Přehled hrozeb pro Android: Adware Andreed v únoru posílil, v Česku ho nejvíce stahovali fanoušci aut

20.3.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Také v únoru se v Česku objevila řada upravených a nelegitimních verzí her a aplikací, kterými se šířil adware.

Na více než patnáct procent opět posílil adware Andreed, který se nejčastěji objevoval ve falešné verzi hry Car Factory Simulator. Doplnily ho opět trojské koně z rodin Triada a Hiddad, které ke svému šíření také zneužívají různé nástroje pro chytré telefony. S ohledem na velké množství aplikací, které mohou být rizikem pro naše data a soukromí, bezpečnostní specialisté doporučují již na samém začátku zvážit, zda danou aplikaci či hru opravdu potřebujeme. Ke zvýšení ochrany dat bychom dle nich měli vždy věnovat pozornost podmínkám použití. Vyplývá to z pravidelné statistiky kybernetických hrozeb pro platformu Android v Česku od společnosti ESET.

Bezpečnostní specialisté zaznamenali v únoru pokračující růst počtu případů adwaru Andreed, který se podle posledních čísel objevuje v Česku ve více než patnácti procentech všech případů. Také v únoru byl adware detekován ve velkém množství nelegitimních her různých žánrů, z nichž viditelně vyčnívala hra Car Factory Simulator. K běžné strategii kybernetických útočníků patří verze her velmi často měnit, a to jak s cílem zmást uživatele, tak bezpečnostní software.

„Adware Andreed se již směle řadí k dlouhodobě přítomným škodlivým kódům pro chytré telefony s platformou Android v Česku. A to, že v únoru opět o něco posílil, svědčí o tom, že ho útočníci nemají potřebu zatím vyměnit za nějakou jinou hrozbu. Útoky s využitím tohoto adwaru se jim zkrátka stále vyplácí. Přispívá k tomu také skutečnost, že uživatelé adware ve většině případů stáhnou sami – ať už tím, že stahují nelegitimní verze her a aplikací z neoficiálních zdrojů, nebo nevěnují pozornost podmínkám použití,“ říká k vývoji na platformě Android Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Uživatelé mohou na adware Andreed nejčastěji narazit, pokud stahují aplikace a hry mimo oficiální obchod Google Play. Jejich motivací je ve většině případů to, že aplikace a hry jsou v obchodech třetích stran a na různých internetových úložištích zdarma.

Adware patří mezi kybernetická rizika, která mají uživatelé ve zvyku spíše podceňovat. I přesto, že se jedná „pouze“ o škodlivou reklamu, je adware nebezpečný z několika důvodů: prostřednictvím reklamy může uživatelům zobrazovat odkazy na podvodné a nebezpečné webové stránky a může stahovat do mobilního telefonu další adware či jiný škodlivý kód, který už bude představovat závažnější riziko pro naše data a soukromí.

V únoru se v detekční statistice objevily také trojské koně Triada a Hiddad. Škodlivý kód Hiddad se nadále objevuje především ve škodlivé verzi aplikace Life Palmistry – Palm&Gender, která nabízí uživatelům čtení z ruky. Stejnou aplikaci využívají útočníci již od loňského listopadu. Trojský kůň Triada se již dříve objevil například ve škodlivé verzi aplikace FM WhatsApp, která oproti klasické aplikaci WhatsApp měla nabízet některé vylepšené funkce. Útočníci v jeho případě vsadili i na falešnou fitness aplikaci, která si měla najít oběti v řadách sportovních nadšenců. V únoru se trojský kůň Triada vydával za bezplatnou VPN aplikaci.

V dynamicky se měnícím světě se naše data a soukromí stávají tím nejcennějším vlastnictvím, které máme. Právě adware, který je často přítomný v řadě aplikací, je i ve srovnání se spywarem či jinými typy škodlivých kódů nezanedbatelným rizikem. Uživatelé by přitom neměli být opatrní pouze v případě falešných aplikací, ale i těch legitimních, které mohou informace o nežádoucím nakládání s našimi daty uvádět v podmínkách používání.

„V podmínkách služby bychom si vždy měli přečíst, jaká data o nás daná aplikace sbírá, jaká společnost je spravuje a s kým je sdílí. Podle toho se můžeme rozhodnout, jestli chceme danou aplikaci vůbec používat nebo jaká oprávnění jí chceme udělit. Pokud to jde, aplikacím bychom měli povolit pouze nezbytná oprávnění pro jejich fungování, a poskytnout jim o sobě co nejméně informací," uzavírá Martin Jirkal z ESETu.

Kromě opatrného stahování aplikací můžeme svá data ochránit také pomocí moderního bezpečnostního řešení. Uživatelům a uživatelkám nabízí mimo zabezpečení před škodlivými kódy i celou řadu praktických nástrojů – správce hesel jim pomůže s bezpečným uchováváním přihlašovacích údajů a virtuální privátní síť (VPN) pak zajistí zabezpečené a soukromé prohlížení internetu.

Uživatelé produktů 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 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-adware-andreed-v-unoru-posilil-v-cesku-ho-nejvice-stahovali-fanousci-aut