教育網路攻擊解剖：真實威脅與防範方法解析

介紹

對教育領域的 IT 和資安人員來說，他們面臨的挑戰遠比駭客還要艱難。駭客只要找到一個漏洞，或盜用一組帳號密碼，就能滲透進校園網路；但身為防禦者的你，卻必須每一次、每一個環節都做到萬無一失。

在這個全球緊密連結的世界裡，如果沒做到滴水不漏，教育機構就會面臨更高風險——不合規的裝置或被釣魚的帳號，可能成為資料外洩的入口，而這種事件會在整個基礎架構中引發連鎖效應。

「知識就是力量。」
– Thomas Jefferson

這句話對正派和惡意的一方，都一樣適用。對壞人來說，知識讓他們能看穿防禦上的漏洞，精準鎖定弱點；對好人來說，知識則能幫助我們理解駭客的手法，進一步洞察他們的攻擊計畫。

在這篇文章中，我們將會：

- 逐步解析「網路攻擊鏈」
- 展示一個針對教育機構的實際攻擊案例
- 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

透過放大檢視網路攻擊鏈的每一個階段，仔細剖析攻擊過程，教育 IT 團隊就能找出風險，並藉由持續回饋來強化防護。**在深入探討網路攻擊鏈之前，我們先來了解駭客為什麼特別鎖定教育產業。**

為什麼學校會成為駭客眼中的肥羊？

教育機構因為資源有限、基礎架構老舊，又握有大量有價值的資料，對駭客來說是越來越誘人的目標。**全球各地的學校經常得在資安與人事、學生服務、薪資 等重要需求間拉扯**，結果往往難以同時兼顧。財務壓力、過時的軟硬體，加上大量師生資料，這些條件疊加起來，讓駭客有可趁之機，也讓 IT 團隊疲於奔命。簡單來說，這一連串骨牌效應，讓學校成了駭客最愛下手的目標。

資源有限

「充分利用有限資源」在教育界不只是口號，而是從學生、老師到行政人員每天都在面對的現實。而不是談預算問題，但以現實面來看，全世界的學校都必須在有限經費中做取捨——資安預算常常得和聘請師資、學生餐食或教師薪資競爭，導致資安難以真正健全。

雖然學區通常會努力把資金分配到特定用途，但有限的財源往往還是會導致某些地方短缺，逼得行政單位必須犧牲一項重要功能，來成全另一項同樣重要的需求。駭客正是看準了這一點，所以他們對學校的攻擊經常能得逞。造成這種攻擊容易得手的原因包括：

過時的電腦裝置

一台電腦的有效壽命大約是 3 到 5 年。除此之外，缺乏對新安全功能的支援、效能不斷下滑，以及相容性問題，也會進一步降低學生和教師的使用體驗。

過時的軟體

就像硬體一樣，軟體也需要定期更新，才能把安全漏洞降到最低。 雖然訂閱制應用程式通常能即時取得最新版本，但長期下來的費用可能比永久授權還高，讓學校難以年年都維持更新。

仰賴單一平台

專為單一平台設計的解決方案，確實能提供對該系統更完整的支援。但「一套打天下」的通用解決方案，往往是靠壓低成本換取有限支援，導致裝置管理不完整、防護不到位。

工作量過重的 IT 人員

一般企業大約是 100 個員工配 1 位 IT 人員；但**在教育領域，這比例通 常高達三倍以上**——1 位 IT 人員要支援 300 人甚至更多。人力不足和 IT 過勞，正是導致資安防護薄弱的關鍵原因，也會讓教育這類受管制產業難以符合法規要求。

薪資缺乏競爭力

在美國，IT 技術人員有 1–3 年工作經驗的平均薪資範圍大約是 45,000–71,000 美元（年薪）。教育領域的 IT 技術人員（相同經驗）的薪資範圍則是 42,000–63,000 美元（年薪）。再加上人力不足，薪資 **比市場行情低 9%** 更讓學校難以吸引或留住優秀人才，進一步衝擊校園網路的安全。

