剖析網路攻擊

在當今全球互連的世界中，資安專業人員在對抗威脅者時，面臨著極其艱鉅的挑戰。後者（駭客）只需利用一個漏洞或竊取一組憑證，就能在組織網路中取得立足點；而作為前者（資安人員）的你，必須在「每一次」防禦中都做到萬無一失……否則就得冒著裝置不合規或憑證遭竊的風險，進而導致資料外洩。

誠如 Thomas Jefferson 所言：「知識就是力量。」在資安領域，這股力量若落在威脅者手中，能讓他們洞悉組織防禦的弱點；若由資安專業人員掌握，則能協助他們理解網路攻擊的本質。

為了達成這個目標，你需要審視「網路攻擊鏈」（Cyber Kill Chain）的每個階段，並仔細剖析攻擊的構成要素。藉由這種方式，你可以在強化防禦的同時，補強潛在的風險漏洞。

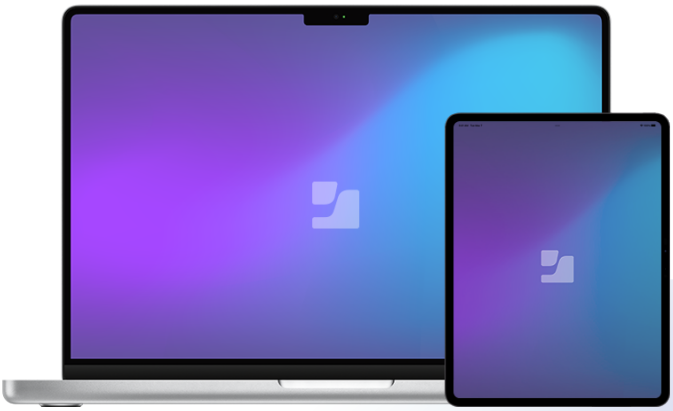
在本技術白皮書中，我們將：

- 逐步解析「網路攻擊鏈」
- 示範攻擊是如何運作的
- 對應各環節與必要的防護措施
- 強調補上資安缺口的重要性

再次拆解攻擊流程

攻擊手法各異，因為駭客會根據鎖定的目標及其擁有的漏洞，選擇不同的威脅手段。雖然攻擊具備相似的元素，但其獨特性加上影響端點安全的各種變數，使得推論網路攻擊成了結合藝術與科學的挑戰。

不過，即使攻擊手法再多變，有一點不變：攻擊都會遵循一定的流程，也就是 Lockheed Martin 所提出的**「網路攻擊鏈」（Cyber Kill Chain）**。攻擊鏈由七個階段組成，從最初的準備到執行惡意工具以達成目標。資安專業人員透過分析每個階段，可以識別出防護裝甲上的裂痕，避免威脅者鎖定並利用這些裂痕來繞過防禦。



「這就是我的 計謀，
而這些就是我的 計畫。」

– Tears for Fears

在學會如何解讀駭客的攻擊藍圖之前，
先來看看 攻擊鏈的七個階段：

1.

偵察（Reconnaissance）：
在線上或線下蒐集並鎖定目標資訊。

2.

武器化（Weaponization）：
利用蒐集到的情資，開發或取得後續攻擊要用的工具。

3.

傳遞（Delivery）：
將惡意工具投遞到目標，以取得存取權限。

4.

利用（Exploitation）：
一旦取得初步存 取，就會利用漏洞與其他安全缺口，進一步擴大入侵範圍。

5.

安裝（Installation）：
在目標系統部署惡意程式，為攻擊成功打下基礎。

6.

指揮與控制（Command and Control）：
與已被入侵的裝置建立溝通管道，為最後的攻擊階段做準備。

7.

