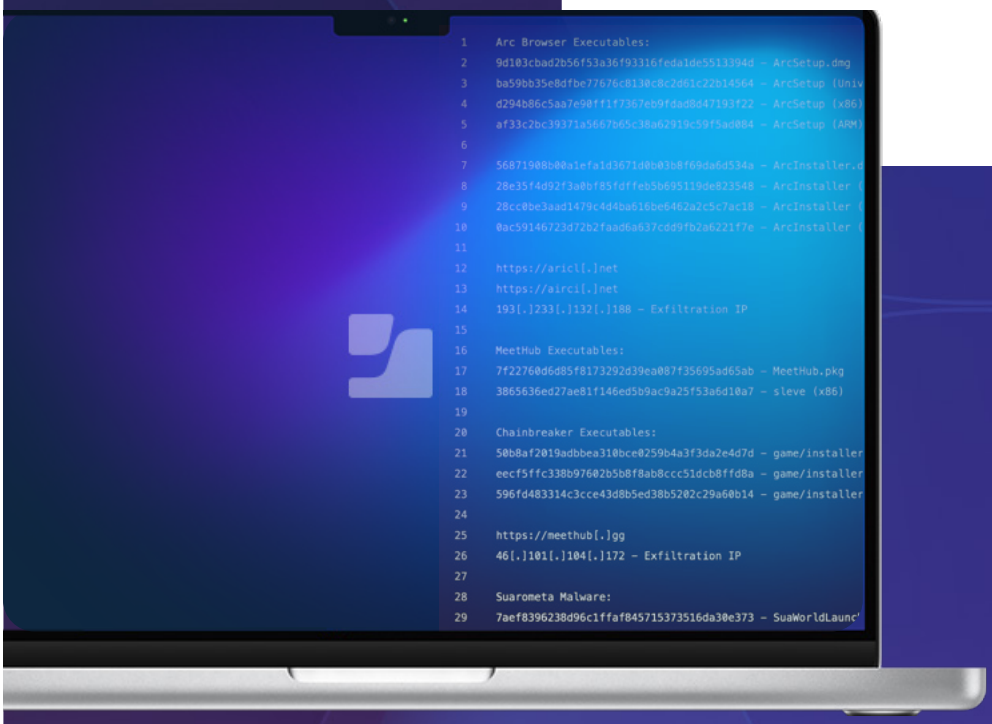
jamf

Security 360：

年度趨勢報告

Mac



前言

在 Jamf，我們熱愛 Mac。這是我們最早開發軟體的平台，至今仍是我們無比熱情投入的裝置。（我們是 **macOS 安全性合規性計畫的官方貢獻者。**）回顧歷史，我們見證了 Mac 在工作環 **境中逐漸扮演更重要的角色。**從創意人員與高階主管的裝置，漸漸演變為工程師等職位日常作業中不可或缺的工具。但隨著 Mac 在職場的普及，它也成為攻擊者更大的目標。

現今 Mac 面臨的威脅格局比以往更加多樣，攻擊方式也愈發巧妙。我們秉持「幫助組織成功運用 Apple」的使命，深入探討影響 Mac 裝置的威脅情勢，為我們的客戶與 Apple 社群提供協助。

— Jaron Bradley，
Jamf Threat Labs 總監

介紹

Jamf 的 Security 360 報告根據真實客戶事件、威脅研究與過去一年的產業趨勢分析所整理而成。本 報告將聚焦於 Mac 生態 ，揭示組織所面臨的安全風險。

我們評估了各種攻擊途徑（如惡意軟體、漏洞與社交工程），這些方式常被用來誘騙使用者、攻擊裝置、滲透企業網路。分析內容涵蓋裝置漏洞、網路威脅、惡意程式等主題。

除了趨勢分析外，報告也納入 Jamf 資安長的觀點，提供保護終端使用者、裝置、應用程式與網路層級的實務洞見。

研究方法

為了了解並量化這些安全趨勢的實際影響，我們分析了全球 90 個國家中、由 Jamf 保護的 140 萬台裝置資料樣本。分析工作於 2025 年第一季 進行，回顧過去 12 個月的趨勢。

