Hrozby pro macOS: Škodlivé kódy ukrývá online reklama, cílem jsou kryptopeněženky

23.1.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Také v posledním čtvrtletí loňského roku byl největší hrozbou na platformě macOS v Česku a na Slovensku adware Pirrit.

Jeho přítomnost opět potvrdila pravidelná statistika kybernetických hrozeb od společnosti ESET za období od října do prosince 2024. Stejně jako v předchozím období jej opět v deseti procentech případů doplnil také infostealer PSW.Agent. Útočníci jej využívají ke krádežím dat pro přístup do kryptoměnových peněženek, dokumentů programů Word či Excel, krádežím přihlašovacích údajů z prohlížečů nebo souborů cookies. Útočníci k jeho šíření využívají reklamy v systému Googlu.

Vývoj na platformě macOS v Česku a na Slovensku byl v posledním čtvrtletí roku 2024 ve znamení jednoznačné převahy reklamního škodlivého kódu, adwaru Pirrit. Ve sledovaném období se objevil s podílem poloviny všech detekcí kybernetických hrozeb. V necelých deseti procentech případů ho nadále doplňuje malware PSW. Agent.

„Čísla ze závěru roku nám potvrzují, že předními hrozbami pro platformu macOS je v Česku nejen adware, ale také infostealer. Adware obtěžuje uživatele instalací nevyžádaných aplikací, které je mohou šmírovat. Škodlivý kód PSW.Agent se již řadí k malwaru určenému ke krádežím dat, a to včetně dat kolem kryptoměn a kryptoměnových peněženek, jako je například Electrum, Binance či Exodus. Dokáže odcizit také dokumenty programů Word či Excel, přihlašovací údaje z prohlížečů nebo soubory cookies, které mohou útočníci opět zneužít pro ověření na webu poskytovatele kryptoměn," vysvětluje Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

Oba typy škodlivých kódů šíří útočníci tak, že je vydávají za podvodné aplikace nebo doplňky ke stažení. V období od října do prosince 2024 tak bezpečnostní experti pozorovali, jak útočníci vydávají adware Pirrit i adware Bundlore za instalátor Flash Update, přičemž oficiální distribuce nástroje Flash Player skončila již v roce 2020. Malware PSW.Agent se poté nejčastěji maskoval za keygen nebo crack verze programů pro aplikace AutoCAD, ArchiCAD nebo za podvodný instalátor aplikace Zoom.

„V případě infostealerů bych uživatelům rozhodně doporučoval pořízení kvalitního bezpečnostního řešení. Jedná se totiž o riziko, které se týká nejen platformy macOS, ale také platformy Android nebo operačního systému Windows," vysvětluje Kropáč. „Útočníci šíří infostealery pro platformu macOS prostřednictvím legitimně vypadajících reklam v reklamním systému Google. Po kliknutí na reklamu jsou uživatelé přesměrováni na stránku, která je vyzve ke stažení nějakého programu. Ten je ale ve skutečnosti malwarem. Objevují se také případy, kdy oběti osloví na sociálních sítích nebo na online fórech domnělí investiční poradci. Jakmile si získají důvěru oběti, vyzvou ji ke stažení škodlivého softwaru. Doporučení uživatelům je tak stále stejné – stahovat aplikace a programy výhradně z obchodu App Store. Mají zde jistotu, že bezpečnostní týmy aplikace pravidelně prohledávají a hledají malware," doporučuje Kropáč.

Manipulativní komunikace spojená s falešnou nabídkou investic do kryptoměn byla také častým scénářem uplynulých několika měsíců. Podle poslední zprávy ESET Threat Report narostly nabídky falešných investic za období od června do listopadu 2024 o 335 %. Jak případ malwaru PSW.Agent, tak nárůst manipulativní phishingové komunikace jsou typickou strategií, jejímž cílem je zajistit

útočníkům finanční zisk. S tím, jak se v posledních měsících zvýšil opět zájem o investice do kryptoměn, je podle bezpečnostních expertů jen přirozené, že je útočníci opět v nějakém scénáři zahrnou do svých útočných kampaní.

„Kryptoměny dosáhly ve druhé polovině roku 2024 rekordních hodnot. Byla tak jen otázka času, kdy je útočníci ve svých útocích zneužijí. Phishingové útoky, které mohou být doplněny i falešnými telefonáty, tzv. vishingem, přitom vyžadují ostražitost a opatrnost už na straně samotného uživatele, kterému může podvodná zpráva přijít do e-mailu, chatovací aplikace nebo do SMS zprávy. V případě falešných investičních nabídek do kryptoměn útočníci využívají také technologie umělé inteligence k tvorbě deepfake obsahu – typicky nějakého videa, na kterém vystupují známí politici, podnikatelé nebo celebrity a doporučují uživatelům nějaký investiční produkt," vysvětluje Kropáč a dodává: „Kromě ochrany bezpečnostním softwarem je důležité, aby uživatelé a uživatelky začali velmi kriticky přistupovat ke všemu, co vidí na internetu, a vyvarovali se unáhleným reakcím a panice. V případě, kdy vám přijde nějaká naléhavá zpráva nebo telefonát, který vás například vystraší nebo zláká něčím senzačním, je vhodné se na chvilku zastavit a zeptat se sám sebe, zda komunikace vůbec dává smysl. Ideální je například z vlastní iniciativy kontaktovat oficiální zákaznickou linku, pokud se jedná například o zprávy z banky nebo jiných institucí. Pokud zní investiční nabídka až příliš dobře, slibuje například rychlé zisky až ve stovkách procent, nebude to s největší pravděpodobností pravda," dodává Kropáč z ESETu.

Kvalitní bezpečnostní software je vhodnou pojistkou pro případy, kdy přes všechnu opatrnost stáhneme malware do svého zařízení. Pokud bezpečnostní program rozpozná škodlivý kód v nějakém souboru, dokáže spuštění souboru zablokovat a přesunout ho do tzv. karantény, o čemž jsou uživatelé vždy informováni prostřednictvím dialogového okna.

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.

Lucie Mudráková

Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.cz

Vítězslav Pelc

Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.cz

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-macos-skodlive-kody-ukryva-online-reklama-cilem-jsou-kryptopenezenky