# Hrozby pro macOS: Zdrojem adwaru byly v únoru falešné aplikace pro stažení torrentů

**7.3.2024 - Rita Gabrielová, Lucie Mudráková | ESET software**

**Mezi nejčastějšími únorovými kybernetickými hrozbami pro platformu macOS se opět objevily adware Pirrit a Bundlore. Po delší odmlce se na přední příčky vyšplhal také adware MaxOfferDeal, který útočníci šíří s využitím optimalizace pro vyhledávače, SEO. Škodlivé kódy se v únoru nejvíce objevovaly v aplikacích pro stahování torrentů a nelegitimního softwaru. Útočníci tak uživatele znovu lákají na filmy, seriály nebo programy zdarma. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.**

Do čela pravidelné statistiky kybernetických rizik pro platformu macOS se v únoru opět vrátil adware Pirrit. Dlouhodobý zástupce adwaru je už několik let v Česku stabilní hrozbou. Útočníci ho šíří prostřednictvím různých aplikací nebo nástrojů a kromě toho, že má negativní vliv na výkon zařízení a znepříjemňuje práci na počítači při procházení internetu, může být prostředníkem ke stažení dalšího malwaru.

„V únoru se mezi detekovanými falešnými aplikacemi, jejichž prostřednictvím se adware a další škodlivé kódy šíří na platformě macOS nejčastěji, objevily převážně nástroje pro stahování torrentů a cracknutého softwaru. Je tak zajímavé sledovat, že útočníci zvolili zrovna tyto nástroje, aby uživatele přiměli ke stahování mimo oficiální místa. Filmy, seriály nebo software zdarma jsou tak pro uživatele stále evidentně lákadlem," říká Jiří Kropáč, vedoucí virové laboratoře společnosti ESET v Brně.

Kromě podvržených aplikací Torrent Downloader a Crack Installer se nadále objevuje falešná aplikace Adobe Flash Player installer. Konkrétně v jejím případě bezpečnostní specialisté opakovaně upozorňují na to, že podpora Adobe Flash Playeru byla ukončena v roce 2020 a na oficiálních distribučních místech již není v nabídce.

Kromě adwaru Pirrit a adwaru Bundlore se v únoru v detekcích opět objevil adware MaxOfferDeal. Ačkoli se tento škodlivý kód neobjevuje ve statistice nijak pravidelně, i na něj mohou uživatelé v Česku narazit již několikátým rokem.

„Adware, jak už jeho název napovídá, je reklamní škodlivý kód. Jeho přítomnost v zařízení se projevuje právě velkým množstvím vyskakovacích oken s různými reklamními nabídkami, a to často poměrně agresivním způsobem, kdy například tato okna nejdou vůbec zavřít, nebo jsou jimi uživatelé zahlceni. Většinou do zařízení stahuje další adware nebo nechtěné doplňky do prohlížečů bez svolení uživatelů, ale útočníci mohou prostřednictvím adwaru zobrazovat i podvodné reklamy nebo reklamní bannery s odkazy na nebezpečné webové stránky. Adware MaxOfferDeal pak útočníci šíří i pomocí optimalizace pro vyhledávače, SEO, známého nástroje online marketingu. Díky tomu dokáží uživatelům nabídnout falešné aplikace nebo programy přímo mezi výsledky vyhledávání na internetu," říká Kropáč.

Manipulativní komunikace je v prostředí kybernetických hrozeb jednou z hlavních strategií, jak si útočníci hledají cesty k uživatelům a jejich cenným datům. Kromě phishingu, vishingu a dalších technik sociálního inženýrství však útočníci manipulují uživatele i lákavými nabídkami oblíbených programů či her.

„Většina uživatelů stále bohužel podceňuje motivace kybernetických útočníků. Ti se přitom snaží být stále o krok napřed za pomoci nových technologií a pečlivou přípravou svých útoků, a to i po stránce

sledování populárních trendů a toho, co na internetu hledáme a co nás zajímá. Řada útoků je dnes již automatizovaná, takže se opravdu může stát, že se na vás zaměří útočník i když vy si myslíte, že jste pro něj nezajímavá osoba. Čím větší počet uživatelů zasáhne, tím víc zvyšuje pravděpodobnost úspěšnosti svého útoku. Pokud si toto uživatelé uvědomí, je to první krok k větší osobní bezpečnosti v digitálním světě, který je již dnes naší neoddělitelnou součástí," dodává Kropáč z ESETu.

Také v případě platformy macOS by uživatelé měli stahovat aplikace výhradně z oficiálního obchodu App Store, kde je bezpečnostní týmy pravidelně kontrolují na přítomnost škodlivého kódu. Před adwarem, potenciálně nechtěnými aplikacemi i webovými hrozbami je pak ochrání moderní bezpečnostní řešení. Spolu s ním mohou uživatelé získat celou řadu dalších nástrojů, jako je například správce hesel nebo virtuální privátní síť VPN.

Uživatelé produktů 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 také 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 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 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-zdrojem-adwaru-byly-v-unoru-falesne-aplikace-pro-stazeni-torrentu