Hrozby pro macOS: Obávaný infostealer se objevuje již v pětině případů

31.7.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Ve druhém čtvrtletí roku 2025 se do čela pravidelné statistiky pro platformu macOS v Česku a na Slovensku přesunul infostealer PSW.Agent. Vyplývá to z detekčních dat společnosti ESET za období od dubna do června 2025. Počet detekcí škodlivého kódu PSW.Agent zatím od začátku letošního roku neustále roste. Jeho cílem jsou kromě přihlašovacích jmen a hesel také data z oblasti kryptoměn a kryptoměnových peněženek. Bezpečnostní experti z ESETu proto doporučují, aby uživatelé a uživatelky vsadili na kvalitní ochranu a měli se na pozoru před manipulativní a podvodnou komunikací.

Zatímco ještě v prvním čtvrtletí letošního roku byl nejčastěji detekovaným škodlivým kódem adware MaxOfferDeal, v období od dubna do června byl již největším rizikem na platformě macOS v Česku a na Slovensku infostealer PSW.Agent. Ten se za sledované období objevil v pětině všech případů škodlivého kódu na této platformě a významně tak oproti minulým měsícům posílil.

„Na platformě macOS jsme v období od dubna do června sledovali nové uspořádání jednotlivých škodlivých kódů. Zatímco v minulosti se na prvním místě velmi často objevoval adware Pirrit, od začátku letošního roku se drží spíše zpátky na stabilní hodnotě okolo 10 procent detekcí. Od ledna také pozorujeme postupný nárůst případů infostealeru PSW.Agent, který se tentokrát objevil již v pětině všech případů," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

„V případě šíření tohoto infosteaIeru útočníci 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 pouze o škodlivý kód. Útočníci tento infostealer také velmi často ukrývají do pirátských a podvodných programů – tzv. cracknutých verzí nebo warez aplikací ke stažení. Na začátku letošního roku útočníci vydávali infostealer PSW.Agent například za aplikace pro online meetingy a konference Zoom či Microsoft Teams," vysvětluje Kropáč. „Infostealery jsou typem škodlivých kódů, které se zaměřují na krádež našich osobních dat. 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," doplňuje Kropáč.

Bezpečnostní experti doporučují svěřit ochranu před infostealery do rukou profesionálního bezpečnostního softwaru a zbytečně neriskovat stahováním nelegálních verzí programů mimo oficiální webové stránky výrobce či obchody s programy a aplikacemi. Naše osobní a citlivá data mají velkou cenu na černém trhu a útočníci vymýšlejí stále nové způsoby, jak se k nim dostat. Velkým rizikem jsou také útoky, ve kterých kombinují manipulativní techniky sociálního inženýrství spolu se škodlivými kódy. V případě podvodné komunikace je doporučením vsadit na obezřetnost, zdravou skepsi a mít na paměti, že současná podvodná komunikace může obsahovat i prvky deepfake obsahu vygenerovaného umělou inteligencí.

Podle poslední zprávy ESET Threat Report H1 2025, která mapuje globální vývoj kybernetických hrozeb od prosince 2024 do května 2025, vzrostly případy podvodného útoku ClickFix, a to o více než 500 %. Útoky ClickFix zobrazují obětem na webových stránkách falešnou chybu, která je manipuluje k tomu, aby zkopírovaly, vložily a spustily škodlivé příkazy na svém zařízení. Útoky jsou zacíleny na všechny hlavní operační systémy, včetně Windows, Linux a macOS.

„Podvodné útoky ClickFix se staly v minulém roce jednou z nejrychleji rostoucích kyberhrozeb a jsou v současnosti druhým nejčastějším typem útoku v rámci technik sociálního inženýrství, a to hned po phishingu. Pomáhají šířit řadu dalších hrozeb – ať už jsou to infostealery, nebo například ransomware, trojské koně využívané k získání vzdáleného přístupu, škodlivé kódy určené k těžbě kryptoměn, nástroje pro zneužívání zranitelností, a dokonce i vlastní malware napojený na státní aktéry," říká Kropáč z ESETu.

Jedním ze společných znaků podvodné komunikace je nás vystrašit a přimět k neuváženým krokům – rychle kliknout na vyskakovací okno nebo stáhnout přílohu či kliknout na odkaz v e-mailu, SMS nebo chatovací aplikaci. Bezpečnostní experti opět proto doporučují zachovat maximální obezřetnost, především při zacházení s našimi komunikačními platformami, a udržovat zařízení i všechny aplikace a programy v něm vždy aktuální, aby útočníci nemohli využít zjištěné zranitelnosti. S blokováním nebezpečných webových stránek a škodlivých kódů vždy pomůže kvalitní bezpečnostní software.

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 TruePositive 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-obavany-infostealer-se-objevuje-jiz-v-petine-pripadu