為了保障隱私並維持最高的資安標準，我們在研究中所分析的中繼資料是來自經彙整的記錄檔，這些資料不包含任何可識別個人或組織的資訊。

研究目的

我們希望透過此分析，幫助組織與使用者了解現有的資安趨勢，並學習如何降低風險。同時介紹 Jamf Threat Labs 的重要研究成果，包括惡意程式與漏洞發現。

有許多行動可以提升 Mac 的安全性，例如，只從可信來源下載軟體。此外，組織也應採取以下安全最佳實務：

- 作業系統持續與即時更新
- 使用者教育與訓練
- 應用程式審查與控管
- 多重要素驗證（Multi-Factor Authentication）
- 零信任安全架構
- 公司 資料的可接受使用政策
- 在各種應用 情境下實施 Apple 最佳作業流程

儘管部分作法為基本配備，部分裝置安全需求則依組織而異。例如，受監管產業的組織可能需符合產業基準或法規（如 CIS 基準、HIPAA）。

本年度報告將分析重點分為三大類風險，這些風險為全球組織的首要關注項：

I. 應用程式風險與惡意程式

II. 漏洞管理

III. 社交工程

我們 也針對**行動裝置**推出了《Security 360》報告，您可在 **這裡**查閱：

報告中的多數分析來自 Jamf 威脅情報，由原始研究、真實數據、新聞分析與資料來源彙整而成。Jamf 威脅情報由 Jamf Threat Labs 與資料科學團隊主導，針對裝置、應用與網路流量持續監控風險、威脅與零時差漏洞。

企業環境中 Mac 的關鍵趨勢

惡意軟體會帶來風險 —— 即使 在 安全 平台中也是如此

Apple **以安全性為核心來建立平台**不僅是平台本身，Apple 也重視向使用者傳達安全性資訊的方式。例如，**Apple 的「平台安全性」網站** 上有一頁專門介紹如何在 macOS 中防範惡意軟體。Apple 不同的技術（如 App Store、XProtect 或 Gatekeeper）在應用程式生命週期的不同階段提供防護層級，以防止惡意應用程式。

在職場使用 Mac 裝置時，安全性必須在提供使用者必要應用與防止高風險應用之間取得平衡。Mac 應用程式類型多元，包括原生 Mac 應用程式、網頁應用程式以及混合型應用，這些都是開發者為了各種用途所打造的。 然而，如今**許多常見的商業用 Mac 應用程式**並非來自 Mac App Store，而是由開發者直接提供 安裝檔。此外，使用者還能夠從任何網站下載應用程式。

單一漏洞就可能讓攻擊者取得整個系統的存取權

事實上：我們每天使用的軟體（包括作業系統與應用程式）都可能存在漏洞。

美國國家標準與技術研究院（NIST）指出：「一般軟體每千行程式碼大約會有 25 個錯誤與漏洞。」常見漏洞與曝險（CVE），會在國家漏洞資料庫（NVD）中發布，讓大眾了解：

- 對 CVE 的認識
- 受影響的產品或廠商
- 威脅的描述

從漏洞被發現到修補之間的時間差，可能會造成損害。即使修補程式釋出，仍需安裝到受影響的裝置上。能夠顯示哪些漏洞存在及其嚴重程度的安全工具，有助於 IT 與資安團隊優先處理最急迫的修補，並提升其流程效率。

社交工程仍然會讓使用者遭受 入侵

社交工程（如釣魚攻擊）仍是威脅行為者最常使用的攻擊手法之一，在資安威脅環境中依然非常活躍。 2024 年 9 月，**Apple 發布了一篇 部落格文章**，向使用者提供指引，幫助他們「避免詐騙並了解收到可疑郵件、電話或其他訊息時該怎麼做」。攻擊者的手法越來越多樣，可能假扮為招募人員、家人、知名品牌等。無論平台或作業系統多安全，社交工程的設計就是從裝置中最不安全的部分入手，也就是使用者本身，以滲透企業資料。

第一部分：針對 Mac 的惡意軟體

本報告旨在說明 Mac 惡意軟體的類型、其對組織造成的影響以及發生頻率。隨著 Mac 在職場上的使用擴大，並有更多關鍵應用在該平台上執行，整個組織的使用者都將成為攻擊目標。

Apple 的惡意軟體防護架構包含 三 層：

1. **防止惡意軟體啟動 或執行**
2. **阻擋惡意軟體在 客戶 裝置上執行**
3. **修復已執行的惡意軟體**

Apple 的技術（App Store、Gatekeeper、XProtect 和簽署認證）為使用者提供原生的威脅緩解方式。例如，XProtect 是內建的防毒軟體。當 Apple 發現惡意軟體時，可以採取多種行動，例如撤銷開發者 ID。

