Hrozby pro macOS: V lednu se nově objevila falešná aplikace slibující prolomení zabezpečení iPhonu

12.2.2024 - | ESET software

V lednu letošního roku zaznamenali bezpečnostní specialisté pokles detekcí hrozeb pro platformu macOS v Česku a na Slovensku.

I přesto se nově objevila falešná aplikace MinaUSB patcher, ve které se ukrýval a jejím prostřednictvím se šířil adware Pirrit. Aplikace slibovala uživatelům domnělou funkcionalitu k provedení tzv. jailbreaku zařízení se systémem iOS, tedy možnost obejít zabezpečení stanovené výrobcem. Aplikace však po stažení nefungovala a pouze dále stahovala reklamní škodlivý kód do zařízení. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Bezpečnostní specialisté zaznamenali v lednu letošního roku výraznější pokles detekcí na platformě macOS. Nadále však mezi objevenými případy stabilně zůstávají všechny známé škodlivé kódy, které se dlouhodobě na této platformě v Česku a na Slovensku objevují.

„Zatímco koncem roku jsme viděli, jak se počet detekcí adwaru Pirrit, který je již několik let přední hrozbou v našem prostředí, znatelně zvýšil, v lednu je naopak vidět u všech detekovaných hrozeb výraznější pokles. I když by se nyní mohlo zdát, že se škodlivé kódy na platformě macOS postupně vytrácí a zařízení s tímto operačním systémem tak jsou méně vystavená kybernetickým rizikům, nemusí to tak být a uživatelé by neměli získat dojem, že jim nehrozí žádné nebezpečí. Útočníci mohou takové období využít k vyzkoušení nových typů hrozeb nebo strategií," říká Jiří Kropáč, vedoucí virové laboratoře společnosti ESET v Brně.

Detailnější analýza lednových hrozeb tento scénář také potvrdila. Adware Pirrit útočníci tentokrát nově šířili ukrytý v podvodné kopii aplikace MinaUSB patcher.

„Aplikace MinaUSB patcher slibovala uživatelům možnost prolomit bezpečnostní prvky v zařízeních Apple, jako je například iPod, iPhone nebo iPad. Tomuto prolomení číselného zámku výrobce se říká jailbreak a díky tomuto kroku by uživatelé získali mimo jiné i možnost stahovat do zařízení aplikace mimo App Store, což jim za standardních okolností Apple nepovoluje. Útočníci cílili na uživatele platformy macOS pravděpodobně kvůli tomu, že v jejím případě je stahování mimo oficiální obchod možné a že všechny produkty od společnosti Apple lze spolu pohodlně propojit. Falešná aplikace ve skutečnosti ale domnělou funkcionalitu jen předstírala a zařízení odblokovat nedokázala. Pouze do počítače instalovala adware, který pak následně může sledovat aktivity uživatelů na internetu," vysvětluje Kropáč.

Šířit škodlivý kód prostřednictvím falešných aplikací, které ale slibují zajímavé funkce nebo již v oficiálních obchodech nejsou dostupné, je stále jedna z nejčastějších strategií, jak dostat adware i trojské koně do našich zařízení.

Kromě falešné aplikace MinaUSB patcher se v lednu opět objevila i podvodná aplikace Adobe Flash Player. Jejím prostřednictvím se tentokrát šířil adware Bundlore. Jak bezpečnostní experti ale opakovaně upozorňují, oficiální verze této aplikace již neexistuje a uživatelé by tak před těmito nabídkami stažení měli být vždy maximálně ostražití.

„Uživatelé mohou mít v případě adwaru pocit, že jim nehrozí žádné velké nebezpečí mimo agresivní a obtěžující reklamu nebo zhoršení výkonu jejich zařízení. Proto jim někdy možná stojí za to stáhnout aplikaci i mimo oficiální distribuční místa. Typicky je k tomu motivuje i to, že mimo známé obchody mohou být aplikace zdarma, nebo právě získají oblíbenou aplikaci, i když už oficiálně není k dispozici. I adware ale může stahovat do zařízení další a daleko nebezpečnější škodlivý kód. V poslední době je stále více také rizikem pro naše soukromí na internetu, protože útočníci díky němu dokáží sledovat naše online aktivity," doplňuje Kropáč z ESETu.

To, že si útočníci hledají cestu k uživatelům systému iOS, není žádným překvapením. Díky své architektuře jsou tato zařízení na rozdíl od počítačů s operačním systémem macOS daleko bezpečnější – aplikace v zařízení spolu mohou totiž komunikovat jen velmi omezeně. Právě takzvaný jailbreak může ale tyto bezpečnostní prvky obejít a vystavit tak zařízení a data uživatelů potenciálnímu nebezpečí.

„Jailbreak je modifikace operačního systému. Na jednu stranu uživatel získá nejvyšší oprávnění, ale na druhé straně vystavuje své zařízení útokům, protože odemkne přístup k citlivým částem zařízení," říká Kropáč a dodává: „Uživatelé mohou díky jailbreaku do iPhonu či iPadu instalovat aplikace, které nejsou k dispozici v oficiálním obchodě App Store, to ale znamená, že už nebudou chráněni v případě, kdy taková aplikace nebude bezpečná. Navíc je provedení jailbreaku považováno za porušení licenční smlouvy."

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 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-vlednu-se-nove-objevila-falesna-aplikace-slibujici-prolomeni-zabezpeceni-iphonu