資安破口系列1一每秒遭1.5萬次網攻，連工廠冷凍庫都不放過…俄羅斯駭客嗆：台灣網路安全不堪一擊！

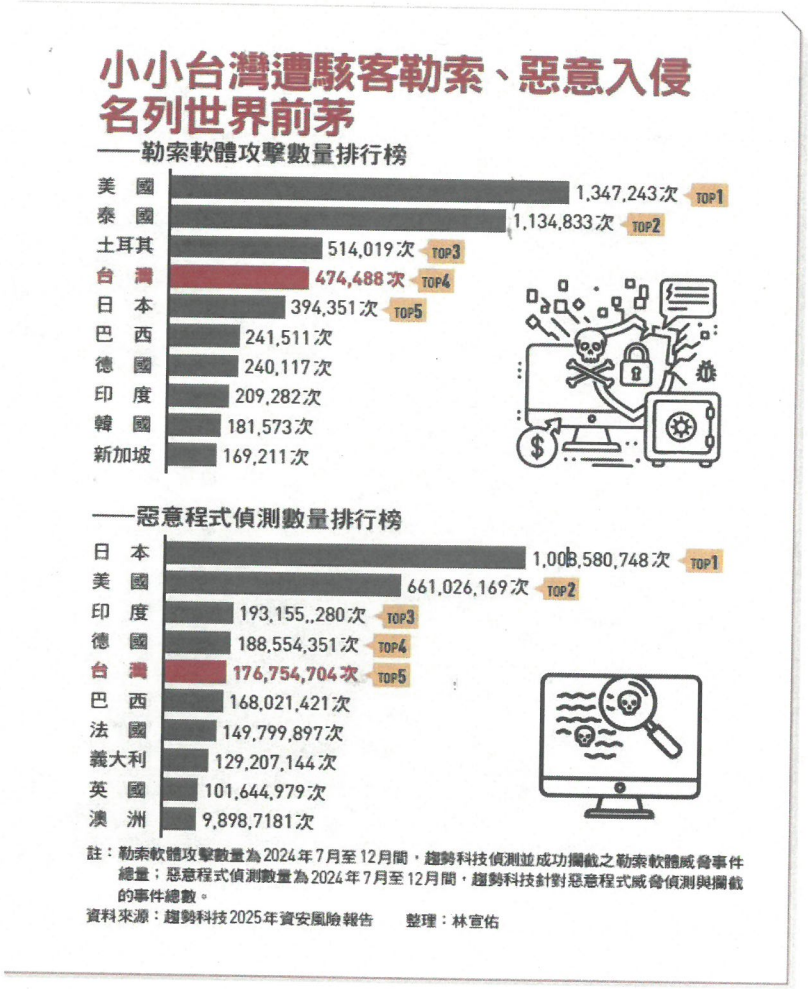
撰文 | 陳子萱 研究員·林宣佑　分類 | 科技 (https://www.businesstoday.com.tw/catalog/18301
圖檔來源 | Shutterstock
日期 | 2025-10-16 12:00