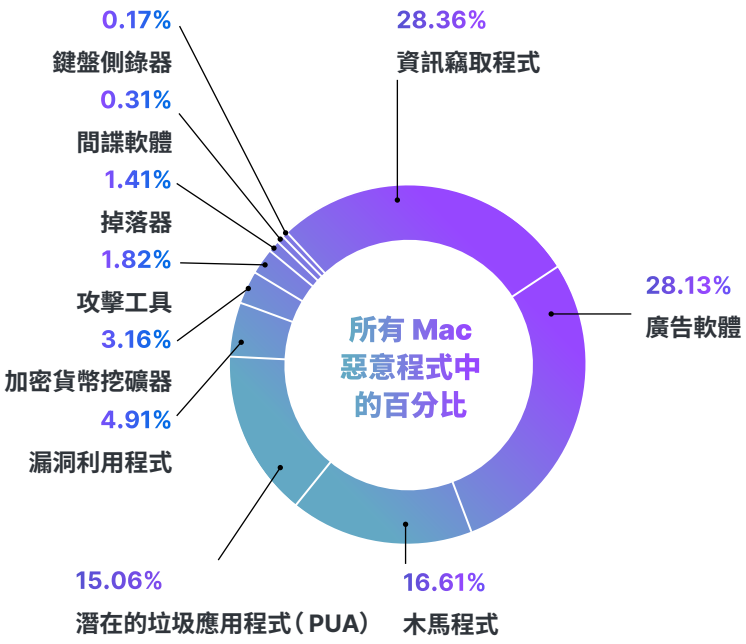
macOS 儘管內建強大的系統安全機制，仍無法完全免於惡意軟體的威脅。**今年三月**，Jamf Threat Labs 與資料科學團隊合作撰文，討論有關 Mac 惡意軟體的迷思、如何以舊有樣本辨識新型惡意軟體，並透過 Titan（一個由 Jamf Threat Labs 開發的 3D 可視化工具）展示 macOS 惡意軟體的攻擊途徑。Titan 有助於提供情境分析，並識別相關的惡意軟體樣本。這些被揭露的惡意軟體家族，顯示出 macOS 平台上「持續成長、日益複雜」的新型惡意軟體數量。這代表著什麼呢？Mac 惡意軟體是真實存在的，有其相關家族，且越來越常被威脅行為者使用。

今年， Jamf Threat Labs發現了一個與北韓（DPRK）有關的惡意程式，**植入 於一款以 Flutter 架構**開發的應用程式中。雖然使用 Flutter 開發跨平台應用程式並不罕見，但這次攻擊之所以值得關注，是因為這是首次發現此框架被用來針對 macOS 裝置。團隊深入解析了這個惡意軟體，包括其 Python 與 Golang 的變種，並指出該惡意軟體「可能正進行更大規模武器化的測試」。我們也注意到，Flutter 框架會在無意間將其使用者所撰寫的程式碼進行模糊化處理，導致其程式碼難以解析。

Mac 惡意軟體家族

以下是根據 我們 的研究，對 2024 年新發現 Mac 惡意軟體實例的完整解析：

這些資料告訴我們什麼？若與去年的惡意程式報告相比，我們可以發現一些一致性：廣告軟體（adware）、木馬程式（trojan）、潛在的垃圾應用程式（PUA），以及利用已知漏洞的應用程式等仍然是惡意程式分類中排名前列的類型。（去年，木馬程式的家族數量最多，占比 17%，今年略微下降至 16.6%。）今年的榜首則是資訊竊取器（infostealers）。實際上，資訊竊取器在整體惡意程式中占比增加了 28.08%。



這類惡意程式的存在與 Jamf Threat Labs 過去一年的研究結果一致，即 macOS 環境持續受到此類惡意程式的攻擊。這些攻擊策略有趣的地方在於，攻擊者不僅使用資訊竊取器來存取他們想要的資料，還會使用本報告前面提到的另一種策略：社交工程。也就是說威脅行為者正在結合多種攻擊手法來欺騙其受害者。對於處於高度曝光產業（如加密貨幣）中的員工或組織來說，無論是培訓還是安全工具層面，都必須保持高度警覺。這些攻擊並非隨機發生，而是經過精心設計的。

調查利用 PyInstaller 在 macOS 上部署資訊竊取器的情況。

2025 年 4 月，Jamf Threat Labs發現了將 Python 程式碼包裝成 Mach-O 可執行檔的未被偵測 macOS 資訊竊取器樣本。（Jamf Threat Labs 在 VirusTotal 上發現三個未被偵測的資訊竊取器樣本。）

