jamf

Security 360：

年度資安趨勢報告

Mac

目錄

簡介

Jamf 的 Security 360 是根據真實客戶事件、威脅研究和過去一年的產業活動分析所整理而成的報告。本報告聚焦 Mac 威脅情勢，旨在突顯出組織面臨的風險。

我們檢視了攻擊者用來造成損害的各種具影響力的攻擊媒介。隨著 Mac 裝置普及，也使其成為攻擊者的熱門目標，攻擊者不斷制定新手段來滲透裝置並竊取資料。

除了分析攻擊者鎖定 Mac 的新穎方式外，這份報告還收錄了 Jamf 資安長的觀點，為負責保護 Mac 機群的資安主管和 IT 從業人員提供深入洞察。

研究方法

為了解並量化這份報告中所述資安趨勢的實際影響，我們匿名探究了超過 150,000 部 Mac 裝置樣本。我們的分析於 2025 年底進行，涵蓋過去 12 個月期間。我們的惡意軟體調查中包含的資料僅取樣位於美國的裝置，但我們的漏洞調查涵蓋全球資料。

為了在收集和處理資料的過程中保障隱私與維持最高標準，我們研究中所分析的中繼資料來自匿名彙總的日誌紀錄，不包含任何個人或組織識別資訊。

總結

44%

的**裝置**帶有**惡意網路流量**

攻擊者隨時都在試圖入侵您的裝置。企業必須時刻保持警覺心，並配備合適的工具，方能偵測並阻斷惡意流量。

41%

的**裝置**具有**嚴重過時的**作業系統

強制執行最低軟體版本可確保您的裝置具備最新的安全修補程式，進而減少已知易遭利用漏洞的數量。

50%

影響 Mac 的 **惡意軟體**為
特洛伊木馬程式

特洛伊木馬程式在今年高居榜首，自 2024 年以來增加了超過 33%。特洛伊木馬程式是進入您系統的後門，會造成持久的損害，並使系統容易受到其他攻擊。

73%

的**裝置**安裝了
有漏洞的應用程式

您的作業系統並非唯一會帶來風險的軟體。應用程式可能包含有漏洞的程式庫、遭受供應鏈入侵或不當處理資料。全面掌握組織內的軟體資產，是風險管理的基石。

26%

的**組織**至少有**一部裝置**
遭到挖礦劫持

挖礦劫持攻擊會利用您裝置的處理能力來挖掘加密貨幣。當攻擊者從中獲利時，您的裝置效能與效率將隨之下降。

企業環境下的關鍵威脅趨勢

1. Mac 已不再是少數攻擊目標。

各種規模和產業的組織都在使用 Mac，且使用率更勝以往。從 2024 年到 2025 年，Mac 裝置**的市佔率成長了 16.4%**，達到近 10%，成長幅度超越任何其他廠商。

2025 年 Mac 出貨量超過 270 萬部，由此可明顯看出 Mac 已無處不在。攻擊者一直密切關注此趨勢，使得 Mac 成為遭利用的熱門目標。儘管具備強大的安全功能，但「Mac 不會感染惡意軟體」的時代早已過去。

隨著 Mac 電腦在企業中的佔有率不斷增加，攻擊者也加強並進化其手法，製造出專門針對 Mac 的威脅 — 進而竊取您的資料。

2. 資訊竊取程式正不斷演進，竊取的資料比以往更多。

資訊竊取程式是最常被散布的惡意軟體類型之一。惡意軟體製作者致力於打造有效且隱蔽的方式，以大規模取得您的資料。這些程式通常行動迅速，在使用者察覺任何異常之前，收集憑證、工作階段權杖、檔案，以及任何可取得的資料。

資訊竊取程式通常是更大規模攻擊的第一階段。這些程式可以挾持資料以勒索贖金，或利用這些資料滲透其他帳戶和系統。這些特點使資訊竊取程式在攻擊者眼中炙手可熱，因此許多開發者將其作為服務來提供。現代資訊竊取程式會建立後門和常駐機制，不僅能在重新開機和登出後持續存活，更能讓攻擊者從 C2 伺服器遠端下達指令。

3. APT 組織持續關注 macOS。

類似 DPRK 相關威脅的進階威脅持續在諸如 **Contagious Interview**、**FlexibleFerret** 及 **Odyssey 資訊竊取程式演進版**等惡意活動與惡意軟體中鎖定 macOS。

攻擊者持續建置後門程式和其他常駐機制。Jamf Threat Labs 在 **ChillyHell** 等惡意軟體中觀察到了此現象。

請在本報告末尾閱讀有關 Jamf Threat Labs 研究的更多資訊。

Mac 惡意軟體與威脅

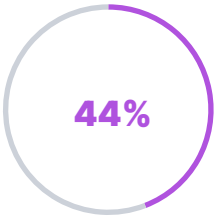
Mac 與 Windows 電腦並不相同，因此其惡意軟體也有所差異。針對 Mac 開發惡意軟體的攻擊者必須考量這些差異，才能了解要利用哪些漏洞。為了讓攻擊奏效，惡意行為者勢必得繞過下列安全功能：

