Hrozby pro macOS: Škodlivá reklama si hledá cesty do zařízení přes napodobeniny přehrávačů

16.7.2024 - Lucie Mudráková | ESET software

Uživatelé a uživatelky počítačů od Apple mohli v posledním čtvrt roce narazit na řadu napodobenin aplikací a nástrojů, které ukrývaly malware.

V čele statistiky nejčastějších hrozeb pro platformu macOS v Česku a na Slovensku zůstávaly i v období od dubna do června 2024 adware Pirrit, downloader Adload a škodlivý kód PSW.Agent, který se řadí mezi tzv. infostealery. Útočníci zneužívali nejen falešnou verzi aplikace Adobe Flash Player, ale i aplikace určené k přehrávání médií, hudební soubory ve formátu MP3 či cracky a warez verze známých komerčních aplikací. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Podle statistiky kybernetických hrozeb pro platformu macOS v Česku a na Slovensku byly nejčastěji detekovanými škodlivými kódy za období od dubna do června 2024 adware Pirrit a downloader Adload. Oba typy škodlivých kódů se objevily téměř v pětině všech případů. Ve druhém kvartálu roku 2024 je doplnil škodlivý kód PSW.Agent, který se v čele statistiky objevuje od letošního jara.

„U všech nejčastěji zachycených škodlivých kódů pro platformu macOS jsme za sledované období pozorovali podobné chování. Útočníci je vydávali za oblíbené nástroje a aplikace pro uživatele počítačů značky Apple. Tyto napodobeniny známých aplikací samozřejmě obsahovaly nebezpečný kód. Uživatelé navíc nemusí na první pohled nic poznat ani po stažení. I když některé aplikace vůbec nefungují, řada z nich se i po stažení chová zcela standardně jen s tím rozdílem, že do zařízení stahují další adware nebo jiný, závažnější škodlivý kód," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

Škodlivé kódy se během sledovaného období objevovaly v řadě různých napodobenin aplikací a nástrojů. Útočníci podporují šíření těchto neoficiálních nebezpečných aplikací také online reklamou a optimalizací pro vyhledávače (SEO). Díky tomu dokáží uživatelům nabídnout podvodné aplikace nebo programy přímo mezi výsledky vyhledávání na internetu.

Adware Pirrit se tentokrát ukrýval především v domnělém instalátoru pro nástroj Adobe Flash Player. Útočníci tuto aplikaci napodobují poměrně často a bezpečnostní experti opakovaně upozorňují, že oficiální vývoj aplikace Adobe Flash Player byl již ukončen před několika lety. Downloader Adload se pak nejčastěji vydával za přehrávače médií nebo hudební alba a písničky ve formátu MP3.

„Zdrojem falešných aplikací jsou nejčastěji neoficiální obchody třetích stran. Uživatelé a uživatelky ale stále stahují aplikace a nástroje i z veřejných internetových úložišť. V případě downloaderu Adload útočníci využili i SEO, optimalizaci pro vyhledávače, aby nabídli nebezpečné verze aplikací cíleně uživatelům," říká Kropáč.

Adware Pirrit má především negativní vliv na výkon zařízení a na uživatelský komfort při procházení internetu. Projevuje se velkým množstvím reklamního obsahu a po kliknutí na některou z reklam mohou být uživatelé přesměrováni na podvodné webové stránky nebo na stránky s dalším malwarem. Downloader Adload pak stahuje do zařízení další adware.

Škodlivý kód PSW.Agent se řadí narozdíl od adwaru a downloaderu k malwaru, který je přímým nebezpečím pro naše osobní data. Infostealery jsou hlavním rizikem také v případě operačního systému Windows. Útočníci je nejčastěji využívají ke krádeži uživatelských jmen a hesel.

„Škodlivý kód PSW.Agent, známý také pod názvem Atomic Stealer, se šíří prostřednictvím sponzorovaných odkazů ve vyhledávačích, k čemuž využívá službu Google AdSense. Kromě jiných dat se cíleně zaměřuje na informace kolem kryptoměn a kryptoměnových účtů. Dokáže ze zařízení odcizit dokumenty programů MS Word nebo Excel, ale i soubory kryptoměnových peněženek Electrum, Binance či Exodus. Cílí ale také na přihlašovací údaje z prohlížečů nebo na soubory cookie, které může zneužít pro ověření na webu poskytovatele kryptoměn," vysvětluje Kropáč.

V posledních měsících se škodlivý kód PSW.Agent šířil jako cracky či warez programy různých komerčních aplikací.

S ohledem na skutečnost, že škodlivé kódy pro platformu macOS shodně napodobují celou škálu aplikací, je jedním ze způsobů ochrany nestahovat aplikace mimo oficiální obchod společnosti Apple, App Store. V případě infostealerů bezpečností experti upozorňují na to, že je na místě stále větší ostražitost samotných uživatelů a uživatelek.

„Z našich analýz vyplývá, že v první polovině letošního roku se při šíření infostealerů objevily již případy zneužití zvučných jmen nástrojů generativní AI, které jsou populárními tématy ve veřejné debatě. Uživatelé a uživatelky na každém rohu poslouchají, jak důležité je naučit se s nástroji umělé inteligence pracovat co nejdříve a jak je potřeba si je osvojit v pracovním procesu. Viděli jsme již případy, kdy útočníci vydávali malware za napodobeniny služeb Midjourney, Sora nebo Gemini. I tyto aplikace útočníci opět inzerují s cílem podpořit jejich šíření mezi nic netušící oběti, a to konkrétně na sociální síti Facebook. Očekáváme, že tento trend hned tak nezmizí a opatrnost při stahování a používání AI nástrojů je tak více než na místě," doplňuje Kropáč z ESETu.

Před infostelary a spywarem je účinnou ochranou bezpečnostní software. Bezpečnostní specialisté uživatelům také doporučují dbát na pravidelné aktualizace operačního systému zařízení a všech aplikací.

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 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

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-macos-skodliva-reklama-si-hleda-cesty-do-zarizeni-pres-napodobeniny-prehravacu