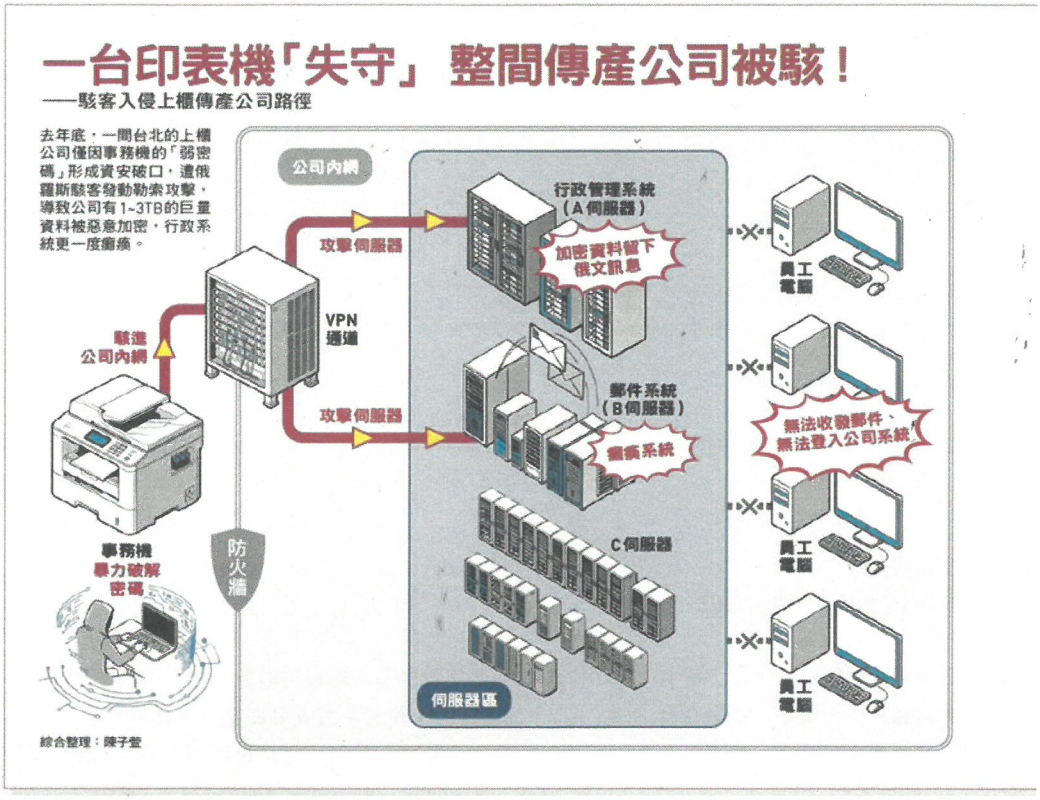
+A -A　加入收藏

印表機、投影機、防火牆、溫控系統……，這些不起眼的連網設備，早就成為境外駭客瞄準的資安破口。他們藉此入侵「手無寸鐵」的民間組織及中小企業、「缺乏防禦盾牌」的政府委外包商，一路進攻，意圖癱瘓設備或竊取資料。

2023年，台灣每秒有1.5萬次的網路攻擊；2024年，台灣政府網站每天受到駭客攻擊達240萬次。

敵我攻防並非正面交鋒，攻擊者瞄準的就是這些無人鎮守的邊陲地帶，而當境外駭客從邊陲滲透，那些被遺忘的邊疆堡壘足夠堅實嗎？





早晨七點，台北一家上櫃傳產公司的辦公大樓裡，一名值班員工才剛坐下，打開公司電腦、啜了一口熱咖啡準備開工；但下一秒，眼前的電腦卻跳出「無法收取電子郵件」的異常畫面。他重新整理網頁，竟換來「無法登入系統」的警訊。沒多久，隔壁區的同事也一一傳來哀嚎，原本還在熱絡寒暄的辦公室，氣氛瞬間凝結。

資安主管聽聞回報後，直覺不對勁，一小時後緊急召集技術人員和資安廠商到場檢查。結果在公司主機內，發現有一到三TB的巨量資料已被惡意加密，「光一組密碼長度就高達三十八位元……，而且還像『包肉粽』一樣層層加密，就算破解一組、還有兩三道關卡要破。」該名高層相當詫異。

接著，他們看到一則俄羅斯文訊息，並附上一組電子郵件。大夥才恍然大悟，這是俄羅斯駭客的勒贖攻擊，駭客還貼心留下兩把「已解鎖」的金鑰樣本，無聲暗示著：想要解碼、就找我付錢。

但這家每年平均資安預算高達五百萬元的上櫃公司，並非沒有資安防護城牆，平時已阻擋不少惡意入侵。經營團隊百思不得其解，而事後分析的結果，讓所有人瞠目結舌──這一次駭客進攻的破口，竟然只是一台印表機。

