

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **25** ze dne **3.1.2023**

Hrozby pro macOS: Adware Pirrit je opět nejsilnější závěrem roku, rizikem je pro naše soukromí na internetu

Adware Pirrit, který je dlouhodobě rizikem pro české uživatele operačního systému macOS, se v listopadu objevil ve více než třetině všech detekovaných případů. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET. Počet jeho detekcí přitom již několikrát měsíc kontinuálně roste a podobně, jako v případech jiných škodlivých kódů, se vrcholu blíží především na přelomu roku. Ke svému šíření v listopadu využíval aplikaci SearchUp, uživatelé na něj ale mohli narazit také po kliknutí na online reklamní bannery, na stránkách s torrenty nebo ve výhodných balících spolu s jiným softwarem.

Podle očekávání bezpečnostních specialistů vzrostl počet detekcí adwaru Pirrit právě nyní na konci roku.

„V listopadu detekce adwaru Pirrit opět narostly. Důvodem bude pravděpodobně to, že uživatelé začali daleko více stahovat aplikace a nástroje mimo oficiální obchody a webové stránky. Mohou to přitom dělat buď záměrně ve snaze ušetřit za nějaký prémiový program nebo placenou hru, nebo zkrátka zadají název aplikace do vyhledávače a již pro ně dále nehraje roli, z jakého místa ji stáhnou,“ vysvětluje Jiří Kropáč, vedoucí virové laboratoře společnosti ESET v Brně.

Adware Pirrit se v listopadu šířil prostřednictvím aplikace SearchUp a jeho přítomnost v zařízení se poté klasicky projevovala dotěrnými a agresivními reklamními kampaněmi. Útočníci prostřednictvím adwaru Pirrit dokážou sbírat osobní informace o uživateli a systému macOS včetně toho, jaká vyhledávají při prohlížení internetu klíčová slova a jaké navštěvují webové stránky.

Útočníci si nás zanalyzují podle vyhledávaných slov a navštívených stránek

Mezi hlavní funkce adwaru patří zobrazování agresivní reklamy a negativně se projevuje na výkonu infikovaného zařízení. Přesto bezpečnostní experti upozorňují, že by ho uživatelé neměli rozhodně považovat za neškodný a ani v případě systému macOS rezignovat na kvalitní zabezpečení.

„Uživatel obvykle přítomnost adwaru v zařízení hned neodhalí. Upozorní ho až některé, poměrně nápadné ukazatele, že něco s jeho zařízením není v pořádku. Při používání počítače se pak typicky objevují vyskakovací reklamní pop-up okna, prohlížení webového obsahu je pomalé a celkově je snížený uživatelský komfort. Uživatel může být také náhle přesměrován na podvodné reklamní stránky, které nabízejí různé produkty nebo služby. Útočníci přitom tyto stránky mohou přizpůsobit tomu, co o uživateli ví právě podle historie navštívených stránek a vyhledávaných klíčových slov. Do internetového prohlížeče pak také mohou být instalována další rozšíření třetích stran, aniž by k tomu uživatel dal pokyn. Prostřednictvím těchto rozšíření pak mohou útočníci sbírat další informace o uživateli a nastavení systému a sdílet je s třetími stranami bez jejich vědomí,“ shrnuje Kropáč.

Adware se šíří prostřednictvím online reklamy, torrentů nebo spolu s dalším softwarem

Nejen adware Pirrit, ale i další nejčastěji detekované škodlivé kódy se v listopadu opět šířily především

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **25** ze dne **3.1.2023**

prostřednictvím neoficiálních obchodů třetích stran. Adware přitom mohou útočníci používat ve větší míře právě proto, že k jeho stažení často dochází vlivem naší neopatrnosti a jeho šíření je tak jednoduché a nevyžaduje větší náklady.

„Pokud uživatelé stahují aplikace výlučně z App Store, výrazně tím snižují riziko, že své zařízení adwarem infikují,“ říká Kropáč a dodává: „Mimo oficiální distribuci se adware v listopadu šířil také prostřednictvím reklamních bannerů nebo jako součást dalšího softwaru zdarma. Stále také vidíme, že se ukrývá v podvodné aplikaci k instalování Adobe Flash Playeru, přičemž oficiální vývoj tohoto programu byl již ukončen. A na adware můžeme narazit samozřejmě také na různých serverech s torrenty, kde se opět vydává za nějaké známé aplikace.“

Uživatelé počítačů od Apple může účinně chránit spolehlivý bezpečnostní software, a to nejen před potenciálně nechtěnými aplikacemi (tzv. PUA), ale také před webovými stránkami, které mohou být zneužity k různým podvodům či k šíření malwaru.

Nejčastější kybernetické hrozby v České republice pro platformu macOS za listopad 2022:

- OSX/Adware.Pirrit (37,50 %)
- OSX/TrojanProxy.Agent (10,83 %)
- OSX/Adware.MacSearch (6,67 %)
- OSX/TrojanDownloader.Adload (5,83 %)
- OSX/Adware.Bundlore (4,17 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: ESET