達成目標（Actions on Objectives）：
完成所有前置準備後， 駭客會啟動工具來達成目的（竊取個資、外洩資料、執行勒索軟體等）。

好戲開場了！

讓我們深入了解網路攻擊鏈的每個細節。在本節中，我們將以針對 macOS 的「惡意軟體即服務」（MaaS）——**Atomic Stealer** (AMOS) 為例，剖析攻擊的構成以及它如何在現實場景中執行。

1.

偵察（Reconnaissance）

在情資蒐集階段，威脅者專注於研究目標，以獲取受害者的基礎設施、網路拓撲、以及上下游服務供應商的詳細資訊。任何細節都能協助他們建立目標組織的側寫。值得注意的是，此階段可能包含「主動偵察」與「被動偵察」。

主動偵察

這可能會驚動組織，因為侵入式工具會留下數位指紋，例如過多的登入失敗嘗試或網路掃描。

被動偵察

這主要依賴開源情報（OSINT），在不驚動目標的情況下匿名蒐集資訊。範例包括：

- 利用社群媒體鎖定高價值產業（如加密貨幣）的受害者。
- 利用社群媒體找出目標組織中擔任關鍵職位的員工。
- 識別合作夥伴關係，以判斷目標企業營運所使用的服務。
- 透過社交工程誘騙員工洩露敏感或機密資訊，以提高攻擊的成功率。

2.

武器化（Weaponization）

完成偵察後，威脅者會整理蒐集到的情資，並開始自訂攻擊初期所需的工具。以我們的範例來說，威脅者執行了幾項任務來將 Atomic Stealer 武器化。他們開發了惡意軟體，並對 DMG 檔案進行了 Ad-hoc 簽署。甚至還為使用者提供了具體的安裝說明，引導他們繞過 Apple 的 Gatekeeper 安全警告。他們建立了一個仿冒 Arc 瀏覽器官網的惡意網站，引導訪客下載被植入木馬的軟體版本。

注意：在第 1 至 2 階段，資安解決方案通常無法有效阻斷攻擊鏈，因為在進入第 3 階段之前，一切都還只是預謀。換個角度想，這不像《關鍵報告》那樣，在第 1 和第 2 階段，攻擊尚未發生。此時存在的僅是威脅者腦中的想法、點子或假設。網路犯罪是從第三階段才正式開始，我們必須等到威脅者嘗試實施犯罪時才能將其制止。

3.

傳遞（Delivery）

在此階段，威脅者將其研究與戰術付諸行動。

步驟一：仿冒網站上線。

步驟二：透過贊助廣告發布，而非正版的 Arc 瀏覽器網站。

步驟三：使用者下載並執行軟體，導致端點感染 Atomic Stealer 惡意軟體。

由於贊助廣告的觸及率廣且位於搜尋結果頂端，鎖定個人裝置進行攻擊，可能在短時間內導致大量端點受感染。雖然這種特定的攻擊不會在直接訪問網站時啟動（這可能是為了規避偵測）。但根據 Jamf Threat Labs 的觀察，利用 Atomic Stealer 變種的攻擊擴散極快，威脅者會透過電子郵件、簡訊（SMS）及社群媒體發起網路釣魚，以接觸更多受害者。

Jamf Pro 與 **Jamf Protect** 協同運作，可確保使用者免受威脅。前者利用內容過濾技術來封鎖釣魚網址，即使使用者點擊了連結也會被阻斷。端點安全功能則主動監控裝置健康狀況，並在合規狀態改變時提醒管理員；同時透過管理配置檔案強制執行資料安全，將商務資料存放在獨立且加密的磁碟區，與個人資料分開，防止混用。若商務資料受到影響，管理員可以自動執行裝置清理流程，包括從受影響的裝置中抹除敏感資料，以防止洩漏。

4.

