Hrozby pro macOS: Rizikem byl v prvním čtvrtletí 2025 adware zneužívající SEO, posílil i zloděj kryptoměn

8.4.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Adware MaxOfferDeal se stal v prvním čtvrtletí letošního roku nejčastějším škodlivým kódem pro počítače od firmy Apple. Bezpečnostní experti jej přitom na předních místech pravidelné statistiky v minulém období nezaznamenali. Vyplývá to z detekčních dat společnosti ESET pro platformu macOS v Česku a na Slovensku za období od ledna do března 2025. Výrazněji dále klesaly detekce adwaru Pirrit, nicméně o několik procentních bodů posílil infostealer PSW.Agent. Jedná se v současnosti o výrazné riziko pro tuto platformu. Cílem infostealeru jsou mimo jiné také kryptoměny a kryptoměnové peněženky.

„Adware MaxOfferDeal je typem škodlivého kódu, u něhož útočníci zneužívají SEO – optimalizaci pro vyhledávače. Jedná se o typ útoku, který se daří uskutečnit díky dostupným a legitimním nástrojům online marketingu, což může přispět k jeho většímu rozšíření i úspěšnosti. V tomto případě se adware šíří prostřednictvím přesměrovaných sponzorovaných odkazů a výsledků vyhledávání. Uživatelům se tak na podvodných bannerech a stránkách nabízí ke stažení různé podvodné aplikace k řešení zdánlivých problémů, které ve skutečnosti neexistují – může se jednat například o podvodné aktualizace prohlížeče, systému nebo různých programů. Některé z nich přitom již nemusí oficiálně fungovat, jako je případ u útočníků velmi oblíbeného Adobe Flash Playeru. Uživatelé si v tomto případě vždy stáhnou jen adware, který sleduje jejich chování na internetu," vysvětluje Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

Adware Pirrit, na nějž mohou uživatelé a uživatelky narazit podobně jako na adware MaxOfferDeal v celé řadě falešných doplňků a aktualizací, pak v prvním čtvrtletí nezopakoval svůj růst z konce loňského roku. Z 50 procent detekcí „spadl" na podíl 13 procent všech zachycených případů pro platformu macOS. Oproti minule sledovanému období ale posílil infostealer PSW.Agent. Ten kyberbezpečnostní odborníci skloňují především v souvislosti s roustoucími hrozbami pro kryptoměnové peněženky.

„Zatímco v posledním čtvrtletí loňského roku se infostealer PSW.Agent maskoval za keygen nebo crack verze programů pro různé aplikace – například pro AutoCAD či ArchiCAD – na začátku letošního roku jej útočníci vydávali především za aplikace pro online meetingy a konference Zoom či Microsoft Teams. I v případě šíření tohoto infostealeru využívají legitimně vypadající reklamy v reklamním systému Google. Po kliknutí na reklamu jsou uživatelé přesměrováni na stránku, která je vyzve ke stažení nějakého programu. Jedná se ale opět pouze o škodlivý kód," říká Kropáč.

Infostealery nejsou rizikem pouze pro platformu macOS. Čeští uživatelé a uživatelky se s nimi pravidelně setkávají také v případě operačního systému Windows. Specializací škodlivého kódu PSW.Agent, který je znám i pod názvem Atmos Stealer (AMOS), je vedle přihlašovacích jmen a hesel také krádež dat kolem kryptoměn a kryptoměnových peněženek, jako je například Electrum, Binance či Exodus.

„Infostealer PSW.Agent je aktuálně velmi rozšířeným škodlivým kódem pro platformu macOS. Ve druhé polovině loňského roku jsme obecně začali sledovat průdký nárůst kybernetických hrozeb pro kryptoměny a kryptoměnové peněženky s tím, jak se kryptoměny dostávají do povědomí stále širší veřejnosti. Během období od června do listopadu 2024 výrazně narostl počet investičních podvodů, a

to o více než 335 % mezi prvním a druhým pololetím loňského roku. V našich detekcích došlo také k nárůstu u cryptostealerů, přitom ten nejdramatičtější růst se týkal právě platformy macOS. S ohledem na prudké výkyvy v cenách kryptoměn se můžeme pravidelně setkávat ať už s podvody nebo škodlivými kódy, protože v hledáčku útočníků jsou jak nakupující, tak držitelé," říká Kropáč.

Bezpečnostní experti doporučují uživatelům a uživatelkám zabezpečit své počítače kvalitním bezpečnostním softwarem, který je spolehlivě ochrání před infostealery i dalšími škodlivými kódy. V případě investičních podvodů pak doporučují vsadit na zdravou skepsi a obezřetnost. Podvodné scénáře bývají dnes propracované a kombinují dohromady několik technik tzv. sociálního inženýrství, jako je phishing či vishing. Součástí podvodů může být i deepfake obsah.

„Pokud si nejste jistí, že obsah, na který se díváte, není vygenerovaný umělou inteligencí, zaměřte se na to, zda osoba ve videu působí reálně, zda sedí pohyb rtů s tím, co říká, nemá trhané pohyby či zda mrká. Můžete také na sociálních sítích zkontrolovat, zda na podvodný obsah již někdo neupozornil. K šokujícím titulkům a reklamám přistupujte se zdravou skepsí. Pokud kliknete na reklamu a jste přesměrováni na jinou webovou stránku, vždy zkontrolujte její URL adresu," radí Kropáč z ESETu.

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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-macos-rizikem-byl-v-prvnim-ctvrtleti-2025-adware-zneuzivajici-seo-posilil-i-zlodej-kryptomen