1. **Gatekeeper**，此功能會透過查看應用程式的**公證與開發者資訊/簽章，來檢查應用程式是否合法且安全**

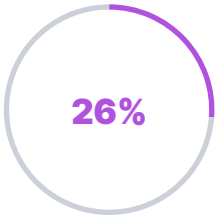
2. **系統完整性保護（SIP），**此功能限制了寫入關鍵系統檔案的能力

3. **透明度、同意和控制（TCC），**此功能要求必須獲得使用者的明確授權，才能存取相機、麥克風、檔案及其他內容

儘管面臨這些困難，**攻擊者仍屢屢得手。**



的**裝置**帶有
惡意網路流量



的**組織**遭受
挖礦劫持攻擊

這正是**了解並揭露最新威脅**至關重要的原因所在。
有許多最新資訊需要掌握。

超過 26,000

Jamf Threat Labs 在 2025 年新增至其資料庫的**惡意軟體樣本**數量

超過 230 項

Jamf Threat Labs 在 2025 年新增的
YARA 規則數量

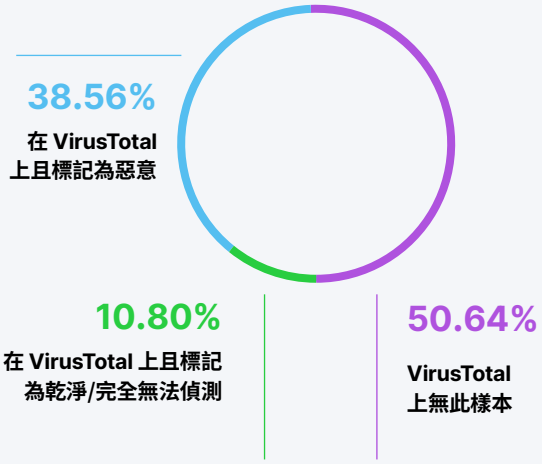
一旦了解您所面臨的威脅，您就需要知道如何偵測這些威脅。
YARA 規則可協助解決此問題 — 研究人員利用這些規則來識別並分類惡意軟體樣本。

但是，那些未知的威脅該怎麼辦呢？攻擊者同樣也很努力，必然會製造出網路安全社群尚未發現的新型攻擊。

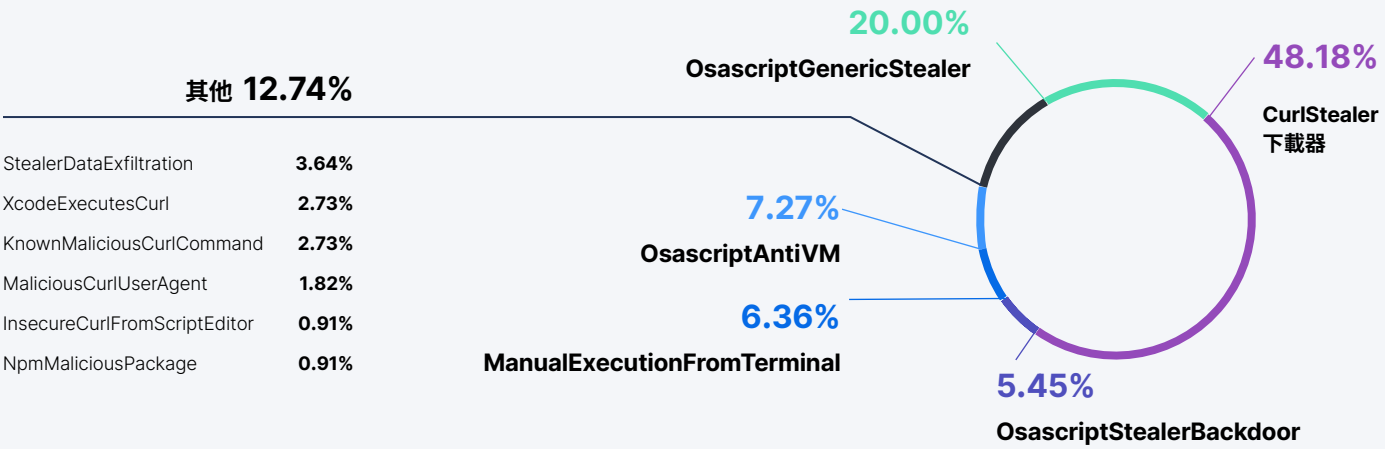
Jamf Threat Labs 也在尋找這些威脅，透過靜態與行為式規則來捕捉野生樣本。在使用 VirusTotal 檢查這些樣本時，發現約有 **50%** 的樣本尚未有其他研究人員上傳。

不幸的是，如果惡意軟體變得太容易識別，製作者就會進行大幅度修改，使其再次變得隱蔽。研究人員必須仰賴先進的偵測技術，藉由檢查**行為**而非靜態檔案特徵來進行偵測。標記為高嚴重性的行為警示會引起 Jamf 進階威脅控制的注意，隨後遭到封鎖。以下是 2025 年最常見的幾種：

