Hrozby pro Android: Útočníci se chystají na léto, v květnu mezi hrozbami nechyběl adware ani zloděj dat

26.6.2025 - | ESET software

Zatímco v uplynulých měsících byl vývoj kybernetických hrozeb na platformě Android poměrně stabilní, v květnu útočníci použili dosud nepříliš známé typy škodlivých kódů – adware Andreed v čele statistiky doplnil škodlivý kód Agent.FIV, jehož úkolem je krást data z telefonu, a dropper Agent.MUY, který má za úkol do našich zařízení nepozorovaně doručit další malware. Bezpečnostní experti před nadcházející sezónou letních prázdnin opět doporučují seznámit s aktuálními hrozbami také děti. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET.

Dle květnové statistiky kybernetických hrozeb pro platformu Android se na předních místech se shodným počtem detekcí umístily tři různé škodlivé kódy – evropská stálice adware Andreed, zloděj dat Agent.FIV a dropper Agent.MUY.

„Jako každý rok před letní sezónou se situace na platformě Android opět stává méně přehlednou. V uplynulých měsících jsme pozorovali převážně stabilní skladbu tří nejčastějších škodlivých kódů, to už nyní ale neplatí. Adware Andreed zůstává nebezpečný hlavně kvůli tomu, že se šíří prostřednictvím falešných mobilních her, které můžeme jak dospělí, tak děti o prázdninách vyhledávat více. Škodlivý kód Agent.FIV útočníci vydávali za různé aplikace, velmi často opět za Spotify, a snažili se jeho pomocí krást informace z našeho telefonu. Dropper Agent.MUY pak vypadal jako aplikace prohlížeče Chrome od Google a jeho úkolem bylo hlavně stáhnout do zařízení další malware," shrnuje květnový přehled kybernetických hrozeb pro platformu Android Martin Jirkal, vedoucí analytického týmu v pražské pobočce ESET.

Pozornost bezpečnostních expertů se tentokrát zaměřila právě na zmíněný škodlivý kód Agent.FIV. Ten se letos na předních místech statistiky objevil poprvé. Útočníci jako jeho „převlek" opět zvolili Spotify, což je značka, ke které se v letošním roce upínají poměrně často. Uživatelé a uživatelky na něj mohli narazit také ve škodlivé verzi aplikace Cricfy TV, která v legitimních případech slouží ke sledování kriketu. Podle bezpečnostních expertů škodlivý kód krade informace z našeho telefonu. Škodlivá verze aplikace se může prozradit právě tím, že po uživatelích požaduje obrovské množství oprávnění.

„Než všichni vyrazíme na dovolené a dětem začnou prázdniny, doporučoval bych v tuto chvíli věnovat pár chvil zabezpečení našich chytrých telefonů a informovat se o aktuálních hrozbách, se kterými se lidé mohou setkat. Jako každý rok, i před začátkem prázdnin je vhodné seznámit v základu s těmito riziky také vaše děti, které jistě mají své vlastní smartphony, nebo si půjčují ten váš. Přeci jen léto maximálně využíváme k relaxaci a odpočinku, a tudíž nemusíme být online tolik ve střehu. A můžete si být jistí, že právě na tohle útočníci spoléhají," říká Jirkal.

Kromě profesionálního zabezpečení v podobě bezpečnostní aplikace v telefonu by měli uživatelé a uživatelky stahovat aplikace výhradně z oficiálního obchodu Google Play, kde bezpečnostní týmy aktivně kybernetická rizika vyhledávají. Opatrnost je na místě hlavně u mobilních her, které útočníci velmi rychle střídají – v květnu šířili adware Andreed ve falešných verzích her Growing Up: Life of the '90s nebo Dead Effect 2.

„Právě hry jsou oblastí, kde můžeme s jistotou tvrdit, že potenciálními oběťmi jsou uživatelé a uživatelky všech věkových kategorií, a to včetně té nejmladší. Hry jsou lákadlem z různých důvodů. Útočníci jejich škodlivé verze nabízejí zdarma nebo za výhodných podmínek, na což mohou obzvlášť slyšet děti, které musí hospodařit jen s kapesným," říká Jirkal. „Legitimní verze her nemusí být ale také dostupné pro všechny verze operačního systému Android, nebo jsou dostupné jen v některých zemích. Řada uživatelů se tak může rozhodnout obejít stahování aplikací z oficiálního obchodu Google Play a stáhnout si hru nebo nějakou jinou aplikaci ve formě tzv. APK – Android Application Package. V případě těchto instalačních souborů je však mnohem vyšší riziko, že budou obsahovat nějaký typ škodlivého kódu. Soubory APK standardně automaticky stahujeme a instalujeme i v Google Play, tam ale podléhají daleko větší kontrole než v případě jiných obchodů a webových stránek či fór," uzavírá Jirkal z ESETu.

Nejčastějším rizikům pro děti na internetu se věnuje také iniciativa Safer Kids Online, která má za cíl pomoci jejich rodičům zorientovat se v nástrahách digitálního světa. Uživatele všech věkových kategorií bude před aktuálními hrozbami varovat také kvalitní bezpečnostní software. Ten dnes obsahuje řadu doplňkových funkcí, jako je například virtuální privátní síť (VPN) pro zabezpečené a soukromé prohlížení internetu, což uživatelé a uživatelky ocení i při cestování, kdy se mohou více připojovat k nezabezpečeným Wi-Fi sítím.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-android-utocnici-se-chystaji-na-leto-v-kvetnu-mezi-hrozbami-nechybel-adware-ani-zlodej-dat