八位數密碼兩小時內破解
駭客一晚就讓上櫃公司癱瘓、損逾千萬

駭客在前一天深夜，看準辦公室裡一台「八位數字密碼」的事務機，不到兩小時就破解成功，透過VPN攻進內網，再迅速橫向移動、掌握內網架構，最終取得公司網域的「最高權限」。此時的駭客等於拿到一把總鑰匙，可以打開公司網域裡的各個大門。接著，駭客針對重點伺服器發動攻擊、瘋狂加密資料，經過數小時行動後，便迅速撤離。隔日，公司的行政運作系統，一開機就癱瘓。

所幸遭加密的巨量檔案，主要為後端行政管理資料，尚未衝擊營運，團隊決定向檢警報案。這次遭駭事件，耗費兩個月時間進行資料修復和資安優化措施，相關經費已超過千萬元。

「這次真的算運氣好……」這位董事長自覺僥倖，他深知，若駭客一路進攻取得集團核心資料，損失恐怕不只是千萬數字而已。

台灣每秒1.5萬次遭網攻
手段變了 專從不起眼設備直搗核心

翻開國安局「二〇二四年中共網駭手法分析」報告，政府機關在二四年每日平均遭駭侵數量高達二四〇萬次，是前一年的兩倍。而在今年的台灣資安大會上，美國在台協會（AIT）處長谷立言也援引資安公司報告，早在二三年上半年，亞太地區的惡意網路威脅有五五%、約二二四八億次攻擊都發生在台灣，相當於在台灣每秒有一．五萬次的網路攻擊。

數以萬計的網攻威脅，大多來自駭客的「測試攻擊」，也就是駭客先來「敲門」、但尚未「打破城牆」，是攻擊者嘗試尋找資安破口的初期攻勢。一旦成功破門，便能長驅直入，來到組織內網，進一步癱瘓設備或竊取資料。

但這些巨量的測試攻擊，到底都發生在哪裡？答案是：可能在你想像不到的「邊陲地帶」。

「印表機、投影機、網路攝影機、VPN設備……，只要是能跟公司網路連線的設備，就有可能被駭客入侵。」研究資安威脅超過二十年的杜浦數位安全執行長蔡松廷指出，作為企業內網入口點的邊緣裝置（edge device），不再只是路由器，當各種機器、設備也能連網，若存在資安弱點，就可能變成駭客的攻擊入口，直搗公司內部系統。

早期，駭客專注攻擊存有關鍵資料的電腦或伺服器；或者，主要依賴惡意釣魚郵件，以單一員工為進攻標的。不過近年來，這些存放公司關鍵資料的核心區塊，開始架設完整的資安防護網，對駭客來說，入侵成本高。

沒想到，隨著連網的邊緣設備興起，恰巧為駭客開闢更多條進攻路線。

要攻打城堡的駭客，不再只盯著配有重兵駐守的大門，轉而從「看守人力單薄」、「沒人看守」、甚至「沒有上鎖」的眾多邊陲角落悄悄竄入；在辦公室的場景裡，那就是你我身旁的事務機、投影機或Wi-Fi分享器。「這些邊緣的連網設備，平常根本不會有人去檢查資安漏洞。」蔡松廷說。

不只是投影機、印表機，奧義智慧執行長吳明蔚進一步指出，近年駭客更已經開始瞄準「年久失修」的防火牆。這本該是保護企業或機關的「城牆」，經常已有一定的資安層級，卻反而更容易遭到輕忽，例如未即時更新系統，導致敵人有機可乘。

延伸閱讀：
資安破口系列2一駭客拿農場「練兵」，生產線一夜全癱瘓！超過百家上市櫃發資安重訊，小公司最慘烈
(https://www.businesstoday.com.tw/article/category/183015/post/202510080057/)
資安破口系列3一俄國駭客嘲笑台灣資安，在社群網站秀戰果
(https://www.businesstoday.com.tw/article/category/183027/post/202510080070/)