JAMF THREAT LABS 發現的樣本



進階行為偵測



以下是這些偵測如何運作的範例：

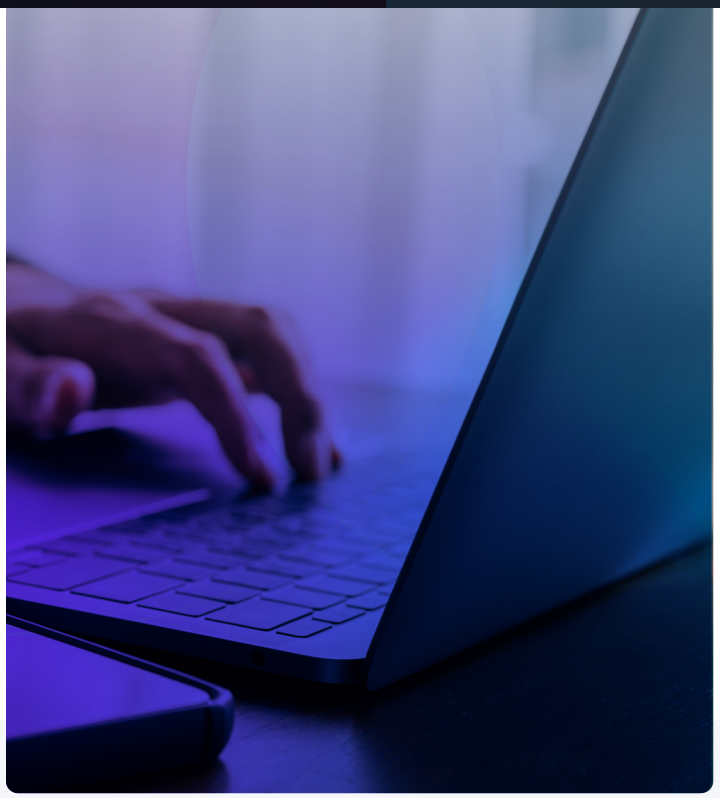
CurlStealerDownloader
使用 curl 下載並執行潛在資訊竊取程式惡意負載的可疑行為

OsascriptGenericStealer
透過 AppleScript 執行偵測到一般 macOS 資訊竊取程式活動

XcodeExecutesCurl
在 Xcode 建置過程中執行了可疑的 curl 命令

NpmMaliciousPackage
執行可能惡意的 NPM 套件，表示安裝或執行階段有可疑的指令碼活動

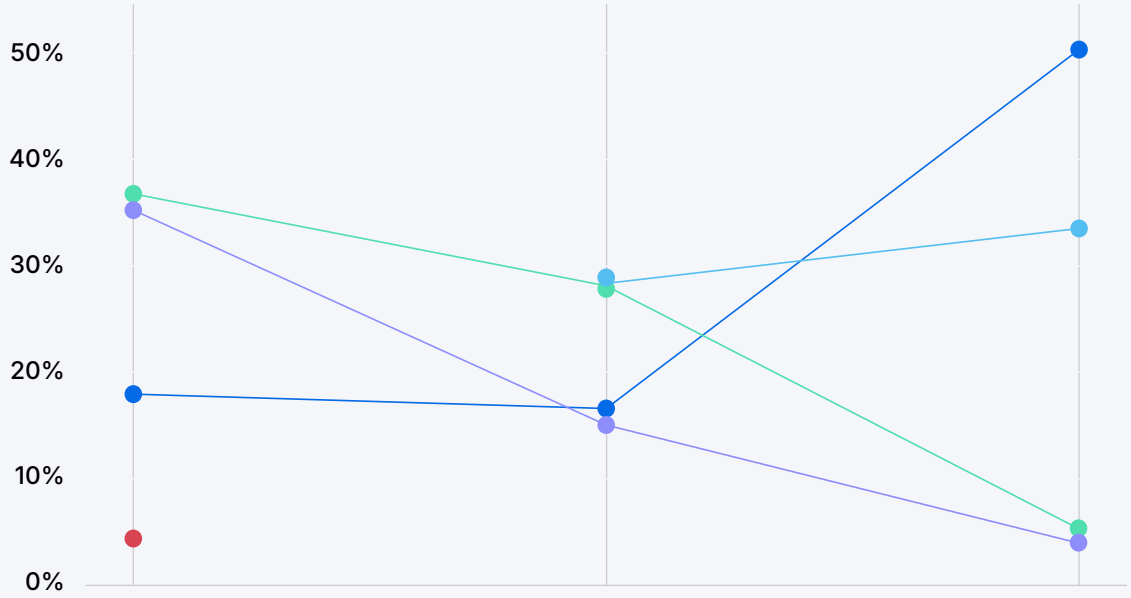
關鍵在於，鎖定 Mac 的威脅既普遍且多樣化。攻擊者正積極開發惡意軟體以謀取私利，並將其出售給出價最高者 — 市場需求高漲的情形更是前所未見。若要開始建立防護，您必須先了解自己正在對抗哪些惡意軟體。



最常見的 Mac 惡意軟體

攻擊策略在 2025 年發生了轉變。在 2024 年，資訊竊取程式與廣告軟體主導了威脅態勢，各佔約 **28%** 的攻擊比例。在 2025 年，特洛伊木馬程式躍居首位，約佔所有攻擊的一半，而資訊竊取程式則緊追在後，約佔三分之一。值得注意的是，資訊竊取程式已演進為利用特洛伊木馬後門，這種情況助長了此增長趨勢。將今年的資料與我們往年的報告進行比較，可以看出威脅的常見程度變化情形：

