Hrozby pro Android: Zdrojem škodlivého kódu byly v lednu verze populárních her a falešná VPN

25.2.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejčastěji detekovaným škodlivým kódem pro platformu Android zůstal v lednu adware Andreed. Vyplývá to z pravidelné analýzy detekčních dat pro platformu Android v zemích EU od společnosti ESET. Stejným rizikem jako pro Českou republiku je také pro uživatele a uživatelky v Německu nebo ve Švédsku. V lednu jej útočníci nejvíce šířili prostřednictvím nebezpečných verzí her Vector, Spider Solitaire či Bike Race Pro. Kromě škodlivého kódu Agent.GKE, který se vydával například za Spotify, Minecraft či aplikaci Flightradar, na sebe v lednu upozornil i trojský kůň Agent.EQD. Útočníci jej šířili jako falešnou VPN aplikaci a jeho úkolem bylo zapojit napadené uživatele do DDoS útoku.

Čeští uživatelé a uživatelky se mohli s adwarem Andreed setkávat po celý minulý rok v podobě falešných verzích známých her. Podle nejnovější statistiky zaměřené na mobilní hrozby pro platformu Android v evropských zemích, je Andreed podobně jako v Česku srovnatelným rizikem také v Německu nebo ve Švédsku.

„Adware je typem škodlivého kódu, který v zařízení zobrazuje velké množství škodlivé reklamy – tedy takové, která může uživatele odvést a nebezpečný web s dalšími škodlivými kódy. V lednu se nejčastěji ukrýval ve škodlivé verzi parkurové hry Vector nebo ve verzi oblíbené a dnes již legendární hry Spider Solitaire. V Česku jsme tuto hrozbu zachytili nejvíce ve škodlivé verzi hry Bike Race Pro," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce ESET. „Hry jsou pro útočníky ideálním způsobem, jak dostat do našich telefonů škodlivý kód. Jejich legitimní verze ale nemusí být 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 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," vysvětluje Jirkal.

Evropské telefony v lednu nejvíce ohrožovaly také trojské koně Agent.EQD a Agent.GKE. Druhý jmenovaný škodlivý kód znají dobře z minulosti také čeští uživatelé a uživatelky. Útočníci ho šíří ve formě dropperu a maskují ho za falešné verze různých aplikací. V lednu se opět jednalo například o Spotify, útočníci ale zneužili také popularitu hry Minecraft či aplikace Flightradar. Česko bylo čtvrtým nejčastějším cílem, a to po Španělsku, Polsku a Německu. Trojského koně Agent.EQD pak útočníci vydávali za škodlivou aplikaci VPN. Cílem byli především uživatelé v Německu, případy se objevily nicméně i v České republice.

„Podle našeho posledního průzkumu jsou již čeští uživatelé a uživatelky poměrně uvědomělí a aplikace stahují pouze ze známých a oficiálních obchodů s mobilními aplikacemi. Většina z nich věnuje pozornost také uživatelským recenzím. Ty bychom si měli přečíst vždy, když chceme nějakou aplikaci stáhnout. Špatné zkušenosti si druzí uživatelé většinou nenechají pro sebe a upozorní na ně. Není také od věci ještě před samotným stažením zvážit, zda danou aplikaci opravdu potřebujeme. Pokud aplikaci využijeme jen po nějaké časově omezené období, je vhodné ji následně odinstalovat," radí Jirkal.

Druhou nejčastější kybernetickou hrozbu pro platformu Android, trojského koně Agent.EQD, šířili útočníci v podobě falešné VPN. VPN je zkratka pro anglický termín Virtual Private Network a jedná se o technologii, která vytvoří zabezpečené šifrované spojení mezi našim zařízením a vzdáleným serverem. Jejím úkolem je poskytnout nám soukromí, bezpečnost a určitou míru anonymity.

„V tomto konkrétním případě se bohužel jasně ukazuje, že pokud uživatelé zdarma stahují nějakou službu či software, který bývá jnak zpravidla placený, mohou se lehce stát cílem škodlivých kódů nebo součástí útoků. Pokud si uživatelé stáhli tuto verzi VPN, zaplatili za to svými daty. Útočníci je byli po stažení schopni zapojit do DDoS útoků. V tuto chvíli jsou již servery škodlivé aplikace nefunkční, pokud se je ale útočníci rozhodnout znovu spustit, škodlivý kód bude znovu aktivní. Uživatelé by měli mít na paměti, že kvalitní a bezpečná VPN je vždy placená, protože provoz této technologie bývá nákladný. V minulosti jsme se mohli setkat i s VPN aplikacemi zdarma, které byly sice funkční, ale podvodné," říká Jirkal.

Bezpečnostní experti doporučují používat i v případě mobilních telefonů moderní bezpečnostní software. Ten je obranou nejen před trojskými koni, spywarem nebo adwarem, ale jeho součástí je i řada dalších funkcí, včetně VPN. V rámci řešení ESET Home Security nabízí funkce VPN důvěrné prohlížení internetu vytvořením soukromého síťového připojení, které zaručuje ochranu při využívání veřejné Wi-Fi sítě. Šifruje online aktivity uživatelů a umožňuje neomezený přístup k obsahu s geografickým omezením, včetně neomezeného a soukromého přístupu k webovým stránkám ve více než 60 zemích. Díky této funkci mohou uživatelé na cestách bezpečně přistupovat k televizním pořadům a filmům ze své domovské země nebo využívat své oblíbené streamovací služby z různých částí světa.

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.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

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.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

Vítězslav Pelc
Senior manažer PR a komunikace

ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-android-zdrojem-skodliveho-kodu-byly-v-lednu-verze-popularnich-her-a-falesna-vpn