PyInstaller 是一個合法的開源工具，讓開發者可以將 Python 腳本包裝成獨立的可執行檔。攻擊者現在也利用同樣的技術，來投放專為 macOS 設計的惡意程式。團隊檢視了幾個關鍵函數，確認該惡意程式的真實本質——一種資訊竊取器。幾個主要功能包括：

- 透過偽造的密碼提示視窗誘使終端使用者輸入憑證。
- 從攻擊者的伺服器執行任意 AppleScript 有害承載資料。
- 直接從 macOS 鑰匙圈（Keychain）中提取儲存的憑證與敏感資訊。
- 掃描檔案系統尋找加密貨幣錢包，並外洩私鑰以竊取加密資產。

隨著資訊竊取器在 macOS 威脅環境中越來越常見，威脅行為者會持續尋找新的散布方式。然而，組織可以採取具體行動，以防禦上述惡意程式。舉例來說：

- 限制應用程式執行權限，只允許 Apple 及已識別開發者簽署的應用程式。
- 為合法 IT 流程中使用的 osascript 視窗加上品牌識別，並訓練員工在輸入密碼前確認品牌標誌。

需注意的惡意程式：

Poolrat

Poolrat 是一個 macOS 後門程式，因參與 3CX 供應鏈攻擊而臭名昭著，能夠在執行檔操作時同時收集系統資料與執行指令。最近還發現了一個更輕量化的版本，稱為 Pondrat 。

Pondrat

Pondrat 是一個後門程式，與 AppleJeus 和 Poolrat 具有相似特徵，透過惡意 PyPi 套件散播。安裝後，Pondrat 會與指揮控制伺服器（C2）建立連線，以利上傳與下載檔案、暫停操作，以及執行任意指令。

NotLockBit

以 Golang 編寫的勒索軟體，偽裝成惡名昭彰的 LockBit 勒索軟體變種。自第一個樣本以來，該勒索軟體就植入一把公開金鑰，用來列舉並加密一組寫死的擴充功能。 最新的 NotLockBit 變種會將資料外洩至攻擊者控制的 S3 儲存空間，並使用 osascript 修改桌布（LockBit 2.0 特徵）。NotLockBit 仍在持續開發中。

ThiefBucket

ThiefBucket 是一個與北韓 Lazarus 集團有關的惡意程式家族，透過精密的社交工程活動攻擊受害者。它以第二階段承載資料的形式，透過偽裝成程式挑戰的方式傳送給目標。這個後門具備數種功能，尤其是自動資訊竊取功能。其他功能包括： - 常駐機制 - 終止程序 - 刪除檔案 - 檔案上/下載 - 自我刪除 - 執行 Shell 指令 - 利用 Spotlight 快速搜尋檔案 - 與 C2 通訊。

HZRat

HZRat 最初針對 Windows 平台，如今已進化為透過偽裝成合法軟體安裝程式來攻擊 macOS 裝置。一旦安裝，HZRat 就會連線至 C2 伺服器，讓攻擊者能執行指令、竊取檔案，以及擷取 WeChat 與 DingTalk 中的使用者名稱、電子郵件、電話號碼等個資。

BansheeStealer

Banshee Stealer 在 Telegram 上以「惡意程式即服務」模式銷售，並附有網頁介面供攻擊者操作。其專長於資訊竊取，可外洩帳號密碼、瀏覽器資料、Session cookie 和加密錢包等敏感資訊。與其他資訊竊取器類似，Banshee 濫用 AppleScript 對話框，誘導終端使用者輸入密碼。當使用者輸入密碼後，它會從 macOS 鑰匙圈中竊取更多敏感資料。Banshee 使用各種防偵測技術，包括反虛擬機、反除錯，以及偵測俄語系統。

InvisibleFerret

InvisibleFerret 是一種以 Python 編寫的木馬程式，藏匿於偽裝應用程式中。最該注意的是，它被 BeaverTail 資訊竊取器作為第二階段惡意程式安裝。該惡意腳本具跨平台能力，允許攻擊者執行偵察、資料外洩、複製剪貼簿內容與遠端指令。若需進一步遠端控制，它也能安裝 AnyDesk 軟體。