主要惡意軟體趨勢



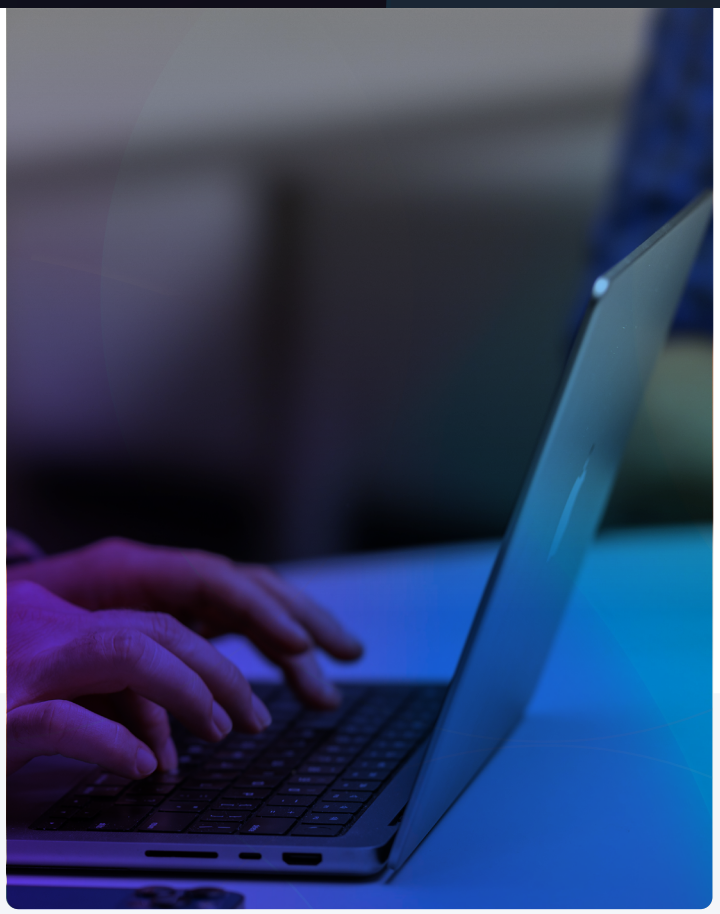
Malware Type	2023	2024	2025
Trojan	17.96%	16.61%	50.32%
Infostealer	-	28.36%	33.52%
Adware	36.77%	28.13%	5.06%
PUA	35.24%	15.06%	4.84%
Exploit	4.40%	-	-

前四大惡意軟體類型佔整體攻擊的**超過 90%**。這些分別是：

	特徵：	意圖：	散佈情形：
特洛伊木馬程式 50.40%	偽裝成合法的應用程式	各式各樣，常用作其他攻擊的後門	社交工程、檔案存放庫等
資訊竊取程式 33.52%	感染後立即竊取系統資料	取得登入資訊與個人識別資訊等敏感資料	有時以服務形式提供，並透過社交工程、惡意網站和軟體下載方式進行散佈
廣告軟體 5.06%	顯示廣告，可能會追蹤使用者行為以進行目標廣告投放或間諜軟體活動	產生廣告收益或收集資訊	綁定其他軟體，或存在惡意網站/附件中
可能不必要的應用程式 (PUA) 4.84%	可能採取多種形式；可能會收集資料、拖慢裝置速度或造成干擾	不一定明確帶有惡意，但可能會利用使用者資料獲利，或透過其他手段產生收益	綁定其他軟體，或透過誤導手法引誘下載

其他 6.26%

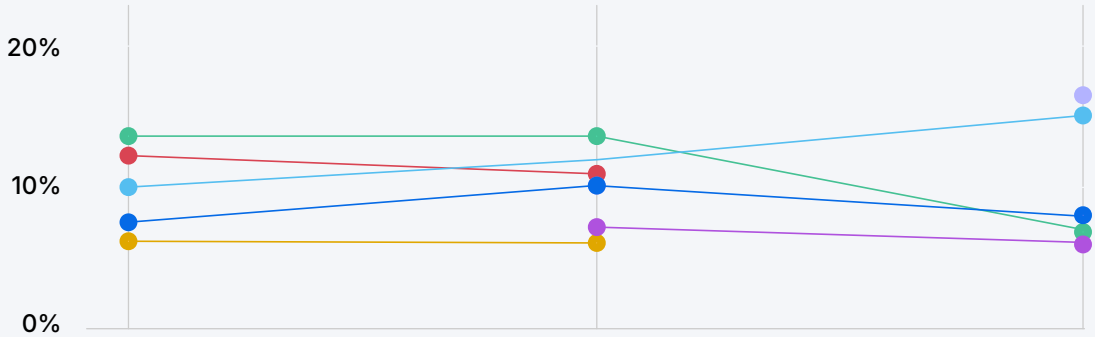
2.0% 漏洞攻擊，1.4% 駭客工具，0.9% 挖礦程式，0.4% 下載器， 0.4% 鍵盤側錄程式，0.3% 勒索軟體，0.2% 投放器



