ESET
ENJOY SAFER TECHNOLOGY™

Vývoj hrozeb pro zařízení Mac

Obecná představa, že Apple zařízení fungují bez povšimnutí kybernetických útočníků, je mylná. Jaké jsou nejčastější hrozby a jak se před nimi chránit?

Nejčastější hrozby pro MacOS:

- **Potenciálně nechtěná aplikace** (PUA)
- **Reklamní malware** (Adware)
- **Potenciálně zneužitelná aplikace** (PUsA)
- **Trojan**

Potenciálně nechtěná aplikace

je široká kategorie softwaru, jejíž záměr není tak jednoznačně škodlivý jako u jiných typů škodlivého kódu. Může však nainstalovat další nežádoucí software, změnit chování digitálního zařízení nebo provádět činnosti, které uživatel neschválil.

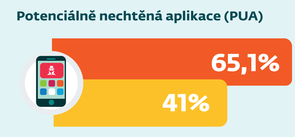
Adware

neboli reklamní malware řadíme do kategorie programů, jejichž úkolem je zobrazovat reklamy. Adware společně s potenciálně nechtěnými aplikacemi patří k nejvíce monetizovaným a mají společné vektory šíření – vyznačují se specifickými technikami pro zabránění detekce a snaží se o ztížení analýzy jejich činnosti.

Potenciálně zneužitelné aplikace

nepředstavuje přímou hrozbu pro uživatele, ale může obsahovat nástroje zneužitelné malwarem.

Vývoj hrozeb za první pololetí letošního roku:



Zabezpečení pro uživatele MacOS

Apple má specifickou bezpečnostní strategii nazývanou „zahrada za zdí" (walled garden). Jedná se o uzavřený ekosystém, který ztěžuje infikaci zařízení. Klíčovým prvkem je technologie zvaná Gatekeeper, která hlídá, aby se na Macu spouštěl jenom prověřený software. Aplikace, které kontrolou neprojdou, lze nainstalovat pouze s výslovným souhlasem uživatele.

Jak hrozbám předcházet:

- K nákupu a stahování aplikací používat výhradně App Store.
- Nestahovat aplikace z nedůvěryhodných zdrojů.
- Vyhnout se stahování a instalaci Flash Playeru.
- Být obezřetný při zadávání citlivých údajů na internetu.
- Používat bezpečnostní software.