缺乏培訓資源

IT 人員對主管提出的**前三大需求之一**， 就是能有系統性的訓練，學習新技能、擴充現有知識。Henry Ford 就曾精闢地說過： **「唯一比訓練員工卻看著他們離職更糟的事，就是完全不訓練他們，卻讓他們不斷留任。」**

有價值的資料

國民中小學校（幼兒園到高中）的資料，因為敏感度高、保存時間長，但防護資源有限，因此對駭客來說特別有價值。學生的個資（PII）可能被拿來進行金融詐騙、身份竊取或社交工程，而且這些濫用往往能潛伏多年不被發現。再加上資料外洩後的法律、聲譽與財務影響，駭客眼中的學校，就像是一座存放數位財寶的金庫，卻沒有銀行那種層層防護能防住 竊賊。

勒索

駭客之所以鎖定資料，最主要的原因就是它對學校與相關利害關係人而言價值極高。駭客非常清楚這一點，因此常用來當籌碼，威脅「付錢才能保證資料不外洩」。金額會依事件而異，但平均來說，**一起勒索 軟體引發的資料外洩，其代價** 約落在 438 萬至 537 萬美元之間。注意：**這個金 額範圍僅包含事件控制成本，不包含實際支付的贖金。**

聲譽

一旦攻擊事件被公開，遺憾的是，傷害往往不會就此結束。學校或教育機構常會面臨外界詢問，這往往會損害其公眾形象。駭客很清楚這一點，並會把這納入攻擊策略，經常對學校進行二次甚至三次勒索。難怪 2025 年第一季，**針對教育領域的全球勒索攻擊數量暴增了 69%** 。

法律

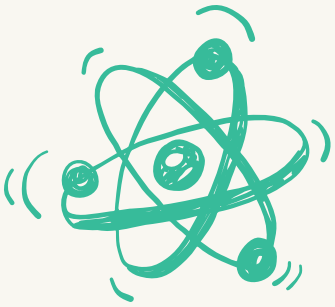
身為受法規管制、並且高度依賴政府資助的產業，教育機構一旦發生資料外洩，必須依法回報並接受調查。 由於教育機構必須承擔保護學生與教職員敏感資料的責任，若發生未經授權的資料外洩，可能會因違反法規而遭受巨額罰款，甚至失去州、聯邦或地方的資金補助。此外，若 未確實採取必要措施，相關人員也**可能因此承擔民事或刑事責任**。

身份盜竊

學生資料為駭客提供了建立「假身分檔案」的基礎，這些檔案可能被用來進行各種犯罪活動。最常見的是金融詐騙（下一段會說明），其次是針對學生進行霸凌、跟蹤，或 **透過社交工程鎖定更多受害者**，以取得更多資訊。

財務

尤其是未成年人，他們通常沒有建立信用或財務紀錄，這讓學生的個資成為**駭客 覬覦的目標，被拿來進行未經授權的金融交易，「往往要過很多年受害者才會發現」**。 此外，由於缺乏財務紀錄，學齡兒童通常也沒有監控服務，難以及時發現有人冒用他們的名義開設銀行帳戶、申請貸款或信用卡，往往要到成年後才會察覺。



什麼是網路攻擊 鏈？（Cyber Kill Chain）

攻擊手法各有不同，因為駭客會依照目標及其漏洞來選擇對應的威脅。雖然許多攻擊有相似之處，但因為變數眾多，使得資安防護既像是一門科學，也是一門藝術。

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，也就是所謂的「攻擊鏈」（Cyber Kill Chain）。這個鏈條分成七個階段——從事前準備到最終執行——每個階段都提供資安團隊找出弱點、攔截駭客的機會。

「那些是我的計謀，而這些是我的計畫」
– Tears forFears

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）：**
蒐集並鎖定目標，不論在線上 或線下。

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）。

針對教育機構的勒索攻擊模型

這一節要探討最近發生在**巴爾的摩市公立學區（BCPS）的勒索軟體攻擊事件**。特別說明一下，在撰寫本文時，這起攻擊仍在 FBI 調查中。因此，本文僅能依照已公開資訊進行推測，提供一個可能的案例來說明類似的攻擊如何在現實中發生。

1.