最常見的 Mac 惡意軟體系列

有各種不同的惡意軟體系列影響著 Mac，沒有哪一種特別突出。在 2025 年，PuAgent 最為常見，佔了 **16.41%**。在 2023 年和 2024 年，Genio 廣告軟體最為常見，佔了 **13.63%**，直到 2025 年跌至第四位，佔了 **7.19%**。

主要惡意軟體趨勢



Malware Type	2023	2024	2025
PuAgent	-	-	16.41%
Generic	10.02%	-	15.09%
Genio	13.63%	13.63%	7.19%
Multiverze	6.84%	9.44%	7.47%
Mackeeper	-	7.19%	7.13%
Imobie	12.25%	10.96%	-
TNT	6.19%	6.07%	-

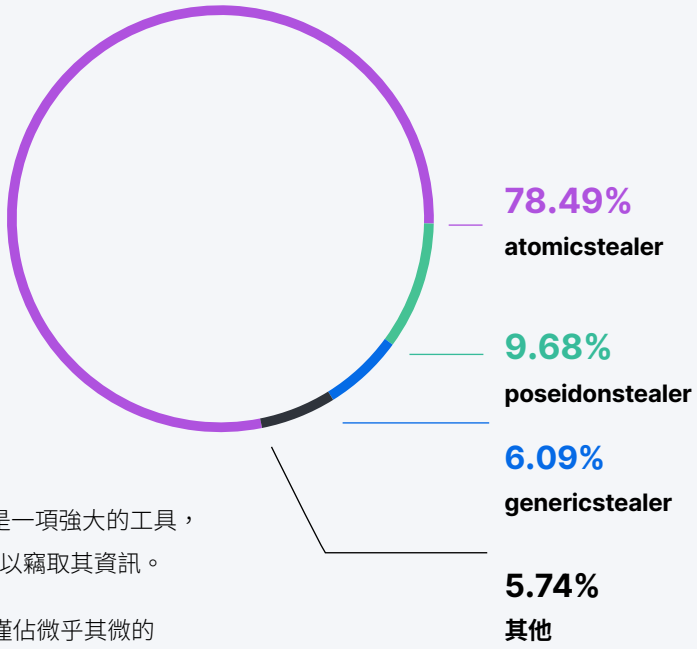
	特徵：	散佈情形：
PuAgent 廣告軟體 **16.4%**	透過變更搜尋引擎、首頁、設定、擴充功能及其他功能來修改瀏覽器。部署彈出式廣告並追蹤使用者行為。	電子郵件附件、惡意下載/連結、免費軟體
一般 各種 **15.1%**	檔案表現出暗示為惡意軟體的可疑行為，但沒有特定已知惡意軟體系列的特徵。	各種
Multiverze 特洛伊木馬程式 **7.5%**	收集使用者資料，包含密碼、信用卡號碼、加密貨幣錢包及其他資訊等隱私資訊。可能會記錄您輸入以及在螢幕上看到的所有內容。使用者可能無法察覺。	網路釣魚電子郵件、惡意網站、惡意廣告、免費軟體、社群媒體
Genio 廣告軟體 **7.2%**	劫持網頁瀏覽器以收集使用者資訊；偽裝成搜尋引擎以顯示贊助結果；難以解除安裝。	綁定合法軟體、惡意下載
Mackeeper PUA **7.1%**	看似合法應用程式，但可能無法達到所稱的效能。傳送彈出式廣告，可能對裝置運作狀況做出不實聲明，並降低裝置效能。	惡意廣告、惡意下載
Imobie **6.3%**		
Revproxy **4.7%**		
atomic_stealer **4.1%**		
Ccleanmac **3.4%**		
Macinformer **3.1%**		
其他 **25.1%**		

資訊竊取程式

如果您想竊取某些東西（請不要這樣做），進出的速度越快，被逮到的可能性就越低。資訊竊取程式通常會在感染您的裝置後，迅速採取行動來竊取您的資料。有時這些程式會在進行破壞後自我刪除，而現代的資訊竊取程式則可能會建立常駐機制。

> 資訊竊取程式在 macOS 生態系統內惡意軟體崛起的過程中扮演了重要角色。雖然過去 AppleScript 對進階使用者很有用，但也已在惡意軟體中遭到廣泛濫用。
>
> Jaron Bradley，Jamf

最常見的資訊竊取程式



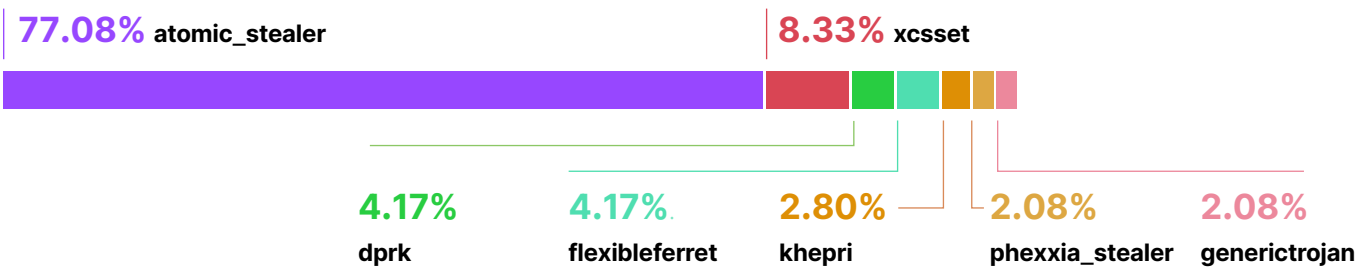
開發人員與進階使用者會使用 AppleScript 來自動化各種事件。這是一項強大的工具，具有無限的可能性 — 無論是好是壞。攻擊者會利用它來欺騙使用者以竊取其資訊。

