Hrozby pro macOS: Hackeři opět lákali na stažení aplikace Microsoft Teams, cílem bylo šířit infostealer

29.7.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Ve druhém čtvrtletí 2026 zůstal nejčastěji detekovanou hrozbou pro platformu macOS v Česku a na Slovensku infostealer PSW.Agent.

- Útočníci ho šíří prostřednictvím podvodu ClickFix. S jeho pomocí se snaží uživatele a uživatelky přesvědčit o vzniklé IT chybě a navést je na podvodné stránky s návodem na její řešení, které jsou ale zdrojem malwaru.
- V případě infostealeru PSW.Agent cílí konkrétně na ty, kteří vyhledávají aplikaci Teams nebo jiné aplikace od společnosti Microsoft pro platformu macOS. Využívají k tomu zmanipulované odkazy ve výsledcích vyhledávání pomocí optimalizace pro vyhledávače či škodlivé online reklamy.
- Specialitou infostealeru PSW.Agent jsou kromě hesel i data kolem kryptoměnových účtů a peněženek, například služeb Electrum, Binance či Exodus.
- Podvod ClickFix se podle poslední zprávy ESET Threat Report dále vyvíjí, nově na něj mohou uživatelé a uživatelky narazit například ve verzi tzv. AI-fix, a to na stránkách, které nabízejí nápovědu pro práci s AI nástroji.

Praha, 29. července 2026 – Největším kybernetickým rizikem pro platformu macOS v Česku a na Slovensku zůstal i ve druhém čtvrtletí infostealer PSW.Agent. Vyplývá to z detekčních dat pro tuto platformu od společnosti ESET za období od dubna do června 2026. Útočníci šíří škodlivý kód pomocí podvodné techniky, kterou bezpečnostní experti nazývají ClickFix. Pomocí manipulace nutí uživatele a uživatelky ke spuštění podvrženého systémového příkazu, přičemž používají falešná varování před možnými problémy s funkčností nebo ztrátou dat, pokud tak neučiní.

Útočníci se na platformě macOS v Česku a na Slovensku stále snaží šířit infostealery určené ke krádeži osobních dat. Nejnovější analýza škodlivých kódů za období od dubna do června 2026 to potvrdila – hlavním rizikem zůstává malware PSW.Agent, známý také jako MacStealer či AMOS Stealer.

„Ačkoli počet detekcí škodlivého kódu PSW.Agent nebyl ve druhém čtvrtletí tak vysoký jako na začátku letošního roku, stále zůstává v našem regionu rizikem. Je to především kvůli tomu, že útočníci k jeho šíření využívají podvod ClickFix, jednu z nejnovějších technik sociálního inženýrství," vysvětluje Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

Podvod ClickFix může mít řadu variant. Útočníci se obvykle snaží uživatele a uživatelky přesvědčit o nějaké vzniklé IT chybě a navést je na podvodné stránky s návodem na její řešení – například v podobě stažení nějaké aplikace či aktualizace nějakého programu.

V případě škodlivého kódu PSW.Agent je scénář následující: Útočníci cílí na uživatele a uživatelky, kteří vyhledávají aplikaci Teams nebo jiné aplikace společnosti Microsoft pro platformu macOS, a to zmanipulovanými odkazy ve výsledcích vyhledávání pomocí optimalizace pro vyhledávače či škodlivé online reklamy. To je ostatně způsob, který útočníci v případě škodlivých kódů pro platformu macOS využívají opakovaně. Jakmile uživatelé a uživatelky kliknou na podvodný odkaz ve výsledcích

vyhledávání, jsou přesměrováni na podvodnou ClickFix stránku. Tam najdou přesný návod, co je potřeba udělat pro úspěšnou instalaci aplikace. Útočníci je přinutí k vykonání příkazu v příkazovém řádku. Jako donucovací prostředek použijí falešné varování, že uživatel přijde o data nebo že aplikace přestane fungovat.

„Tím, že se uživatelé a uživatelky leknou a raději rychle splní kroky, které na podvodné stránce najdou, vpustí infostealer do svého zařízení. Specialitou infostealeru PSW.Agent jsou kromě hesel i data kolem kryptoměnových účtů a peněženek, například služeb Electrum, Binance či Exodus. Obrana před touto kybernetickou hrozbou je pak stejná jako v případě infostealerů u operačního systému Windows – vždy přítomná skepse k jakékoli nevyžádané komunikaci a pořízení kvalitního bezpečnostního softwaru," říká Kropáč.

Malware spojuje sílu s manipulací, která se rychle proměňuje

Ačkoli se podvod ClickFix nejprve objevoval v souvislosti s podvodnými výzvami CAPTCHA, i v jeho případě kyberútočníci využívají popularitu nástrojů generativní umělé inteligence. Kromě výše popsaného případu se ClickFix objevuje i v dalších scénářích – nově například na stránkách, které nabízejí nápovědu pro práci s AI nástroji, v rozšířeních internetových prohlížečů či při ověřování přístupu do cloudového prostředí.

„V naší poslední globální zprávě o kybernetických hrozbách ESET Threat Report jsme popsali i novou variantu AI-fix. Tyto případy nám bohužel ukazují, jak velkou důvěru jako uživatelé v generativní AI máme, a jak snadno se dá zneužít. V tomto případě vkládají kompromitované řetězce ClickFix do obsahu vygenerovaného nástroji umělé inteligence. Na webových stránkách, které zneužívají domény předních poskytovatelů AI služeb, pak opět nabízejí uživatelům a uživatelkám řešení neexistujících problémů," vysvětluje Kropáč a dodává: „Při klikání na reklamy a výsledky vyhledávání bychom měli vždy zkontrolovat, na jakou stránku jsme odkazováni a zda se jedná o přesměrování na věrohodnou URL adresu. Varováním by pro nás vždy měly být také senzační a lákavé nabídky, výhody či něco zdarma. Nejbezpečnější cestou je stahovat aplikace, programy a hry vždy pouze přes oficiální obchody s aplikacemi."

Nejčastější kybernetické hrozby v Česku a na Slovensku pro platformu macOS za období od dubna do června 2026:

1. OSX/PSW.Agent (48 %)
2. OSX/Adware.Pirrit (25 %)
3. OSX/Agent (6 %)
4. OSX/Adware.MacSearch (2 %)
5. OSX/Riskware.Frp (2 %)

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

O společnosti ESET

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

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