偵察（Reconnaissance）

在情報蒐集階段，駭客會收集有關學校基礎架構與網路環境的詳細資訊。這可能包含透過公開來源與社交工程，找出供應商、服務商以及關鍵人員。偵察可能是被動的，也可能是主動的；主動偵察有時會因為異常活動（例如大量掃描受害者網路造成流量激增）而觸發警示。目標是建立受害機構的輪廓，找出漏洞，並提高攻擊成功率。了解這些手法，能幫助 IT 負責人提早發現警訊，並加強防護。

2.

武器化（Weaponization）

在偵察之後，駭客會利用蒐集到的情資，客製化工具來進行下一步攻擊。這通常包含開發或購買惡意程式，或搭建整個攻擊架構與運作框架，來規劃勒索軟體的運作方式。現在，許多攻擊者仰賴勒索軟體即服務（RaaS）供應商，這種「統包式」的商業模式降低了攻擊成本與技術門檻。這樣 的模式讓任何程度的駭客都能用相對低成本取得進階攻擊能力， 只要與服務商分贓即可。多了解這種模式，有助於 IT 團隊提前預測並因應不斷演變的威脅。

3.

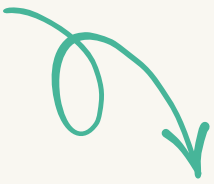
傳遞（Delivery）

在傳遞階段，駭客通常透過釣魚郵件等社交工程手法，把惡意程式散布到多個終端，幾乎不費力氣，輕而易舉。 像電子郵件、簡訊、社群媒體這類管道，都能大幅提高攻擊成功率，尤其是在針對個別使用者時。像 Jamf for K-12 這類解決方案，能幫助防禦這些攻擊，例如阻擋釣魚網址、監控裝置健康狀態，以及透過安全註冊設定檔來隔離資料。若發生資料外洩，IT 團隊能自動化清除資料，以保護敏感的校園資訊。這些 工具能幫助 教育機構打造 更主動的 防禦策略。

4.

利用（Exploitation）

在利用階段，駭客會用惡意程式來攻擊系統漏洞、提升權限，或利用釣魚取得的帳密進入網路，這通常取決於前期的偵察成果。進階惡意程式往往透過加密來隱藏行為，以規避偵測。Jamf 的解決方案能透過監控裝置健康狀態、啟動即時修復流程，以及停用已遭入侵的帳號，來降低這些攻擊的風險。此外，Jamf 在管理、身分與資安上的無縫整合，也能協助啟用多重驗證 (MFA) 來強化帳號安全，並確保裝置隨時更新到最新修補程式。這種多層次防護，讓 IT 團隊能降低風險，並在校園環境中快速應對事件。



5.

安裝（Installation）

在安裝階段，勒索軟體會被部署到受害裝置上，為後續攻擊鋪路，鎖定學生和老師資料，並癱瘓部分學區的 IT 系統。為了抵禦這個階段，IT 團隊必須隨時掌握狀況並確保合規，透過偵測、阻止與修復威脅來保護環境。Jamf 能協助阻擋已知惡意軟體、隔離有害程式碼，並監控裝置健康狀態的安全變化。針對未知威脅，裝置紀錄可轉送到 SIEM 平台，讓教育機構能更深入進行威脅獵捕，加快事件回應。

6.

指揮與控制（Command and Control）

在指揮與控制階段，受感染的裝置會開始連線到攻擊者的伺服器，以取得檔案目標和加密金鑰，讓攻擊者能進行資料竊取和勒索。遭入侵的裝置會被掃描，以鎖定高價值檔案（例如 Word、Excel、PDF 和資料庫），有時還會額外下載工具，支援攻擊者後續的行動。攻擊的目標是要在校園網路中取得最大的存取範圍。阻止這類通訊是關鍵。整合的身份與資安工具，可以停用被盜用的憑證、阻擋存取惡意伺服器，並在裝置不符規範時自動觸發修復流程，幫助 IT 團隊守護校園環境，同時降低攻擊成功的機會。

7.