BeaverTail

BeaverTail 是一個偽裝成合法應用程式的資訊竊取器，透過社交工程發送給受害者。與其他資訊竊取器相似，它會蒐集鑰圈圈資料、瀏覽器 Cookie、加密錢包等資料並上傳至攻擊者控制的伺服器。它也能在受害者系統上執行額外的遠端惡意程式，如 InvisibleFerret 後門。有部分來源將其歸因於北韓。

PoseidonStealer

Poseidon Stealer 在 Telegram 上販售，為 Atomic Stealer 的競爭對手，也是一種「惡意程式即服務」。其專長於資訊竊取，可外洩帳號密碼、瀏覽器資料、Session cookie 和加密錢包等敏感資訊。和 Atomic 類似，Poseidon 利用 AppleScript 對話框誘騙終端使用者輸入憑證。當使用者輸入密碼後，它會從 macOS 鑰匙圈中竊取更多敏感資料。這款惡意程式以合法應用程式做為偽裝，並透過 Google Ads 惡意廣告進行推廣。

Kuiper

Kuiper 是用 Go 語言開發的勒索軟體即服務（RaaS），由一名名為 Robinhood 的使用者在地下論壇發布。它結合使用 RSA、ChaCha20（針對小於 600MB 的檔案）與 AES（針對大於 600MB 的檔案）加密檔案。雖然大多數功能針對 Windows 設計，但 macOS 版本會透過 /dev/urandom 產生亂數金鑰與初始向量，解碼勒索訊息、遞迴加密目標檔案（副檔名改為 .kuiper），然後清除記憶體中的金鑰並重啟系統。

已觀察到的 Mac 惡意程式

若要更細緻地了解 Jamf 在客戶環境中觀察到的 Mac 惡意程式，以下 為排名前 10 的惡意程式家族：

家族名稱：	類別	比例
Genieo	廣告軟體	13.63
Imobie	潛在的垃圾應用程式（PUA）	10.96
Multiverze	廣告軟體	9.44
Mackeeper	潛在的垃圾應用程式（PUA）	7.19
Tnt	潛在的垃圾應用程式（PUA）	6.07
Jailbreak	潛在的垃圾應用程式（PUA）	5.74
Ccleanmac	廣告軟體	4.33
Puagent	木馬病毒	3.07
Macinformer	潛在的垃圾應用程式（PUA）	2.33
Pirrit	廣告軟體	2.33

這些數字顯示，儘管資訊竊取程式等多種類型的惡意軟體數量大幅增加，廣告軟體與潛在的垃圾應用程式（PUA）仍然是終端使用者最常下載與安裝的應用程式。這是在所有作業系統平台中常見的趨勢，因為廣告軟體的觸及範圍更廣，而資訊竊取程式的攻擊則更具針對性。

Jamf Threat Labs 發布 了一篇關於**資訊竊取程式針對加密產業個人的部落格文章**。 攻擊者的目標是什麼？蒐集各種加密錢包中的憑證資料。研究團隊追蹤了兩起將資訊竊取程式植入受害者系統的攻擊事件：

1. 透過Google 贊助廣告：搜尋「Arc Browser」時，使用者點擊 Google 廣告會被導向惡意網站。
2. 透過虛擬會議：在洽談機會（如工作面試）時，攻擊者要求使用 Meethub 來安排會議。

在兩種情況下，使用者都被引導下載應用程式，繞過 Gatekeeper 並輸入他們的 macOS 登入 密碼。

我們 所研究的惡意軟體家族及上述範例說明了核心資安原則的重要性，例如：

- 僅從合法來源下載應用程式
- 採用審查流程（例如透過 Mac App Store 等可信第三方，或來自裝置管理廠商）
- 執行最新版本的資安軟體

資安長的觀點

- **導入專為 Mac 打造的 EDR 解決方案：** 我們經常看到軟體以 Windows 為優先，將 Apple 裝置視為企業內的次要對象。這樣的時代早已過去，尤其在資安方面更是如此。我們必須聚焦於從根本為 Apple 裝置設計的資安產品，因為威脅環境日漸成熟且持續擴張。
- **實作強大的 MDM 解決方案：**
  裝置管理是保障資安的關鍵。考量到使用者所擁有的自由度與存取權限，必須建立強健的架構來管理裝置與裝置上的使用者，以在惡意軟體爆發前就加以防範。
- **確保有效的溝通策略：**
  從資安與 IT 的合作、資安品牌宣導、訓練計畫、終端使用者意識提升到高層公告。有效地傳達你的資安計畫、所使用的工具及目前的策略，有助於所有人達成共識並專注於共同目標。

