Hrozby pro macOS: V prvním čtvrtletí raketově narostly případy podvodu ClickFix

13.4.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

V prvním čtvrtletí letošního roku převládl na platformě macOS v Česku a na Slovensku podvod ClickFix – stál za třemi čtvrtinami všech zachycených útoků škodlivým kódem. Vyplývá to z detekčních dat společnosti ESET za období od ledna do března 2026.

Útočníci se zaměřili na uživatele a uživatelky, kteří vyhledávali aplikaci Microsoft Teams pro počítače s platformou macOS. Prostřednictvím zmanipulovaných výsledků vyhledávání je přesměrovávali na podvodnou ClickFix stránku, na které je pak přiměli vložit škodlivý skript do příkazového řádku. Tímto způsobem si stáhli a nainstalovali do zařízení infostealer určený ke krádeži dat. Podvody ClickFix jsou jednou z nových technik tzv. sociálního inženýrství. Útočníci při nich často pracují s naším strachem – pod záminkou nutné opravy nějaké chyby nebo hrozby pádu počítačového systému nás přinutí spustit ve svém zařízení škodlivý kód.

Česká a Slovenská republika byly v prvním čtvrtletí letošního roku cílem škodlivé kampaně, která dle bezpečnostních expertů ze společnosti ESET do určité míry stále probíhá. Útočníci k šíření malwaru tentokrát využili podvod ClickFix. Cílem nezvykle velkého počtu zachycených útoků byli tentokrát uživatelé a uživatelky počítačů od společnosti Apple.

„ClickFix je podvodná metoda spadající mezi techniky sociálního inženýrství. Jedná se o manipulativní komunikaci, která zneužívá lidské emoce a ze své podstaty je určitě srovnatelně nebezpečná s jinými kybernetickými útoky," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně. „Útočníci nejdříve nalákají oběť na škodlivou webovou stránku, a to buď pomocí SEO, optimalizace pro vyhledávače, nebo prostřednictvím škodlivé online reklamy. Na této stránce se pak objeví výzva k urgentnímu řešení nějakého problému, kterou doprovází dramatický kontext – když to uživatel neudělá, něco mu domněle nebude fungovat, něco se mu vymaže atd. Cílem je přimět uživatele zkopírovat a spustit útočníkem předem připravený příkaz do příkazového řádku. Tím ale nevědomky vpustí malware do svého zařízení," vysvětluje Jiří Kropáč.

Podvodníci chtějí tímto způsobem spustit v napadených zařízeních škodlivý kód Mac Stealer, který bezpečnostní experti z ESETu monitorují pod označením PSW.Agent. Ten se v případě platformy macOS v našem regionu vyskytuje dlouhodobě. Jedná se o infostealer, který sbírá a útočníkům obvykle odesílá uživatelská data a citlivé informace – uložená hesla k webovým stránkám, data ke kryptoměnovým peněženkám a další dokumenty.

Hledali Microsoft Teams, našli infostealer

Podvodný scénář útoku ClickFix může mít řadu různých variant. Typicky je uživatel vyzván k řešení nějaké opravy dočasné chyby. Útočníci ale mohou vyzvat svou oběť i ke stažení nějaké hledané aplikace nebo vynutit aktualizaci nějakého programu.

„V kampaních z prvního čtvrtletí letošního roku útočníci manipulovali výsledky vyhledávání pomocí SEO, optimalizace pro vyhledávače. Cílem byli uživatelé a uživatelky, kteří hledali aplikaci Microsoft Teams pro počítače s platformou macOS. Jakmile klikli na podvodný odkaz ve výsledcích vyhledávání, byli přesměrováni na podvodnou ClickFix stránku. Tam narazili na přesný návod, co je potřeba udělat k úspěšné instalaci aplikace. Útočníci je přiměli ke zkopírování a spuštění skriptu,

který byl na podvodné stránce uvedený. Touto lstí dostali do zařízení zmíněný infostealer, schovaný pod domněle oficiální aplikací, který měl následně ničím nerušenou cestu k uživatelským datům," dodává Kropáč z ESETu.

Infostealery jsou v Česku dlouhodobou hrozbou také v případě operačního systému Windows, kde se šíří především prostřednictvím podvodné e-mailové komunikace. Ukradené údaje a data pak útočníci prodávají na černém trhu. Následně mohou sloužit jako podklady pro přípravu dalších kybernetických útoků.

Právě nedostatečná kontrola při stahování aplikací a programů může stát za úspěšně provedeným kyberútokem. Nejbezpečnější cestou je stahovat aplikace, programy a hry vždy pouze přes oficiální obchody s aplikacemi a vyvarovat se senzačních nabídek lákajících na něco zdarma či na nějakou výhodu. Na malware pak mohou uživatelé a uživatelky narazit také na veřejných úložištích a fórech. Při klikání na reklamy a výsledky vyhledávání bychom tak měli vždy zkontrolovat, na jakou stránku jsme odkazováni a zda se jedná o přesměrování na věrohodnou URL adresu. Nejjistější ochranou před infostealery je pak bezpečnostní software, který malware a nežádoucí chování v zařízení včas rozpozná a škodlivou činnost zablokuje.

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

1. OSX/PSW.Agent (78,32 %)
2. OSX/TrojanDownloader.Agent (2,80 %)
3. OSX/Exploit.Agent (2,10 %)
4. OSX/Adware.Bundlore (2,10 %)
5. OSX/Spy.Agent (1,40 %)

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 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-v-prvnim-ctvrtleti-raketove-narostly-pripady-podvodu-clickfix