Hrozby pro macOS: Detekce adwaru Pirrit se v závěru roku vyšplhaly až ke 40 % všech zachycených případů

10.1.2024 - Rita Gabrielová , Lucie Mudráková | ESET software

Detekce adwaru Pirrit dosahovaly v loňském prosinci téměř 40 procent všech zachycených případů škodlivého kódu na platformě macOS v Česku a na Slovensku.

Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET. Adware Pirrit je již několikátým rokem v českém prostředí stabilní hrozbou a útočníci ho často šíří prostřednictvím různých nelegitimních verzí aplikací. Podle výhledu bezpečnostních expertů pro letošní rok se s ním čeští uživatelé budou setkávat i nadále.

Detekce adwaru Pirrit, hlavního kybernetického rizika na platformě macOS v Česku a na Slovensku, se na konci roku vyšplhaly až k podílu 40 procent všech zachycených detekcí. S adwarem Pirrit se mohli uživatelé v Česku setkávat průběžně celý uplynulý rok a útočníci tak opět potvrdili, že se jedná o jejich oblíbený škodlivý kód.

„Adwaru se nejen v Česku daří dlouhodobě. Uživatelé mu zpravidla nevěnují takovou pozornost jako jiným škodlivým kódům a nepovažují ho za nebezpečný, což se jim ale může vymstít – adware může stahovat do zařízení daleko závažnější škodlivé kódy a získávat informace o tom, co děláme na internetu,“ říká Jiří Kropáč, vedoucí virové laboratoře společnosti ESET v Brně.

„V letošním roce je opět pravděpodobné, že adware bude v Česku nadále hlavní hrozbou. S rostoucím počtem uživatelů zařízení od Apple se nejen zvyšuje počet potenciálních obětí, ale také se může zvýšit cílenost a sofistikovanost útoků. Adware je často podceňovaný, i když může představovat vážné bezpečnostní riziko. Mnoho uživatelů považuje adware za méně nebezpečný než jiné formy malware, jako jsou viry nebo trojany. Tento názor může vést k nedostatečné ochraně a opatrnosti,“ dodává Kropáč.

Adware Pirrit se dlouhodobě šíří prostřednictvím falešných verzí různých více či méně populárních aplikací, které uživatelé nejčastěji stáhnou v obchodech třetích stran, na internetových úložištích nebo na různých fórech. Příkladem může být aplikace Adobe Flash Player, kterou útočníci stále nabízejí ke stažení, přestože její oficiální verze již neexistuje.

Mezi dalšími hrozbami byly i v prosinci škodlivý kód Downloader.Adload či Proxy.Agent. Oba typy jsou podle bezpečnostních expertů dobrým příkladem, proč by uživatelé neměli rizika na platformě macOS podceňovat.

„Trojský kůň Downloader.Adload je typem škodlivého kódu, který poté, co infikuje zařízení, do něj dál stahuje nějaké komponenty nebo doplňky pro internetový prohlížeč, ale bez vědomí uživatele. Cílem škodlivého kódu Proxy.Agent je zase sledovat odchozí webovou komunikaci a aktivitu uživatele na internetu. Tím, že útočníci získají informace o chování uživatelů na internetu, mohou následně upravovat příchozí webovou komunikaci tak, že změní výsledky vyhledávání ve vyhledávači. Upřednostní svůj obsah, který může být zavádějící nebo podvodný, nebo přesměrují uživatele na preferovanou webovou stránku, například do nějakého e-shopu,“ říká Kropáč.

Škodlivý kód Proxy.Agent tak funguje jako lokální webový proxy server, přes který probíhá

komunikace internetového prohlížeče Safari nebo Firefox.

Adware se nejvíce vyznačuje velkým množstvím vyskakujících reklamních oken, stahováním nepovolených doplňků do internetového prohlížeče nebo zpomalením výkonu zařízení.

„Díky těmto ukazatelům mohou uživatelé postřehnout, že s jejich zařízením není něco v pořádku. Právě agresivní reklama může být pro útočníky také nástrojem, jehož prostřednictvím mohou šířit různá podvodná sdělení. Uživatelům bych rozhodně doporučil stahovat aplikace a nástroje pouze z oficiálního obchodu App Store a využívat i pro ochranu před adwarem kvalitní bezpečnostní software,“ říká Kropáč z ESETu.

Moderní a kvalitní bezpečnostní řešení již dnes není pouhým antivirem, ale nabízí spolu s ochranou před kybernetickými riziky i 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 produktů 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-detekce-adwaru-pirrit-se-v-zaveru-roku-vysplhaly-az-ke-40-vsech-zachycenych-pripadu