# Hrozby pro macOS: Investice i Spotify, útočníci šíří škodlivé kódy v napodobeninách populárních aplikací

**17.10.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software**

**Adware Pirrit a malware PSW.Agent zůstávají nejčastěji detekovanými hrozbami pro platformu macOS v Česku a na Slovensku. Jejich přítomnost opět potvrdila pravidelná statistika kybernetických hrozeb od společnosti ESET, tentokrát za období od července do září 2024. Zatímco adware je kybernetickou hrozbou, kterou útočníci využívají především k instalaci škodlivých doplňků do prohlížeče či zobrazovaní nebezpečného či podvodného reklamního obsahu, škodlivý kód PSW.Agent využívají ke krádeži našich dat, a to jak přihlašovacích údajů do různých účtů, tak citlivých osobních dat, která poté dále mohou přeprodávat. Již několik měsíců jej útočníci také používají k získání přístupů do kryptopeněženek. Útočníci šíří oba typy škodlivých kódů prostřednictvím napodobenin legitimních aplikací, naposledy například prostřednictvím falešné aplikace pro investování Meta Trader či přehrávače Spotify.**

Ve třetím čtvrtletí letošního roku se na předních příčkách pravidelné statistiky opět objevily adware Pirrit a malware PSW.Agent. Zatímco adware Pirrit zobrazuje uživatelům na napadeném zařízení agresivní vyskakující okna s reklamou, má negativní vliv na výkon zařízení a rizikem se stává především ve chvíli, kdy prostřednictvím reklamy může odvést uživatele na nebezpečné webové stránky, malware PSW.Agent je již přímým rizikem pro naše data. Útočníci jej totiž využívají k jejich krádeži.

„Za poslední čtvrt rok vidíme, že detekce adwaru Pirrit jsou o něco vyšší než za posledně sledované období. Stále se nám tak potvrzuje, že se jedná o škodlivý kód, který mají útočníci v oblibě. Adware Pirrit se tentokrát nejčastěji šířil jako falešná verze aplikace pro investiční obchodování, MetaTrader," říká Jiří Kropáč, vedoucí výzkumné pobočky společnosti ESET v Brně. „Malware PSW.Agent, který je součástí širší rodiny malwaru Atomic Stealer, se vedle adwaru také pomalu stává stálicí mezi škodlivými kódy pro platformu macOS a jeho detekce zatím stabilně zůstávají okolo 11 procent. V minulém čtvrtletí se vydával především za cracky či warez programy různých komerčních aplikací. Tuto strategii útočníci stále neopustili. Při bližší analýze jsme například zjistili, že se tento škodlivý kód naposledy vydával za crack pro komerční aplikaci Adobe Illustrator. Útočníci však v jeho případě zvolili i další osvědčený postup a škodlivý kód ukryli do falešné verze známého přehrávače Spotify," doplňuje Kropáč.

„Malwaru se uživatelé mohou bezpečně vyhnout tak, že budou aplikace a programy stahovat výhradně z App Store a vyvarovat se různých internetových fór a pochybných obchodů třetích stran. V jejich případě mají jistotu, že spolu s domnělou aplikací stáhnou jako bonus také nějaký škodlivý kód. Malware bývá dnes také součástí propracovaných manipulativních útoků, při kterých útočníci sázejí na naše emoce, především na strach a zvědavost. K šíření adwaru i spywaru mohou využívat komunikaci prostřednictvím e-mailu i chatovacích aplikací. V nevyžádaných zprávách bychom nikdy neměli otevírat přiložené soubory, stahovat je do zařízení a klikat na odkazy," varuje Kropáč.

Jsou to právě zvučná jména populárních aplikací, která lákají útočníky k tomu, aby je zapojili do svých útočných kampaní proti uživatelům. Podle zprávy Threat Report H1 2024 se již v první polovině letošního roku objevily případy, při kterých útočníci zneužili jména nástrojů generativní umělé inteligence. Malware vydávali za napodobeniny služeb Midjourney, Sora nebo Gemini. Tyto

falešné aplikace inzerovali také prostřednictvím legitimních nástrojů na sociální síti Facebook.

Infostealery přitom i v České republice patří mezi největší současná rizika pro běžné uživatele. Právě k tomuto typu hrozby se řadí již zmíněný škodlivý kód PSW.Agent.

„Na základě naší analýzy můžeme potvrdit, že se malware PSW.Agent cíleně zaměřuje na informace a data kolem kryptoměn a kryptoměnových peněženek. Z účtů a ze zařízení dokáže odcizit soubory kryptoměnových peněženek, jako je například Electrum, Binance či Exodus. Odcizí ale také dokumenty programů Word či Excel. Jeho cílem jsou dále i přihlašovací údaje z prohlížečů nebo soubory cookies, které může zneužít pro ověření na webu poskytovatele kryptoměn," vysvětluje Kropáč.

Jako v řadě jiných případů, i malware PSW. Agent útočníci šíří přes sponzorované odkazy ve vyhledávačích, a to hlavně v případě internetového vyhledávače Chrome a služby Google AdSense, nebo obecně prostřednictvím podvodných aktualizací a bannerů. Využívají tak legitimní nástroje online marketingu pro účely kyberkriminální činnosti.

Počítače a chytré telefony od značky Apple se dlouhodobě těší pověsti bezpečných zařízemí, kterým se kybernetické útoky vyhýbají. Jak ale potvrzují bezpečnostní experti, i útoky na tyto platformy existují. Na rozdíl od jiným operačních systémů nejsou ale tak časté.

„Platformu macOS si můžeme představit jako konkurenci k operačnímu systému Windows. Oproti operačnímu systému iOS, se kterým se uživatelé setkávají v případě mobilních telefonů iPhone, je také daleko otevřenější a útočníci se na ni více zaměřují. Je však důležité dodat, že uživatelů s touto platformou je daleko méně než uživatelů s operačním systémem Windows. Nové útoky se tak objevují většinou se zpožděním a není jich tolik," říká Kropáč z ESETu.

S ohledem na hrozby v podobě adwaru a infostealerů pak doporučuje dávat pozor na manipulativní komunikaci, která uživatelům přijde bez předchozího vyžádání, a pečlivě volit, odkud stahujeme aplikace a programy. Kvalitní bezpečnostní software je pak další pojistkou pro případy, kdy přes všechnu opatrnost stáhneme malware do svého zařízení. Pokud bezpečnostní program rozpozná škodlivý kód v nějakém souboru, dokáže spuštění souboru zablokovat a přesunout ho do tzv. karantény, o čemž jsou uživatelé vždy informováni prostřednictvím dialogového okna.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete 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.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze,

celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-macos-investice-i-spotify-utocnici-siri-skodlive-kody-v-napodobeninach-popularnich-aplikaci