達成目標（Actions on Objectives）

在網路攻擊鏈的最後階段，攻擊者會執行最終目的，可能包含資料外洩、勒索、橫向移動，或是發動 DDoS 攻擊。勒索軟體通常會加密檔案、刪除原始檔，並留下勒索要求；更嚴重的情況甚至會威脅公開或進一步利用被竊取的資料，要求額外贖金。每一次攻擊都會依照駭客的目標量身設計，結果往往難以預測，對教育機構更可能帶來毀滅性的影響。將管理、身份與資安工具完整整合，可以封鎖惡意流量、阻止資料外洩，並停用遭竊取的憑證。自動化修復流程和即時遙測，能確保只有符合規範的裝置能存取學區資源，打造縱深防禦策略。

jamf

補強你的防護漏洞

因為防護不足、過度依賴桌面作業系統而產生的資安缺口，會讓行動裝置暴露在風險中，讓駭客有機可乘。

雖然行動裝置不是造成資料外洩的唯一風險，但因為職場使用越來越普及，加上個人裝置存取公司資料的情況增加，行動裝置仍然是首要攻擊目標。**Jamf Threat Labs** 的研究數據指出：**「有 40% 的行動使用者正在使用存在已知漏洞的裝置。」**在 這些裝置上，若風險因子沒有被管控，駭客就能夠：

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

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。有些攻擊（例如影響 BCPS 的勒索軟體事件）顯示出駭客可能會 **和多個攻擊團體合作，以取得初步存取權限** ，再展開攻擊行動。由於攻擊的動態特性，即使是作業系統內建的防護措施（不論平台），也可能被繞過，讓裝置、使用者和資料面臨外洩風險，就像 **BCPS 事件中 25,000 名受影響對象**一樣。

依循成熟的 **縱深防禦架構** 來規劃資安策略，能大幅降低裝置上的風險， **抵禦網路威脅**，阻止已知攻擊，並在事件發生時快速透過自動化修復流程回應，維持端點的合規性。

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，這些多層防護也能延伸到整個企業，為所有要求存取公司資源與資料的裝置與作業系統提供基本的安全防線。

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**
- **擴充的設定與稽核 框架，協助客戶符合合規要求**
- **一致性的弱點管理、威脅防護與政策控管**
- **完整的端點遙測資料可輸出至第三方的日誌收集與 分析工具**
- **涵蓋 Mac 與行動平台（包含 macOS、iOS/iPadOS 和 Android）的安全性報告；同時也將網路威脅防護擴展到 Windows 和 Chromebook**
- **無論是公司配發或個人裝置，都能一致執行政策**

總結

網路攻擊鏈為 IT 團隊提供了一個有架構的視角，去預測勒索軟體攻擊如何從 偵察到資料外洩與勒索逐步展開。

正如巴爾的摩市公立學校的真實案例，每個階段都揭示了防護上的裂縫，若未加以補強，這些弱點就會被利用。在預算有限、基礎建設老舊、IT 團隊負擔過重的情況下，學區在抵禦進階威脅時面臨相當大的挑戰。

Jamf for K-12 透過整合裝置管理、身份與存取控管、以及端點安全，協助打造縱深防禦策略，全面保護教育領域最重要的資源：學生、老師和學區資料。我們的方法能讓支援團隊在 Apple 與多平台環境中，以同樣的水準來偵測、阻擋並修復威脅。透過即時遙測、自動化流程和安全存取控管，學區能修補關鍵的安全漏洞，並確保符合規範。在當今的威脅環境下，多層防護已經不是選擇題，而是教育安全的必要條件。

想親眼看看縱深防禦在你的環境中如何運作嗎？

jamf

立即體驗 Jamf

www.jamf.com/zh-tw/