Přehled hrozeb pro Android: Srpnová bilance kyberhrozeb v Česku opět poukázala na podceňovaný adware

23.9.2024 - Lucie Mudráková | ESET software

Srpnová statistika kybernetických hrozeb pro platformu Android zatím potvrdila očekávání bezpečnostních expertů a uživatelé se ani ve druhé polovině léta nesetkali s výraznými odchylkami od dlouhodobě monitorovaných škodlivých kódů. V čele kyberhrozeb nadále stojí adware Andreed a doplňuje ho malware Agent.HQS s bankovním trojským koněm Cerberus. Bezpečnostní experti upozorňují, že ačkoli je adware někdy ze strany uživatelů podceňovaným rizikem, může být součástí větších a propracovanějších útoků, jejichž cílem jsou naše data a finance. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Ani v srpnu se trend vývoje kybernetických hrozeb pro platformu Android v Česku nezměnil. Na předních místech statistiky stále zůstává adware Andreed, následovaný malwarem Agent.HQS a bankovním trojským koněm Cerberus.

„Počet detekcí adwaru Andreed začal s příchodem prázdnin klesat a v srpnu tento pokles pokračoval. Uživatelé by ale rozhodně neměli předpokládat, že riziko v podobě adwaru je v České republice menší, nebo že se adware z našeho prostředí trvale stahuje," říká k aktuálnímu vývoji Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. „Adware většina uživatelů a uživatelek nepovažuje za velkou hrozbu. I reklama však může být kromě toho, že zahltí naše zařízení, škodlivá. Prostřednictvím reklamy mohou útočníci inzerovat podvodná sdělení nebo nás odkazovat na nebezpečné stránky obsahující malware. Škodlivou reklamu využívají také ve větších a propracovanějších útocích jako prostředek k manipulaci. V takové kampani se útočníci zaměřili například i na české banky. Pomocí nové phishingové techniky se snažili oklamat právě uživatele chytrých mobilních telefonů a přimět je k instalaci domnělých aktualizací pro bankovní aplikace," dodává Jirkal.

I kvůli tomu, že je adware jako kybernetická hrozba dlouhodobě podceňovaný, jej podle bezpečnostních expertů útočníci stále s oblibou využívají. V Česku jej dlouhodobě šíří prostřednictvím napodobenin mobilních her, na které mohou uživatelé narazit v obchodě třetí strany. V srpnu se v případě adwaru Andreed jednalo o napodobeninu hry Mini Ninjas, objevoval se ale nadále také v aplikaci určené k luštění křížovek. Bezpečnostní experti dlouhodobě upozorňují na to, že oběťmi adwaru mohou být i děti, pro které může být řada falešných her lákavá.

V srpnu se situace nezměnila ani v případě malwaru Agent.HQS. Objem jeho detekcí sice v červenci oproti předchozímu období narostl, další růst počtu případů byl v srpnu již minimální. Útočníci jej také maskují za domnělou aplikaci, a to konkrétně za MXtech videoplayer. Agent.HQS se šíří v podobě tzv. dropperu, který si lze představit jako obálku doručující škodlivý kód. Pokud dropper uživatelé stáhnou a nainstalují, „rozbalí se" a umožní instalaci dalších škodlivých kódů. Útočníci se touto strategií snaží obcházet bezpečnostní řešení.

„Detekované škodlivé kódy na platformě Android stále doplňuje i bankovní trojský kůň Cerberus, který se ve větším počtu detekcí vrátil do Česka letos na jaře. Rizikem je především v okamžiku, kdy navštěvujeme internetové bankovnictví přes prohlížeč chytrého telefonu, a ne přes bankovní aplikaci. Jedna z hlavních funkcionalit tohoto malwaru je tzv. webinject. Díky ní útočník dokáže upravit webovou stránku, například naší banky, tak, že přidá nová pole do formulářů, odebere

ochranné prvky nebo převezme kontrolu nad tím, kam jsou posílána naše data. Útočníci tímto způsobem dokáží na svůj server posílat získaná hesla, přepsat bankovní účet, kam peníze zasíláte, nebo odcizit údaje z bankovních karet. Rozsah úprav webové stránky závisí jen na tom, nakolik je útočník zdatný v tom, co dělá," vysvětluje Jirkal.

Škodlivé kódy jsou obecně velkým rizikem pro řadu našich dat, která mají pro útočníky velkou cenu. I adware jim může posloužit k získání celé řady informací o našem zařízení nebo o našem chování na internetu. Z nich si pak mohou poskládat obrázek o tom, kdo jsme. Lépe pak na nás zacílí útoky využívající techniky sociálního inženýrství, pro které je společným znakem především manipulativní komunikace.

„Na jednu stranu již řada uživatelů přistupuje ke své digitální bezpečnosti velmi odpovědně – spravuje a používá bezpečně svá hesla, neriskuje při stahování aplikací a nástrojů mimo oficiální obchody s aplikacemi a snaží se v této oblasti vzdělávat. Na druhou stranu ani útočníci nespí a své útoky stále zdokonalují. Výjimkou dnes nejsou propracované útočné scénáře, za nimiž stojí skupina hackerů a podvodníků, kteří jsou často velmi dobře zorganizovaní i ve větších skupinách. Jejich cíli jsou čím dál častěji právě uživatelé chytrých telefonů, které dnes již ve spoustě aktivit sekundují či přímo nahrazují počítače a notebooky. V proměnlivém prostředí hrozeb by tak uživatelé neměli podceňovat profesionální ochranu i tohoto zařízení, která může velmi dobře fungovat jako pojistka v případech, kdy přes všechnu opatrnost narazíme na malware," dodává Jirkal z ESETu.

Kvalitní bezpečnostní software chrání uživatele nejen před hrozbami v podobě malwaru, ale také před potenciálně nechtěnými aplikacemi či pochybnými webovými stránkami. Pokud je webová stránka, na kterou se adware snaží uživatele přesměrovat, na seznamu podvodných stránek, bezpečnostní program k ní zablokuje přístup. Uživatelům se pak objeví varování s informacemi, proč je webová stránka blokována. Program také v případě, že nějakou aplikaci nebo soubor detekuje jako nebezpečné, zapne při jejich stažení či spuštění detekci rezidentní ochranou souborového systému. Tato funkce stažení nebo spuštění zablokuje a přesune nebezpečný objekt do karantény.

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 výzkumná a 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-srpnova-bilance-kyberhrozeb-v-cesku-opet-poukazala-na-podcenovany-adware