利用（Exploitation）

雖然承載資料的遞送方式可能不同，但根據 Jamf Threat Labs 的深入研究：**「其目標與邏輯最終是一致的。」**換言之，受影響使用者的憑證仍會遭竊，且其敏感資料會被外洩。

這正是 Atomic Stealer 的目的——在誘導使用者輸入憑證（其實是利用 macOS 原生的「osascript」指令發起的 AppleScript 請求）後，竊取使用者資料。

值得注意的是，雖然惡意軟體在後台執行的操作已被 **Jamf Threat Labs** 詳細記錄（詳見「達成目標」章節），但這些基於惡意程式碼的變種，甚至隨時間演進的開發，讓威脅者有機會在使用者毫無察覺的情況下執行各類行動。例如，透過繞過 **Apple 的 TCC（透明度、同意與控制）架構來進行監控。**即使威脅者在釣魚攻擊中成功竊取了憑證，Jamf Trusted Access 也能透過即時收集豐富的遙測數據，通知管理員裝置健康狀態的變更，進而阻斷攻擊鏈的後續發展。此外，它還會觸發自動修補流程，例如部署更新以修補漏洞，防止「利用」階段繼續發展。

至於憑證本身，**Jamf Connect** 負責管理身份與存取權限，在事件處理期間可停用受影響的帳號。為了加快**應變與恢復，**與 Jamf Protect 的整合啟動了**零信任網路存取** (ZTNA)，在發現受影響憑證被用於存取其他應用程式/服務時，自動將風險降至最低。它會將威脅隔離在受影響的服務中，防止其在基礎設施內「橫向移動」，同時讓使用者能在未受影響的服務上維持生產力。最後，每次發起請求時都會進行持續的硬體與軟體檢查，提供額外保護。在驗證流程完成修補並確定受影響裝置合規之前，該裝置與憑證的存取權限將維持停用。

5.

安裝（Installation）

威脅者繼續執行惡意程式碼並部署惡意軟體，以建立「持續性」（Persistence）。這能維持他們對受駭系統的存取權限。同時，他們會利用自訂或原生工具（如命令列工具和惡意程式碼建立後門），在受駭裝置所連接的網路中進行「橫向移動」（Lateral Movement），進一步擴大勢力範圍。直接就 AMOS 而言，由於其目標是「一波帶走」使用者的所有資訊且不留下太多痕跡，因此 Atomic Stealer 在此階段採取的步驟很少。對於其他類型的攻擊，此階段通常是為了在隱蔽狀態下進行當前與未來的行動。

防範此階段的關鍵在於**利用可視性與安全性**，透過偵測、防範與修補已知威脅來確保合規性。主動監控裝置健康狀況能讓管理員在裝置安全態勢偏離基準時收到警報，以便進行分類並啟動事件應變流程。Jamf Protect 可阻止已知惡意程式碼執行，包括在威脅執行前將其隔離並移除。針對未知威脅，裝置日誌會轉發至第三方 SIEM 解決方案，協助**「威脅獵捕」團隊**偵測並移除隱藏在系統中伺機而動的威脅。

6.

指揮與控制（Command and Control）

Atomic Stealer 的首要目標是竊取憑證；其次是利用偷來的密碼竊取資料。但根據威脅者的進一步意圖，攻擊可能不會就此結束。由於「鑰匙圈」（Keychain）提供了憑證的集中安全儲存，搜刮這類豐富的資源通常能讓攻擊者取得各種功能、軟體與服務的權限。這對攻擊者來說非常有吸引力，因為可以：

- 獲取更多權限，進而存取具有高價值的資產。
- 透過「橫向移動」擴大攻擊範圍。
- 透過販售個資或勒索受害者來謀取不法獲利。

簡單來說：數據資料越多，獲利的機會就越大。

阻斷與受駭裝置的通訊十分重要。ZTNA（零信任網路存取）能監控端點並封鎖與惡意服務（如 C2 伺服器）的連線，有效切斷攻擊者與受駭裝置間的溝通。此外，ZTNA 會持續監控裝置與憑證的合規健康狀況，防止受駭的裝置與憑證存取受保護的資源；在限制不合規裝置存取的同時，也會與 Jamf Pro 協作，自動執行修復流程以處理受漏洞影響或遭入侵的裝置。

7.