資訊竊取程式在 2023 年之後變得更加普遍，但當時它們在攻擊中僅佔微乎其微的 **0.25%**。 2024 年這個比例卻急遽增加至 **28.36%**，最終在 **2025 年達到 33.52%**。儘管資訊竊取程式相當普遍，但有更多的攻擊是使用其他類型的惡意軟體，例如特洛伊木馬程式。說到這個...

特洛伊木馬程式

特洛伊木馬程式在 2025 年的猖獗程度飆升，最終佔了**所有惡意軟體攻擊的 50.3%** 而躍居榜首。最常見的特洛伊木馬程式 **atomic_stealer** 在所有特洛伊木馬攻擊中佔了 **77.08%**。您可能已經注意到，它與 2025 年主要的資訊竊取程式極為相似 — 這絕非巧合。許多竊取程式會利用特洛伊木馬程式建立後門，以便再次潛入。

活躍的特洛伊木馬程式



了解敵人，您就成功了一半。

我們討論的許多惡意軟體都是眾所皆知的。您的威脅偵測軟體很可能會將它們識別出來。如前面所述，並非所有惡意軟體都能透過其程式碼識別出來。可識別可疑行為的進階偵測機制，對於發現尚未經過網路安全社群分析的威脅至關重要。實作進階工具將能長久保護您的組織免受零時差攻擊。

設定也同樣重要。惡意軟體時常會利用使用者的行為，例如進行高風險下載或落入社交工程攻擊的陷阱。在這方面，資安政策與使用者教育訓練會有所幫助。

偵測機制至關重要；而預防則始於軟體本身。網路攻擊依賴軟體漏洞 — 應用程式與作業系統設計中的缺陷都會讓攻擊有機可乘。強制執行裝置與應用程式更新，是修補這些漏洞並防堵攻擊者的最佳方法。我們會在下一節繼續深入探討。

我們資安長的觀點

隨著 Apple 裝置在企業中持續普及，所選的資安解決方案應專為 Apple 生態系統所打造，而非從 Windows 為主的做法改造。組織應優先考量專為 macOS 從頭開始設計架構的資安產品，確保威脅偵測、強制合規與應變功能都可與 Apple 平台的運作方式完全一致，而非視為事後補救的措施。

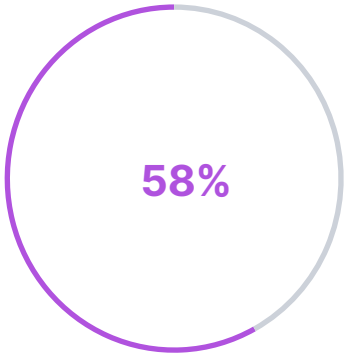
應用程式與作業系統漏洞

作業系統是裝置的基礎。它驅動著裝置上的工具、服務、應用程式與安全防護。攻擊者會不斷尋找防線上的破綻，以滲透其防禦系統。

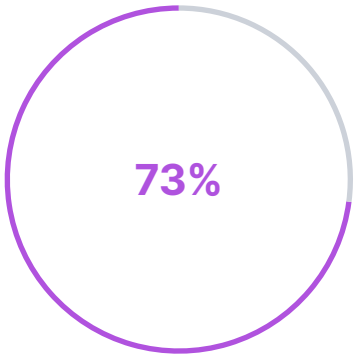
漏洞會不斷累積。 即使是較不嚴重的漏洞也可能成為攻擊中關鍵的一步，但有時修補這些漏洞會被視為非優先處理事項。

說到漏洞修補 — 這可是件大事。 遺憾的是，即使是最安全的作業系統，也難免存在漏洞。這是無法避免的，但並非無法補救。Apple 不斷推出軟體更新來修復漏洞。為了持續受到保護，您的組織必須強制執行這些更新。但情況不一定會如此順利。

應用程式也同樣重要。每個應用程式都有其漏洞、資料處理政策、開發程式庫等問題。



的**組織**至少有**一部裝置**的
作業系統嚴重過時



的**裝置**至少包含一個
有漏洞的應用程式

什麼是 CVE?