漏洞管理

並非所有漏洞都具有相同的重要性。它們的嚴重程度各有不同，大多會有一個評分等級。**Apple** 提供一份修補過的 macOS 安全漏洞清單，並列出修復該漏洞的作業系統版本。例如，在 2024 年，Apple 發布了 macOS 15.1.1，用來修補 **CVE-2024-44308** 和 **CVE-2024-44309** 這兩個漏洞 —— 這兩個漏洞可能允許惡意網頁內容突破 Web Content 沙盒。這些 CVE 被評為高嚴重等級。不過 Apple 也會針對低分數的 CVE 發布安全更新。這代表著什麼呢？優先順序很重要。當 IT 和資安團隊能全面掌握裝置上所有系統與應用程式的漏洞時，他們就能妥善處理最緊迫的問題。

Apple 提供一種更特殊的安全更新方式，稱為「快速安全回應（Rapid Security Responses）」，可在常規更新之間推出**重要安全改進**。為什麼這些修補更新有幫助？它們是輕量級的更新 —— 代表組織可以自動套用更新，而不會造成內部系統故障。舉例來說，在 2024 年 6 月至 2025 年 4 月之間，Apple 記錄了 **20 次** 包含 CVE 的 macOS 主要與次要版本安全更新。

深入解析一個真實漏洞：繞過 Transparency, Consent and Control（TCC）機制

在 Apple 的作業系統中，Transparency、Consent 與 Control（TCC）是一項關鍵的安全架構，用於要求使用者授權或拒絕應用程式存取敏感資料，例如麥克風、鏡頭與完整磁碟存取權。 繞過 TCC 的漏洞指的是這些控制機制失效，導致應用程式可以在未經使用者同意的情況下存取私密資料。這 表示攻擊者可以在不通知使用者的情況下，取得檔案、資料夾、健康資料、麥克風與鏡頭等資訊的未授權存取權限。

Jamf Threat Labs 發現了 **CVE-2024-44131，這是一個影響 Mac 裝置上「檔案提供者（File Provider）」功能的 TCC** 權限繞過漏洞。Apple 迅速於 macOS 15 中推出修補程式。像 CVE-2024-4413 這類的 CVE 強調了組織需要具備能偵測與阻擋異常行為的工具。主動監控應用程式行為與防止未授權存取資料，有助於組織在漏洞被 修補前搶先應對。

我們來深入檢視幾個最近（本報告撰寫於 2025 年 4 月）Apple 發布中的重要漏洞：

Apple CVE 修補內容	日期	漏洞評分	衝擊
macOS Sequoia 15.4.1	2025 年 4 月	CVE-2025-31200 CVSS – 分數：7.5｜嚴重性：高	CoreAudio
macOS Sequoia 15.4	2025 年 3 月	CVE-2025-24234 CVSS – 分數：7.8｜嚴重性：高	AccountPolicy
macOS Sequoia 15.4	2025 年 3 月	CVE-2025-24180 CVSS – 分數：8.1｜嚴重性：高	Authentication Services
macOS Sequoia 15.3	2025 年 1 月	CVE-2025-24085 CVSS – 分數：7.8｜嚴重性：高	CoreMedia

如前所述，在開發軟體時，漏洞是不可避免的（平均每 1000 行程式碼會出現約 25 個錯誤）。對資安專業人員來說，關鍵是能夠察覺並處理這些漏洞，以保護資料安全。作業系統未必總能保持最新（例如測試應用程式或代理程式），但組織仍需保持警覺並維持防護。

這不只是作業系統的漏洞問題。2024 年 11 月底，資安機構發布了 **2023 年最常被利用的漏洞報告**。（這是該報告的最新版本。）報告深入分析了排名前 15 的漏洞，包括 CVE 編號與每個漏洞可被攻擊者利用的方式。這些漏洞存在於多種運算平台的作業系統與應用程式中，是組織員工與學生日常使用的工具。如報告指出：「2023 年，惡意網路攻擊者利用的零日漏洞數量高於 2022 年，讓他們得以入侵企業網路並攻擊高價值目標。」該資安機構也進一步提供開發人員與終端使用者組織可採取的漏洞緩解措施。對於終端使用者組織，報告建議：

- 及時更新軟體、作業系統、應用程式與韌體
- 定期執行自動資產盤點
- 實施健全的修補管理流程
- 建立並記錄安全基準設定
- 定期進行系統備份，確保安全
- 維護最新的資安事件應變 計畫

