnostní komunity jsou však nuceni nebezpečné verze her neustále měnit, což přispívá k tomu, že se kyberbezpečnostní situace pro platformu Android v Česku neustále proměňuje.

„Jeden měsíc vidíme, že sílí detekce adwaru, v jiném měsíci ho střídá jiný typ malwaru. A ačkoli pozorujeme, že vážných typů malwaru pomalu ubývá, pravděpodobně nezmizí nikdy. Útočníci do svých strategií neustále investují a obměňují je, využívají roční období, svátky, studují chování uživatelů. Uživatelé by tak rizika pro chytré telefony neměli podceňovat, naopak by měli zůstávat informovaní o aktuálních hrozbách. Pokud mají děti, které už také vlastní svůj chytrý telefon, je na místě jim vysvětlit základní pravidla bezpečného digitálního života. Útočníci totiž prostřednictvím her cílí i na ně," říká Jirkal.

Kromě adwaru, který se vyznačuje zobrazováním agresivních reklam a inzerováním různých odkazů

na méně či více pochybné a nebezpečné webové stránky, mohou falešné hry a aplikace šířit i závažnější typy škodlivých kódů. Škodlivý kód Spy.SpinOk je softwarový modul s funkcemi spywaru, který dokáže shromažďovat informace o souborech v napadeném zařízení a následně je odesílat útočníkům. Downloader Agent.CZB pak stahuje z internetu jiné škodlivé kódy, které v zařízení nepozorovaně spustí. Podle posledních informací by mohl mít i funkce k převzetí kontroly nad telefonem a získávání informací ze zařízení.

Nejen před adwarem, ale také před závažnějšími škodlivými kódy, jako je například spyware, uživatele ochrání bezpečnostní software. Ten dokáže odhalit i hrozby, které mohou v našich zařízeních zůstávat nepozorovaně po delší dobu a ohrožovat tak naše data a soukromí.

„Bezpečnostní řešení dokáže uživatele ochránit nejen před malwarem, ale také před podvodnými weby či potenciálně nechtěnými aplikacemi. Řada řešení již navíc není jen antivirem, ale nabízí komplexní ochranu a řadu pokročilejších funkcí, jako je ochrana před dosud neznámými hrozbami, správce hesel pro bezpečnou správu přihlašovacích údajů nebo VPN, virtuální privátní síť, pro bezpečné připojení k veřejným Wi-Fi sítím," vysvětluje Jirkal. „Ke svému celkovému zabezpečení pak samozřejmě mohou přispět sami uživatelé, a to tím, že nebudou stahovat aplikace a hry z neověřených obchodů s aplikacemi nebo z veřejných internetových úložišť. Děti by kromě tohoto pravidla měly navíc vědět také o bezpečném nakládání s hesly nebo o nástrahách manipulativní komunikace prostřednictvím sociálního inženýrství," dodává Jirkal z ESETu.

Nejčastějším rizikům pro děti na internetu se věnuje také iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

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-rijnu-byl-skodlivy-kod-nejcasteji-ve-falesnych-hrach-utocnici-opet-cili