TLP:CLEAR
Szabadon terjeszthető!

Riasztás magyar macOS felhasználókat célzó Odyssey Stealer kampányról

Tisztelt Ügyfelünk!

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** (NBSZ NKI) riasztást ad ki a magyar **macOS felhasználókat is célzó Odyssey Stealer** kampány kapcsán. A rendelkezésre álló elemzés szerint több mint húsz különböző, macOS-specifikus fertőzési minta köthető az Odyssey Stealer kártevőcsaládhoz. A támadók **legitimnek látszó, azonban kártékony kódot tartalmazó szoftvercsomagokkal** próbálják megtéveszteni a felhasználókat, köztük TradingView és CleanShot utánzatokkal. **A kampány célja a digitális identitás, a hitelesítő adatok és a kriptovaluta vagyon megszerzése.**

A kártevő a fertőzött rendszerekről képes lehet a böngészőkben **tárolt jelszavak, aktív munkamenet cookie-k és automatikus kitöltési adatok megszerzésére, hamis rendszerüzenetek megjelenítésére továbbá hozzáférést szerezhet a kriptotárcákhoz**. A kártevő emellett célba veszi a **macOS Keychain tartalmát**, **Apple Notes** feljegyzéseket és **Telegram fiókhoz tartozó bejelentkezési adatokat** is. Az összegyűjtött adatokat curl -X POST kérésekkel **továbbítja a vezérlőszerverek irányába**. A kártevő ARM64 és x86_64 architektúrájú minták formájában is előfordulhat.

Javasolt intézkedések

Javasolt minden olyan macOS végpont **soron kívüli ellenőrzése**, amelyen a közelmúltban **nem hivatalos vagy nem megbízható forrásból származó alkalmazás telepítése** történt. Indokolt a LaunchAgent és LaunchDaemon **bejegyzések vizsgálata**, a felhasználói **könyvtárak átvizsgálása**, valamint a böngészőkben, helyi tárolókban és kriptotárcákban kezelt **hitelesítő adatok felülvizsgálata**.

Javasolt továbbá a **hálózati naplók ellenőrzése az azonosított domainek és IP-címek irányába mutató kommunikációra**, különösen a HTTPS forgalomba ágyazott adatkiáramlási mintákra. Érintettség gyanúja esetén indokolt az érintett végpont hálózatról történő leválasztása, a mentett jelszavak és munkamenetek érvénytelenítése, valamint a kompromittálódott hitelesítő adatok haladéktalan cseréje.

IoC-k:

- odyssey1.to
- 83.222.190.214
- charge0x.at

- 86.54.25.204
- 192.253.248.181
- sdojifsfiudgigfiv.to
- rgueapp.com
- Campaign ID: newooble
- Build ID: 3d5920bc4d0c45eb
- Seed: 0x1401d
- Multiplier: 72651
- ~/Library/LaunchAgents/com.apple.odyssey.plist
- ~/Library/LaunchAgents/com.apple.sys-update.plist

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833