如上所示，Apple 會定期針對已知漏洞提供作業系統更新。我們一直在強調，更新軟體是關鍵所在。組織最常透過行動裝置管理（MDM）方案來更新作業系統及員工日常使用的商業應用程式。然而，資安防禦還有其他層面。事件應變計畫、遙測資料的收集與分析，以及內部修補流程，都是組織領先部署的實例。執行上述措施也能開啟進階防禦層面，例如識別軟體漏洞等級，或透過威脅獵捕流程找出端點中潛藏的風險——這些方法整合運作，有助於降低組織風險。

Jamf Threat Labs 發現 macOS 中的 Gatekeeper 存在一項漏洞，CVE 編號為 CVE-2023-41067。此漏洞影響 Launch Services，可能導致未簽章且未經認證的應用程式執行，且不會向使用者顯示適當的安全提示。Gatekeeper 是第一道防線，用來阻擋未使用有效開發者 ID 簽署的網路下載應用程式。 雖然 Apple 迅速修補了此 CVE，但這也顯示任何系統都可能出現漏洞。正確的控管措施與訓練能有助於降低類似 Gatekeeper 漏洞帶來的風險。

在過去 12 個月中， 我們發現：

32%

的組織至少有一台裝置存在重大漏洞。

資安長的觀點

- **確保 你 能掌握整個組織的漏洞狀況：**
  盡可能瞭解終端使用者裝置或基礎架構中存在的漏洞，是一個絕佳的起點。你可以從這些資料出發，分析特定應用程式的影響範圍、潛在風險等。這是以資料導向方式為漏洞設定優先處理順序的好方法。
- **導入完善的修補計畫：**
  回到前述的 MDM 重點，擁有一套能協助維持軟體或作業系統在最新或支援的 N-X 版本的工具，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，也能更順利地支援業務運作。
- **導入風險為本的存取機制：**
  若有不符規範的裝置嘗試存取公司資源，應限制其存取，直到終端使用者修正問題，讓裝置盡可能輕鬆地恢復合規狀態。

第 3 部分：社交工程攻擊

社交工程是一種攻擊者透過操縱與欺騙個人以獲取敏感資料或存取憑證的手法。根據世界經濟論壇《**2025 年全球資安展望報告**》指出，「42% 的組織在過去一年中曾遭遇社交工程攻擊」。

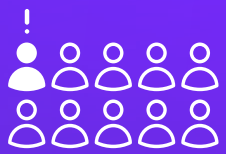
釣魚攻擊（Phishing）是社交工程的一種，是目前對組織構成威脅最普遍且破壞性最強的方式之一。雖然釣魚攻擊在行動裝置上更為常見（由於螢幕小、可攜性強且常在辦公室外使用），但 Mac（以及所有桌機或個人電腦）對攻擊者來說仍是極具吸引力的目標。畢竟，Mac 的使用者仍是資安防線中最脆弱的一環——終端使用者。

隨著攻擊手法日益複雜且更難以辨識，我們的個人與工作資訊持續面臨風險。隨著 Mac 裝置在工作中愈加普及，攻擊面也持續擴大。 攻擊者採用更高階的策略，利用逼真的介面、使用者體驗與仿真的溝通方式來誘騙毫無防備的受害者。不過，企業仍可採取保護使用者與資料的防護措施（例如持續性的員工訓練與威脅防護工具）。

在過去 12 個月中，我們發現：

25%

的組織曾遭社交工程攻擊



1 in 10

使用者點擊了惡意釣魚連結。

Jamf Threat Labs 發布了一篇文章，說明 **FBI 正在持續研究朝北韓（DPRK）**如何透過非法手段，特別是在加密貨幣產業中獲取財務利益。該 團隊指出一項具體攻擊事件：「一名使用者在 LinkedIn 上被一位自稱是科技公司人資團隊招募專員的人士聯繫。」攻擊者向使用者發送了一個壓縮的程式挑戰檔案（這是現代開發職位中常見的一個步驟），以評估其技能。當使用者點擊時，惡意程式（此案例中為資訊竊取程式）便會開始執行。訓練員工如何使用社群媒體與下載軟體，仍是所有組織應實施的重要課題。

釣魚攻擊中最常被濫用的前 20 大品牌

我們的研究發現，一些高知名度品牌經常被用於釣魚攻擊，可能是因為它們的名稱具有高度識別度與信任度。我們將這些品牌分為四類：

1. 娛樂	2. 商務	3. 公用事業	4. 個人用途
Netflix	Outlook	美國郵政服務 (USPS)	Amazon.com Inc
Bet365	Office365	俄羅斯天然氣工業公司 (Gazprom)	Telegram
Steam	Allegro	AT&T Inc	Facebook, Inc
	InterActive Corp	Orange S.A.	Chase
	騰訊	DHL	WhatsApp
		BT Group	Yahoo, Inc.