常見漏洞與暴露 (CVE) 計畫是網路安全社群所發現漏洞的資料庫。每個 CVE 列表都會識別受影響的軟體或程式庫、列出嚴重程度分數，並提供可能的漏洞利用方法

過時的軟體極為常見。使用者不一定都會急著更新，特別是他們認為更新會中斷其工作流程的時候。但強制執行更新期限與最低作業系統版本，才能夠長久保護您的裝置機群和資料 — 例如防止利用這些漏洞的入侵行為。

2025 年值得注意的 macOS 漏洞

CVE-2025-46287 | 嚴重程度：9.8（嚴重）	CVE-2025-43539 | 嚴重程度：8.8（高）	CVE-2025-46285 | 嚴重程度：7.8（高）
描述：		
攻擊者或許能偽造其 FaceTime 來電者身份。	處理檔案可能會導致記憶體損毀。	應用程式可能會取得根使用者權限。
受影響的元件		
通話架構	AppleJPEG	核心
衝擊：		
透過顯示誤導性資訊，攻擊者就能欺騙使用者執行錯誤的操作。	攻擊者可修改資料以執行未經授權的程式碼。	攻擊者可執行任意程式碼。
已修補的作業系統：		
macOS Tahoe 26.2、Sequoia 15.73 及 Sonoma 14.8.3	macOS Tahoe 26.2、Sequoia 15.73 及 Sonoma 14.8.3	macOS Tahoe 26.2、Sequoia 15.73 及 Sonoma 14.8.3

Jamf 發現的漏洞

CVE-2025-43296 | 2025 年 10 月
System Settings Gatekeeper 繞過漏洞，已於 macOS Tahoe 26 中完成修補。

CVE-2025-43348 | 2025 年 11 月
Finder Gatekeeper 繞過漏洞，已於 macOS Tahoe 26.1 中完成修補。

我們確認在 2025 年遭到利用的其他漏洞如下表所示。

CVE ID	元件	衝擊
CVE-2025-24113 CVSS 分數：4.3 | 嚴重程度：中	Safari	造訪惡意網站可能會導致使用者介面誘騙攻擊。
CVE-2025-46289 CVSS 分數：5.5 | 嚴重程度：中	AppSandbox	應用程式可能可以存取受保護的使用者資料。
CVE-2025-43482 CVSS 分數：5.5 | 嚴重程度：中	音訊	應用程式可能可以造成拒絕服務。
CVE-2025-43517 CVSS 分數：3.3 | 嚴重程度：低	通話記錄	由於日誌記錄問題，應用程式可能可以存取受保護的使用者資料。
CVE-2025-43542 CVSS 分數：7.5 | 嚴重程度：高	FaceTime	透過 FaceTime 從遠端控制裝置時，可能會意外揭露密碼欄位。
CVE-2025-43532 CVSS 分數：2.8 | 嚴重程度：低	Foundation	處理惡意資料可能應用程式因記憶體損毀而意外終止。
CVE-2025-43512 CVSS 分數：7.8 | 嚴重程度：高	核心	應用程式可能可以提升權限。

漏洞管理是一場持續的抗戰 — 但絕非必敗之戰。

為了隨時掌握軟體漏洞，您需要擬定完善的策略。最基本的要求是，您必須持續識別、緩解並監控影響系統和裝置的漏洞。

取決於您的 IT 與資安團隊規模和能力，您不一定能夠自行狩獵威脅。所幸有資安社群，它會是您的堅強後盾。威脅研究人員與軟體廠商會持續追蹤悄悄出現的最新入侵跡象，並將潛在漏洞新增至資料庫中，以協助組織了解漏洞存在之處。您的團隊可參考這些資料來掌握目前的資安態勢，並採取相應的應變措施。市面上的資安工具可協助簡化此流程。

貴組織所需的確切工具，將依據您的規模、技術能力、所屬產業等因素而有所不同。但一般而言，您會需採取以下措施：

- **設定裝置並強制執行政策**
- **管理使用者帳戶和身分**
- **讓裝置和軟體保持在最新狀態**
- **監控裝置運作狀態**
- **強制執行存取政策**

行動裝置管理、端點防護、身分管理和遙測工具都有助於完成這些任務，讓您在威脅出現時搶先一步應對。

我們資安長的觀點

穩健的資安策略建立在可視性、遙測與自動化等核心原則之上，而在漏洞管理中，這一點尤為關鍵。**資安團隊**應該：

了解其漏洞

深入洞悉整個組織的漏洞是關鍵的第一步。全面深入了解終端使用者裝置與基礎架構中存在哪些漏洞，可為資料驅動的安全態勢奠定基礎。接下來，團隊可以分析應用程式足跡、評估潛在風險並確定影響範圍，使資安團隊能夠根據證據而非假設來排定漏洞處理的優先順序。

實施基於風險的裝置存取方法

當不合規的裝置試圖存取企業資源時，應限制其存取，直到裝置恢復合規為止，且修復流程的設計應盡可能讓終端使用者感到順暢無阻。

制定完善的修補計畫

回到前述的 MDM 重點，擁有一套工具來確保軟體或作業系統的最新或支援的 N-X 版本合規，對於維持穩定安全的環境是十分重要的。若能在幾乎不影響終端使用者的情況下做到這點，也能更順利地進行合作並支援業務運作。

閱讀來自 Jamf Threat Labs 的 macOS 最新研究

OpenClaw：這個實用的 AI 工具可能會悄悄成為您最大的內部威脅

2026 年 2 月

OpenClaw 是一種開放原始碼架構，用於建構自主 AI 代理程式來執行 shell 命令、存取檔案以及與應用程式互動，由於缺乏內建的安全邊界，因而形成重大的企業安全風險。此架構的危險性在於不受限制的系統存取、潛在資料外洩風險，以及容易受到間接提示注入攻擊（將惡意指令嵌入合法業務內容中）的漏洞。近期資安通報展示了攻擊者如何利用各種漏洞來取得持續存取權，使 OpenClaw 部署成為高風險的內部威脅，必須具備全方位的偵測機制、預防與治理策略，才能在企業環境中安全地進行管理。

