V říjnu se adware šířil falešnými aplikacemi pro sledování a stahování videí na YouTube

13.1.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Adware Pirrit zůstal s pětinou všech detekovaných případů i v říjnu nejčastějším škodlivým kódem pro platformu macOS v Česku a na Slovensku.

Stejně jako škodlivý kód Downloader.Adload se tentokrát šířil prostřednictvím falešných verzí aplikací pro stahování videí nebo pro jejich sledování bez reklam na platformě YouTube. Bezpečnostní specialisté proto varují uživatele, aby aplikace a programy nadále stahovali pouze z oficiálního obchodu App Store. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Adware Pirrit se v říjnu podle posledních dat pravidelné statistiky objevil v pětině všech případů a zatím nepokračuje v tempu, které bezpečnostní specialisté pozorovali letos v září. Upozorňují však na to, že v říjnu se mohli uživatelé setkat s napodobeninami aplikací známé platformy pro sdílení videí YouTube.

„Detekce adwaru Pirrit v říjnu nepřekročily hranici počtu detekcí ze září, objevily se nicméně nové napodobeniny aplikací, které adware využívá ke svému šíření. Podobná strategie se v říjnu potvrdila také v případě dalšího nejčastěji detekovaného škodlivého kódu, Downloaderu.Adload. Oba dva zástupce škodlivého kódu jsme objevili v aplikacích ListenToYouTube a Youtube mp3 converter. Útočníci tak zacílili na fanoušky této platformy a nabízeli jim falešné aplikace lákající na reklamami nerušené přehrávání videí a hudby anebo stahování videí ve formátu mp3. V obou případech samozřejmě tyto aplikace nefungovaly tak, jak měly, a stahovaly do počítače další adware a nežádoucí obsah," říká k říjnovému přehledu hrozeb Jiří Kropáč, vedoucí virové laboratoře společnosti ESET v Brně.

Mezi nežádoucími aplikacemi, které škodlivé kódy stahovaly prostřednictvím falešných verzí YouTube aplikací do zařízení uživatelů, byly například Mackeeper nebo YouTubeDownloader.

Bezpečnostní experti upozorňují uživatele na to, aby nepodceňovali ochranu před adwarem, a to i přes to, že není tolik závažným škodlivým kódem jako například spyware nebo ransomware. V konečném důsledku může prostřednictvím agresivní reklamy inzerovat odkazy na webové stránky s podvodným nebo nebezpečným obsahem a být rizikem pro naše soukromí.

„Tím, že adwaru nemusí řada uživatelů věnovat takovou pozornost, jako jiným škodlivým kódům, stává se pro útočníky vhodným nástrojem, jak se dostat do jejich zařízení. Pro šíření adwaru se přitom nezdráhají využít ani dostupné nástroje online marketingu. Příkladem může být adware MaxOfferDeal, který v říjnu také patřil k nejčastějším škodlivým kódům – k jeho šíření využívají útočníci optimalizaci pro vyhledávače neboli SEO a díky tomu dokáží uživatelům poskytnout nabídky falešných aplikací nebo programů přímo mezi výsledky vyhledávání na internetu," doplňuje Kropáč.

Kromě zabezpečení počítače kvalitním bezpečnostním řešením je pak účinná obrana před adwarem a dalšími riziky, která se s ním pojí, přímo v rukou samotných uživatelů. Ti totiž mohou na adware nejčastěji narazit při stahování aplikací a programů na internetových úložištích nebo v neoficiálních obchodech třetích stran.

„Uživatelé mohou hledat aplikace a programy mimo oficiální obchody v domnění, že ušetří nebo že

program pořídí za výhodnou cenu. Právě tak na ně útočníci cílí – známé aplikace nabízejí zdarma, pokud jsou jejich legitimní verze zpoplatněné, nebo ve výhodných balíčcích s jiným softwarem. V konečném důsledku se ale s ohledem na jejich bezpečnost daleko více vyplatí, když budou aplikace stahovat výhradně z oficiálního obchodu společnosti Apple, App Store," říká Kropáč z ESETu.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

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-v-rijnu-se-adware-siril-falesnymi-aplikacemi-pro-sledovani-a-stahovani-videi-na-youtube