Mac 的使用情境多樣——包括求職、下載應用程式或在如加密產業等特定行業工作——這些都是威脅行為者常利用的場景，藉此取得資料。在上方的表格中，我們列出前 20 個遭用於釣魚攻擊的網站，並依照這四 類進行分類。

這些品牌因其知名度、聲望及對企業與個人的影響力，而被不法分子用於社交工程攻擊中以入侵使用者。他們成為一場日益精密攻防戰中不自覺的參與者。同時也值得注意的是，此清單並未涵蓋所有被攻擊者利用的品牌。這僅是過去一年的前 20 名品牌，未來可能每年、每月甚至每週都會有所變動，但這也足期揭示攻擊者的思維方式。他們正在利用這些品牌與使用者多年來建立的信任來進行剝削。隨著混合與遠距工作模式增加，攻擊者也在嘗試新的方式來誘使人們點擊惡意連結。

在現代世界中，我們的個人資訊時刻處於風險之中。隨著 Mac 在工作中愈加普及，攻擊面也持續擴大。 攻擊者採用更高階的策略，利用逼真的介面、使用者體驗與仿真的溝通方式來誘騙毫無防備的受害者。不過，企業仍可採取保護使用者與資料的防護措施（例如 持續性的員工訓練與威脅防護工具）。

Jamf 在一年內共偵測到約 **1,000 萬次釣魚攻擊**，影響了我們樣本群中的 **140 萬台裝置**。此外，我們發現約 **1.5 – 2%** 的攻擊經常被歸類為零日攻擊，意味著攻擊者使用尚未被發現或列入常見資料庫的新網域來執行釣魚攻擊。辨識並驗證零日釣魚攻擊，有助於組織保護使用者免受全新且未被偵測的釣魚網站侵害。

資安長的觀點

- **導入完善的訓練計畫：**
  這是我們成功的關鍵之一。我們執行進階的釣魚模擬攻擊、進行遊戲化訓練、針對提出需求的使用者提供單次訓練，並全年無間斷地允許使用者回報釣魚郵件，並即時獲得確認與回饋。這對我們來說不只是每年一次的「做完就好」訓練。
- **掌握最新趨勢與攻擊手法：**
  這或許看似顯而易見，但攻擊者總會利用任何機會，往往包括新聞中出現的新事件、突破性技術或爭議性話題。你需要調整訓練內容與封鎖策略來因應這些情況。這可能會讓某些使用者感到不安，但透明度是關鍵。訓練的目的是為了讓他們準備面對那些不會顧及他們感受、甚至會刻意挑起情緒以混淆與欺騙受害者的惡意行為者。
- **採取多層防禦策略：**
  沒有單一方法或工具可以讓你完全避免成為針對性釣魚攻擊的受害者。你需要從多個角度來進行防護。 封鎖惡意網域。確保已實施多重驗證（MFA）。 採行零信任架構。 啟用「不可能速度」等異常登入偵測規則。 其中一兩項措施可能還不夠，但多層防禦能最大限度地降低成為釣魚受害者的風險。

總結

Mac 惡意軟體正日益進化。但組織可以採取措施來降低 macOS 惡意軟體的風險。例如，收集並分析遙測資料有助於辨識並回報惡意軟體。威脅行為者持續尋找新的方式來入侵使用者與系統。但若具備合適的工具，組織可降低惡意軟體的影響。

建立正確的資安衛生習慣有助於降低風險。 定期更新作業系統與停用不必要的控制項（例如：第三方應用程式商店），可協助組織符合內部基準與外部標準框架。建立企業級應用程式商店並持續審查應用程式（尤其是私有或自訂應用程式），可讓組織更有效地監控、修復並修補存在漏洞的應用程式。

社交工程 是攻擊者取得敏感資訊最常見的方式之一。超過 90% 的網路攻擊來自釣魚攻擊。釣魚攻擊形式多樣，並不限於電子郵件。在整體裝置上（包含瀏覽器與應用程式）部署防護措施，對保護使用者與組織相當重要。

jamf

歡迎聯絡我們，深入了解 Mac 威脅環境。
或者聯絡您的的經銷商。