Hrozby pro macOS: Rizikem zůstává agresivní reklama i falešné verze oblíbených programů

12.9.2023 - Lucie Mudráková | ESET software

V čele pravidelné statistiky kybernetických hrozeb pro platformu macOS v Česku a na Slovensku se v srpnu opět objevil adware Pirrit. Ačkoli se škodlivé kódy pro tento operační systém v posledních měsících výrazněji proměňují, adware Pirrit potvrzuje, že je stálým a stabilním rizikem. Vedle dlouhodobě přítomného adwaru Bundlore se pak ve statistice objevil také adware InstallCore. Ten je v našem prostředí letos novinkou, přesto i v jeho případě útočníci využívají osvědčené postupy – adware se ukrývá ve falešných verzích známých aplikací a po stažení do zařízení nainstaluje další škodlivý software. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Nejčastěji detekovaným škodlivým kódem na platformě macOS byl v srpnu opět adware Pirrit.

„Adware Pirrit je klasickým zástupcem kódů zobrazujících agresivní reklamy. Uživatelé ho většinou stáhnou do zařízení sami a dobrovolně, často jako součást jiných programů nebo her, které útočníci nabízejí v obchodech třetích stran nebo na různých internetových úložištích zdarma či ve výhodných balících," vysvětluje Jiří Kropáč, vedoucí virové laboratoře společnosti ESET v Brně.

Dalšími škodlivými kódy, na které mohli uživatelé v srpnu narazit, byly například adware Bundlore nebo adware InstallCore. Ten se mezi nejčastějšími hrozbami objevil letos poprvé.

„Adware InstallCore se s větším podílem detekcí objevil v českém a slovenském prostředí po delší době. Jedná se o obdobu adwaru Bundlore, akorát od jiných útočníků – distributorů. InstallCore se nejčastěji vydává za klasické aplikace. Poté, co takovou aplikaci do zařízení nainstalujeme, škodlivý kód dále stáhne a nainstaluje adware, který nás bude mít za úkol sledovat. V srpnu se takto InstallCore vydával například za multimediální přehrávač MediaPlayer nebo grafický editor SnapSeed," říká Kropáč.

Právě programy nebo hry, které jsou mezi uživateli populární, jsou velmi často zneužívány kybernetickými útočníky. Zvučné jméno populární hry nebo softwarového nástroje funguje jako zaručená návnada pro ty uživatele, kteří při pořizování softwaru chtějí ušetřit.

„Standardní a prakticky neměnnou strategií útočníků je nabídnout v nějakém neoficiálním obchodě domnělou aplikaci nebo hru bez poplatku. Pokud uživatelé vyhledávají hry přes internetový prohlížeč a ne v oficiálním obchodě App Store, mohou na takové nabídky snadno narazit. V takových případech by měli věnovat pozornost například recenzím, které daná verze programu nebo hry v takovém obchodě má," doplňuje Kropáč.

I když adware nepatří mezi hrozby srovnatelné například s ransomwarem nebo spywarem, ani v jeho případě se uživatelům nevyplatí podcenit kvalitní zabezpečení. Bezpečnostní software totiž dokáže včas upozornit na potenciálně nechtěné aplikace (tzv. PUA) i podvodné a pochybné webové stránky, na které může adware v podobě agresivní reklamy velmi často odkazovat.

„V poslední době se na platformě macOS často setkáváme se škodlivými kódy, které mohou mít negativní dopad na soukromí uživatelů. Některé z nich se totiž přímo zaměřují na sledování našich

aktivit na internetu. Uživatelům bych tak rozhodně doporučil chránit zařízení bezpečnostním softwarem a nestahovat programy nebo hry mimo oficiální obchody," doplňuje Kropáč z ESETu.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

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 produktů 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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-macos-rizikem-zustava-agresivni-reklama-i-falesne-verze-oblibenych-programu