威脅行為者擴大濫用 Microsoft Visual Studio Code

2026 年 1 月

與 DPRK 有關的威脅行為者已進一步發展 Contagious Interview 活動，藉由濫用 Visual Studio Code 工作設定檔，在受害者開啟惡意 Git 儲存庫時植入 JavaScript 後門程式。此後門程式會建立常駐命令與控制（C2）通訊、收集系統資訊，並具備遠端程式碼執行能力。此技術利用開發人員的信任工作流程 — 當使用者將儲存庫標記為受信任時，惡意組態檔會自動執行隱藏命令，這顯示了威脅行為者如何持續調整其策略，以便整合到合法的開發工具中。

從 ClickFix 到程式碼簽章：MacSync Stealer 惡意軟體悄然轉變

2025 年 12 月

MacSync Stealer 已超越拖曳至終端機（drag-to-terminal）的技術，目前透過具備程式碼簽署與公證的 Swift 應用程式進行部署，可悄悄擷取並執行惡意負載，完全不需透過終端機互動。此變種透過假冒的安裝程式散佈，採用複雜的植入程式（dropper）來執行連線檢查、強制執行速率限制、驗證惡意負載，並在執行前移除隔離屬性。這種轉向簽章與公證交付的轉變反映出更廣泛的趨勢，即攻擊者將惡意程式碼偽裝成合法應用程式，以規避偵測並繞過 macOS 安全控制措施。

FlexibleFerret 惡意軟體持續發動攻擊

2025 年 11 月

FlexibleFerret 是與 DPRK 有關的惡意軟體系列，其透過複雜的假招募活動鎖定 macOS 使用者，誘騙受害者執行偽裝成招募評估的惡意終端機命令。這種多階段攻擊在假造的求職網站上使用 JavaScript 部署具有廣泛功能的後門程式（包括檔案外洩與命令執行），同時透過偽造的 Chrome 提示來收集憑證，並將資料傳送至攻擊者控制的 Dropbox 帳號。這種不斷演進的威脅藉由誘使使用者手動執行命令來繞過 Gatekeeper，因此使用者務必對不請自來的「面試」評估與終端機指令保持資安意識，這點成為防禦的關鍵。

DigitStealer：幾乎不留痕跡的 JXA 型資訊竊取程式

2025 年 11 月

DigitStealer 是一種複雜的 macOS 資訊竊取程式，在 VirusTotal 上完全未被偵測出來，同時採用了進階的反分析技術，包括限制在 Apple Silicon M2 或更新版本晶片上執行的硬體特徵偵測。該惡意軟體部署了四個常駐於記憶體的惡意負載，用於竊取瀏覽器資料、加密貨幣錢包和憑證，並透過合併三個獨立的元件將 Ledger Live 變成特洛伊木馬來規避偵測，再透過動態後門建立常駐機制。它利用合法的 Cloudflare 服務進行惡意負載代管和多階段混淆，展現了對 macOS 內部運作的深入了解，而由於其絕大多數是完全在記憶體中執行，因此行為偵測變得至關重要。

ChillyHell：深入剖析模組化 macOS 後門

2025 年 9 月

ChillyHell 是一個複雜的 macOS 後門程式，自 2021 年以來一直保持公證狀態且未被偵測到，最初與鎖定烏克蘭政府官員的攻擊有關。這種模組化 C++ 惡意軟體建立了多種常駐機制，透過 DNS 和 HTTP 進行通訊，並部署了包含反向 Shell、自我更新、惡意負載傳送和密碼暴力破解等功能。其進階規避技術證明，經過簽章和公證的應用程式不一定是安全的。

具備簽章並進行竊取：揭露 Odyssey 資訊竊取程式的新見解

2025 年 7 月

一個複雜的 macOS 資訊竊取程式成功取得了 Apple 的程式碼簽章與公證，使其能夠繞過內建的安全控制機制，同時部署常駐後門程式，並將合法的加密貨幣應用程式替換成遭植入特洛伊木馬的版本。該惡意軟體使用誘騙的 SwiftUI 介面來收集密碼，動態下載經混淆處理的惡意負載，並建立持續的命令與控制連線，以便從遠端執行程式碼。最令人擔憂的是：它會主動識別分析環境特徵，並將研究系統列入黑名單以規避偵測，展現出國家級的精密程度。

偽裝的 Python：拆解 macOS 上的 PyInstaller 惡意軟體

2025 年 5 月

攻擊者利用 PyInstaller 將惡意的 Python 程式碼偽裝成原生 macOS 執行檔 — 這是首次在 macOS 資訊竊取程式中觀察到此技術。該惡意軟體無需安裝 Python 即可執行，透過偽造的密碼提示竊取憑證、收集鑰匙圈（Keychain）資料與加密貨幣錢包，同時使用多重混淆層來規避偵測。這項技術代表了 macOS 惡意軟體散佈方式的重大演進，讓攻擊者能夠部署複雜的資訊竊取程式，同時可能繞過傳統的安全機制。