達成目標（Actions on Objectives）

在最後這個階段，攻擊者會全面執行其計畫，不論是：

- **間諜活動（Espionage）**
- 資料外洩（Data exfiltration）
- 勒索（Extortion）
- 供應鏈攻擊（Supply chain attacks）
- 網路恐怖主義（Cyber terrorism）

不論是上述哪種行為或其組合，結果都是威脅者「辛勤工作」後的收割。這個部分很難量化，因為就像每個組織都有獨特需求一樣，每個攻擊者的行為也會完全或部分取決於其獨特的目標。以 Atomic Stealer 為例，前文提到的 osascript 指令被用來模擬系統合法警示的外觀與感覺，但實際上是利用使用者的憑證從 Apple 鑰匙圈中收集以下形式的機密數據：

- 使用者名稱與密碼
- 瀏覽器工作階段 Cookie
- 敏感使用者資料
- 付款卡片細節
- 加密貨幣錢包
- 系統中繼資料

補強你的防護漏洞

防護不周留下的資安缺口，以及僅關注桌上型作業系統而忽視行動裝置安全的作法，會讓威脅者有機可乘，透過入侵行動裝置在組織網路中取得立足點。

雖然行動裝置並非導致資料外洩的唯一風險，但隨著職場普及率提高，加上越來越多人使用個人裝置存取工作資料，演進中的威脅態勢持續將目標鎖定在行動裝置上。**Jamf Threat Labs 的研究**量化了這項風險：「40% 的行動使用者所使用的裝置存有已知漏洞。」在有漏洞的裝置上，未經檢查的風險因素會讓威脅者能夠：

- 在裝置上執行惡意程式碼
- 繞過內部資安防護措施
- 存取未經授權的商業資料
- 擅自取得隱私資料
- 在使用者毫不知情、也未同意的情況下進行監控
- 以受感染的裝置為跳板，進一步攻擊並入侵網路
- 竊取個人與商業資料，以及私人資訊

Apple 以設計結合外型與功能而聞名，兼顧美感與實用。這樣的理念也延伸到設計的一大核心：安全與隱私，且重要性正持續提升。macOS 和 iOS 系統本身內建了多層防護，從硬體到軟體層級，來保護裝置、使用者和資料免於各種威脅。

駭客不斷演變攻擊手法，出現新的威脅與惡意程式，例如愈來愈常見的「資訊竊取工具（Infostealers）」。僅靠靜態特徵碼偵測引擎的防護，已難以抵禦這些進階攻擊。根據《Dark Reading》報導，像 Atomic Stealer 這樣的威脅展現了「完全不同的開發鏈，而非單一核心版本的更新」。正因如此，**精密威脅正不斷規避內建防護**，使裝置、使用者與資料陷入風險。

