Hrozby pro macOS: Útočníci závěrem loňského roku kradli na počítačích od Apple uživatelská data

1.2.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

S více než třetinovým podílem všech zachycených detekcí uzavřel loňský rok na platformě macOS malware PSW.Agent. Jedná se o infostealer, který útočníci využívají ke krádeži citlivých a osobních údajů svých obětí. Vyplývá to z detekčních dat společnosti ESET pro Česko a Slovensko za období od října do prosince 2025. Bezpečnostní experti po celý loňský rok pozorovali vzrůstající počet detekcí tohoto malwaru, který pomalu zatlačil do pozadí dlouhodobě převládající adware. S proměnou kyberhrozeb pro počítače od společnosti Apple tak připomínají, že ani v případě této platformy by uživatelé a uživatelky neměli rezignovat na profesionální ochranu.

„Škodlivý kód PSW.Agent jsme na platformě macOS sledovali po celý loňský rok. Poslední čtvrtletí pak potvrdilo, že tu máme opravdu významnou změnu v rozložení škodlivých kódů. Zatímco v minulých letech jednoznačně převládal adware, tento rok ve všech sledovaných obdobích stále více přebíral pomyslné žezlo právě infostealer určený ke krádežím našich dat. Infostealery známe velmi dobře například z prostředí operačního systému Windows. Rád bych zde zdůraznil, že se jedná o poměrně zásadní zprávu pro uživatele a uživatelky počítačů od společnosti Apple. Jakkoli mohli v minulosti vnímat, že kybernetické hrozby pro tuto platformu bývají spíše mírnější, měli by nyní opravdu zpozornět. V případě infostealerů jsou v sázce naše osobní údaje, které mohou útočníkům zpřístupnit naše účty a cestu k našim penězům. Doporučoval bych jim tak zvážit kvalitní bezpečnostní software," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně.

Zatímco během roku 2025 šířili útočníci pod označením PSW.Agent především malware rodinu Atmos Stealer (AMOS), v posledním čtvrtletí loňského roku převládla rodina označovaná názvem Cuckoo infostealer. Obě rodiny infostealerů jsou si velmi podobné, jak po stránce svých funkcí, tak zacílení.

„I s využitím malwaru Cuckoo infostealer útočníci dokážou získat citlivá, osobní a jinak zajímavá uživatelská data. Jejich cílem nadále zůstala také data z prostředí kryptoměnových účtů a peněženek. Zajímají je také různé dokumenty nebo přihlašovací údaje k našim účtům," shrnuje Kropáč. „V posledním čtvrtletí jsme se nejvíce setkali s tím, že útočníci ukrývali malware pod falešné konvertory, tedy nástroje k převodům multimediálních souborů – jednalo se například o falešný program Spotify Music Converter nebo Amazon Music Converter. Pokud si uživatelé takový program stáhli, protože například chtěli stáhnout a převést hudební soubor z aplikace do formátu mp3, vpustili při spuštění nástroje škodlivý kód do svého počítače. Aby podpořili rozšíření těchto škodlivých nástrojů mezi uživatele, využili útočníci techniku SEO, Search Engine Optimization. Podobně, jako online reklamní specialisté v legitimních podnikatelských odvětvích," dodává Kropáč.

Stejně jako v případě jiných aplikací nebo her bezpečnostní experti doporučují, aby uživatelé a uživatelky vždy stahovali programy a nástroje pouze z oficiálních obchodů daných platforem, v tomto případě tedy z App Store. Spolehlivým zdrojem malwaru jsou naopak veřejná úložiště a uživatelská fóra. Zpozornět bychom měli vždy, když narazíme na nějakou výhodnou nabídku. Pokud nějaká aplikace slibuje vyřešení problému na počítači úplně zdarma, vždy by to měl být podle nich varovný signál.

V posledních třech měsících roku 2025 se na platformě macOS objevily i další typy škodlivých kódů, byť v daleko menším zastoupení, než tomu bylo v případě infostealeru. Jednalo se například o scareware nebo tzv. cryptominery.

„Škodlivý kód Downloader.Adload známe jako malware, který stahuje do zařízení další škodlivé kódy. V období od října do prosince loňského roku to tentokrát byly nejrůznější škodlivé čistící aplikace či nástroje určené k odinstalování programů. Downloader.Adload tyto škodlivé doplňky stahoval skrytě a ty se pak jako tzv. scareware snažili uživatele vystrašit nějakou urgentní zprávou o nutnosti nápravy a vyčištění jejího zařízení od nějaké hrozby," říká Kropáč. „V desetině všech případů se objevil i škodlivý kód OSAMiner určený ke skryté těžbě kryptoměn bez vědomí majitele zařízení. Uživatelé ho opět mohli nejčastěji stáhnout jako domnělou aplikaci pro údržbu operačního systému poté, co klikli na podvodné reklamní okno v internetovém prohlížeči. Útočníci jej využívají k těžbě kryptoměny Monero," dodává Kropáč z ESETu.

Bezpečnostní experti předpokládají, že s falešnými škodlivými programy a aplikacemi, které útočníci vydávají za legitimní služby známých značek, se budeme setkávat i v letošním roce. Profesionální bezpečnostní software dokáže uživatele ochránit nejen před pokročilými škodlivými kódy, jako jsou infostealery nebo ransomware, ale upozorní nás i v případě, kdy klikneme na nebezpečný odkaz, otevřeme nebezpečnou webovou stránku nebo se pokusíme stáhnout potenciálně nechtěnou a škodlivou aplikaci.

Uživatelé řešení 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-utocnici-zaverem-lonskeho-roku-kradli-na-pocitacich-od-apple-uzivatelska-data