Hrozby pro macOS: Rizikem uplynulých týdnů byl malware využívaný ke krádežím v kryptopeněženkách

28.5.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Nejčastější hrozbou pro platformu macOS zůstává dlouhodobě přítomný adware Pirrit. V uplynulých týdnech ale na sebe nejvíce upoutal pozornost škodlivý kód PSW.Agent, který se svými funkcemi řadí mezi tzv. infostealery, škodlivé kódy určené ke krádeži našich dat. Malware PSW.Agent se pak cíleně zaměřil na kryptoměnové účty, a to s pomocí sponzorovaných škodlivých reklam a bannerů. Právě zneužití legitimních nástrojů online marketingu je jednou z častých strategií útočníků na této platformě. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Podle dat z posledních dvou měsíců je na platformě macOS v Česku a na Slovensku nadále rizikem především adware Pirrit. S více než desetinou všech zachycených detekcí je škodlivým kódem, který se v našem prostředí vyskytuje dlouhodobě a stabilně.

„Adware Pirrit, který se projevuje například vyskakujícími reklamními okny, a tím má negativní vliv na výkon zařízení a na uživatelský komfort při procházení internetu, se od začátku letošního roku objevuje v menším počtu detekcí. I když by se tak mohlo zdát, že se škodlivé kódy na platformě macOS postupně vytrácí a uživatelé jsou tudíž méně vystaveni kybernetickým rizikům, nemusí to tak být. Útočníci mohou takové období využít k vyzkoušení nových typů malwaru nebo strategií," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

Jednou z nových hrozeb na této platformě je v posledních týdnech například škodlivý kód PSW.Agent. Řadí se mezi tzv. infostealery, které útočníci využívají ke krádeži našich dat, jako jsou uživatelská jména a hesla.

„Detekovaná malware rodina, do které spadá škodlivý kód PSW.Agent, je variantou s názvem Atomic Stealer. Šíří se přes sponzorované odkazy ve vyhledávačích, a to hlavně v případě vyhledávače Chrome a služby Google AdSense, nebo obecně prostřednictvím podvodných aktualizací a bannerů," říká Kropáč. „Podle našich dat se škodlivý kód v uplynulých měsících vydával především za falešnou aplikaci Crack Installer, která má umožnit obejít časové nebo licenční omezení placených programů. Tuto funckionalitu ale aplikace vůbec neobsahuje a pouze obětem odcizí jejich data," doplňuje Kropáč.

Podle analýzy bezpečnostních specialistů se malware PSW.Agent zaměřuje cíleně na informace a data kolem kryptoměn a kryptoměnových peněženek. Z účtů a ze zařízení odcizí dokumenty programů Word nebo Excel či soubory kryptoměnových peněženek, jako je například Electrum, Binance či Exodus. Jeho cílem jsou také přihlašovací údaje z prohlížečů nebo soubory cookies, které může zneužít pro ověření na webu poskytovatele kryptoměn. Ukradená data pak malware odesílá na kontrolní server útočníků.

Nejen v případě škodlivého kódu PSW.Agent slouží kybernetickým útočníkům legitimně dostupné nástroje online marketingu. U třetího nejčastěji detekovaného škodlivého kódu, adwaru MaxOfferDeal, zneužívají útočníci i optimalizaci pro vyhledávače, tzv. SEO.

„Adware do napadeného zařízení většinou stahuje další adware nebo různé doplňky pro prohlížeče,

ke kterým ale uživatelé vůbec nemusí dát souhlas. Útočníci mohou ale s jeho pomocí zobrazovat i podvodné reklamy nebo reklamní bannery s odkazy na nebezpečné webové stránky. Mohou přitom zneužít i SEO, známý nástroj online marketingu. Díky tomu dokáží uživatelům nabídnout podvodné aplikace nebo programy přímo mezi výsledky vyhledávání na internetu," vysvětluje Kropáč.

Bezpečnostní specialisté doporučují uživatelům a uživatelkám, aby rizika spojená s adwarem nepodceňovali. Stejně jako závažnější typy malwaru se totiž adware může zaměřit na naše uživatelská data, která mohou útočníkům sloužit k celé řadě dalších útoků. Naše data navíc mají svou cenu i na černém trhu.

„Také na platformě macOS se celá řada škodlivých kódů šíří prostřednictvím falešných aplikací z nelegitimních obchodů nebo internetových úložišť. Uživatelé tak mají ochranu před touto hrozbou v rukách částečně sami, pokud nebudou stahovat aplikace a hry mimo oficiální distribuční místa a obchod App Store," říká Kropáč.

„Spolehlivou ochranou před škodlivými kódy je vždy aktualizovaný operační systém a internetový prohlížeč v kombinaci s kvalitním bezpečnostním softwarem. Ten dnes navíc obsahuje celou řadu praktických nástrojů pro celkovou správu našich digitálních životů. Jedním z nich může být například správce hesel, specializovaný program, který uchovává naše hesla v zašifrované podobě a automaticky je doplňuje při přihlašování do účtů. Je tak daleko bezpečnější variantou k internetovým prohlížečům, které nejsou před útoky dostatečně zabezpečené," dodává Kropáč z ESETu.

Uživatelé řešení od 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 také 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 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-uplynulych-tydnu-byl-malware-vyuzivany-ke-kradezim-v-kryptopenezenkach