Atomic Stealer 攻擊解析

瞭解 Atomic Stealer 如何從社交工程展開，進行憑證竊取與後續入侵。

1

偵察（Reconnaissance）

威脅份子蒐集目標相關資訊，為攻擊進行準備。

範例：社交工程行動會辨識受害者並建立受害者資料輪廓。

2

武器化（Weaponization）

攻擊工具會依據蒐集到的情資進行建置與封裝。

範例：惡意程式碼會嵌入外觀正常的 App 中。

3

傳遞（Delivery）

惡意 App 透過誘騙管道進行傳遞。

範例：贊助廣告引導使用者下載偽裝 App。

4

利用（Exploitation）

偽裝提示視窗誘騙使用者洩露憑證。

範例：偽裝更新提示視窗會擷取登入資訊與敏感資料。

5

安裝（Installation）

持續性機制會在初次入侵後維持存取權限。

範例：隱藏後門可讓攻擊者持續存取裝置。

6

指揮與控制（Command and Control）

遭竊的憑證會用於存取其他系統與資料。

範例：攻擊者透過指揮與控制擴大存取權限並在網路內橫向移動。

7

達成目標（Actions on Objectives）

攻擊者利用既有存取權限執行大範圍入侵。

範例：帳號接管、橫向移動、資料竊取與勒索。

jamf

AMOS 的重要性

33%

資訊竊取器相關 **惡意軟體**

50%

木馬式 攻擊

50%

的**威脅** 可規避偵測

資料來源：Jamf Security 360：2026 年 Mac 裝置年度趨勢報告

立即取得白皮書