Hrozby pro macOS: Útočníkům se šířením malwaru pomáhají legitimní reklamní nástroje

12.11.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Podle poslední statistiky kybernetických hrozeb pro platformu macOS to zatím vypadá, že dlouhodobou převahu adwaru Pirrit postupně změní daleko závažnější infostealer PSW.Agent, jehož detekce se za třetí čtvrtletí letošního roku přehouply již přes 27 % zachycených případů. Vyplývá to z detekčních dat společnosti ESET pro Česko a Slovensko za období od července do září 2025. Nejen v případě tohoto škodlivého kódu útočníci využívají reklamní systém společnosti Google. Pomocí reklam totiž lákají i na stažení downloaderu Adload, který byl ve sledovaném období rovněž nezanedbatelným rizikem v našem regionu.

Ve třetím čtvrtletí letošního roku nadále rostl počet detekcí infostealeru PSW.Agent. Ten je zatím nejvýraznějším škodlivým kódem na platformě macOS v letošním roce a nechává za sebou i nechvalně proslulý adware Pirrit, který je hrozbou pro uživatele a uživatelky počítačů od Apple v našem regionu již několik posledních let.

„Infostealer PSW.Agent, který je znám i pod jménem Atmos Stealer či AMOS, dělá přesně to, co jemu podobné škodlivé kódy určené ke krádeži osobních údajů – rizikem je pro hesla a uživatelská data v zařízení, která jeho prostřednictvím útočníci napadnou. Specialitou tohoto malwaru jsou ale ještě i data kolem kryptoměnových účtů a peněženek, například služeb Electrum, Binance či Exodus. A protože jeden z našich letošních průzkumů potvrdil, že lidé v Česku mají zájmen o nákup kryptoměn, nemusí se tak jednat o riziko jen pro úzkou skupinu lidí," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

Útočníci při šíření infostealeru PSW.Agent využívají legitimně vypadající reklamy v reklamním systému Google. Pokud člověk na reklamu klikne, je přesměrován na webovou stránku a vyzván ke stažení nějaké aplikace. Jedná se ale pouze o její podvodnou verzi, která ukrývá škodlivý kód. V minulosti jsme se tak mohli setkat například s falešnými verzemi aplikací pro online meetingy a konference Zoom či Microsoft Teams.

„Uživatelům a uživatelkám bych doporučoval věnovat velkou pozornost komunikaci na internetu, a to nejen té příchozí po e-mailu či přes komunikační platformy, ale právě i té marketingové. Šíření infostealeru mohou útočníci podpořit i zdařilým příběhem, který nás má přesvědčit na něco kliknout nebo něco stáhnout. Je to běžná praxe, kterou pozorujeme i v případě kyberhrozeb pro další operační systémy nejen v České republice. Infostealery již patří k vážnějším hrozbám, proto je určitě na místě zvážit i pro počítače s platformou macOS profesionální ochranu v podobě bezpečnostního programu. Nejen, že dokáže chránit vaše data před škodlivými kódy, rozpozná ale například i podvodné aplikace, odkazy a webové stránky," dodává Kropáč.

Za období od července do září 2025 věnovali bezpečnostní experti pozornost také škodlivému kódu Downloader.Adload. I v tomto případě vsadili útočníci na techniky sociálního inženýrství a spolu s využitím malvertisingu lákali své oběti přes škodlivé Google reklamy na webové stránky, kde měly najít rady s řešením technických problémů na jejich zařízení.

„Stránky s technickou podporou byly samozřejmě podvrh a byly jen zdrojem malwaru. Zdánlivě

slibovaly uživatelům a uživatelkám řešení nefunkčního přehrávání médií, problémů se zvukem či s nedostatkem místa na disku. Jakmile chtěli uživatelé stáhnout a spustit soubor se slíbeným řešením anebo zadat doporučený příkaz do příkazového řádku, zahájil se proces stahování škodlivého kódu. Útočníci jich přitom nastražili hned několik a dle toho pak páchali škodlivou akci – krádež údajů, instalaci dalšího, nežádoucího softwaru, zobrazování agresivní reklamy a podobně. Uživatelům bych na tomto místě doporučoval obracet se vždy pouze na oficiální stránky s podporou pro jejich zařízení a zdravou skepsi v případě senzačních reklamních sdělení, na která na internetu narazí," říká Kropáč z ESETu.

S blokováním nebezpečných webových stránek a škodlivých kódů vždy pomůže kvalitní bezpečnostní software. Společnost ESET nyní svá řešení nabízí v akci 3za2 – od 1. září do 31. prosince 2025 mají zákazníci z řad domácností i firem možnost získat tříleté předplatné za cenu dvou let. Více informací o kampani, včetně seznamu konkrétních řešení a podrobných podmínek, najdete na webových stránkách společnosti ESET.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení digitální bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete 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 RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

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

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.

tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-macos-utocnikum-se-sirenim-malwaru-pomahaji-legitimni-reklamni-nastroje