「駭客只需成功一次就足夠，但是我們連半次失誤都無法承擔。」

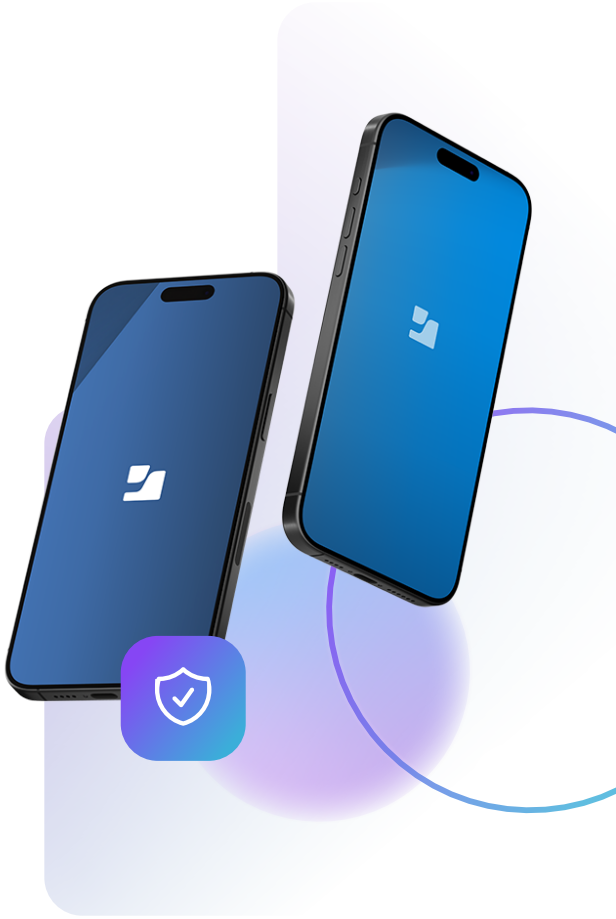
– Chris Triolo, HP

將管理、身份識別與安全性全面整合為單一解決方案。透過網路端與裝置端的協同運作，全面封鎖惡意流量。此外，防止商務資料外洩能確保其不被攻擊者竊取。ZTNA 驅動了此工作流程：透過自動偵測憑證遭竊的情況並將其停用，以阻斷對受保護商務服務的存取，將風險降至最低。由於遙測數據是以安全且全面的方式共享，自動化流程能持續執行風險緩解，直到漏洞修補完成。只有在端點被驗證為「合規」後，存取所請求資源的請求才會獲得核准。

依循成熟的**「縱深防禦」（Defense-in-depth）架構**來規劃資安策略，是組織降低風險、抵禦已知攻擊，並在事件發生時透過自動化修補流程快速回應以維持端點合規的最佳機會。

透過整合與多層次的解決方案，組織能以全面性的防護來應對進階威脅，確保在不同層級上偵測並降低風險。同時，這些多層防護延伸至整個企業，為所有請求存取公司資源與資料的裝置與作業系統類型提供基本的防禦基準。

根據 **Frost & Sullivan 在《Frost Radar: Endpoint Security, 2023》**對 Jamf 解決方案的報告中指出，Jamf 之所以被評為端點安全領導者，是因為我們的解決方案具備縱深防禦能力：



即時偵測惡意應用程式與指令碼，並提供建議的使用者應對措施。

擴展配置與稽核框架，協助客戶符合複雜的合規標準。

為公發和個人 BYOD 裝置，貫徹一致的政策和提供對等的支援。

一致性的弱點管理、威脅防護與政策控管。

強化端點遙測數據的豐富度，以便匯出至第三方日誌收集與分析工具。

Trusted Access 是獨家為 Apple 裝置打造的解決方案，它同時具備裝置管理、身分辨識與存取管理及端點防護的能力 。

跨 Mac 與行動平台（包括 macOS、 iOS/iPadOS 與 Android）的資安報表。其它的網路（Web）威脅防護，除了支援上述平台，也延伸至 Windows 與 Chromebook。

總結

只要威脅者持續鎖定裝置、使用者與資料，資安控制措施就有其必要性，以將風險降至最低並防止威脅演變成更嚴重的資料外洩事件。

一個長效的資安計畫應反覆包含以下目標：

- 具備風險意識並建立可接受的風險容忍度。
- 實施多層次的風險緩解與威脅預防控制措施。
- 整合裝置管理、身份與存取管理以及 端點安全解決方案，使其相互協作。
- 整合 IT 與資安團隊，打破部門孤島，促進溝通並加快事件響應。
- 利用自動化工作流程快速補救威脅，同時將人為錯誤降至最低。
- 將商務需求與標準框架對齊，以強化資安控制並維持合規。
- 建立緊急應變團隊以加速事件處理；若無法建立專職團隊，應與信任的專業資安團隊（如 Jamf Threat Labs）建立合作夥伴關係，協助獵捕未知威脅。