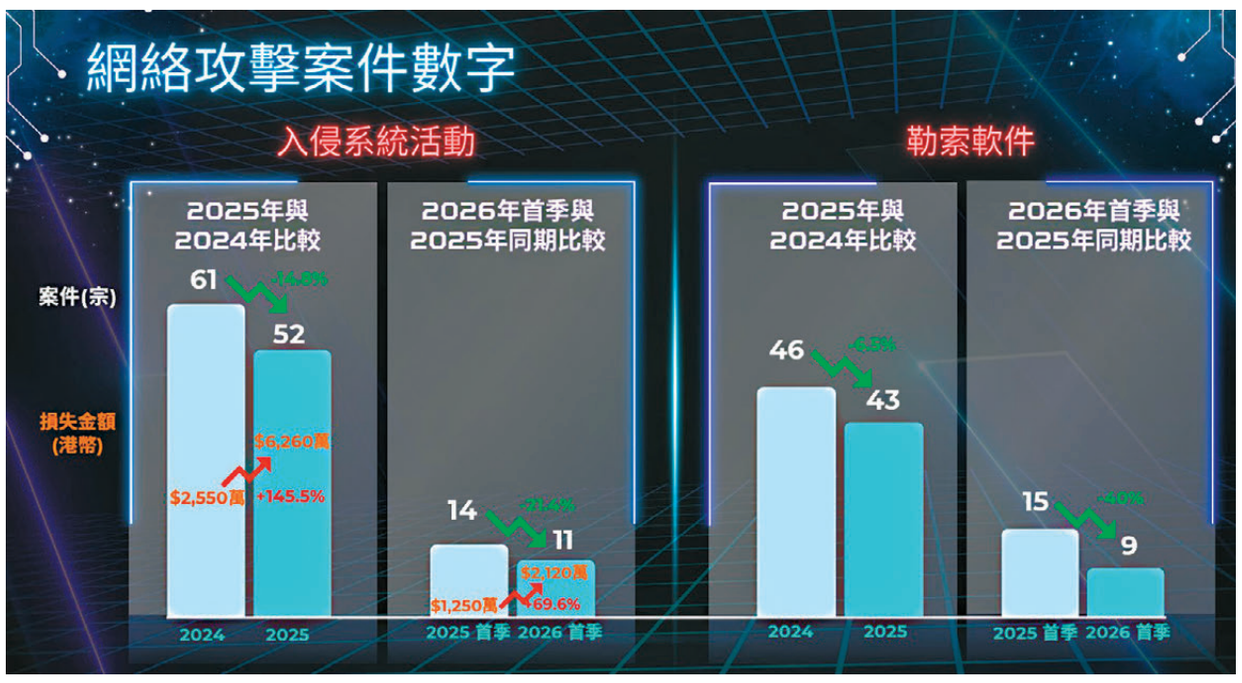
港網絡威脅情報年增2.4倍達154萬項

警方遏止五大國際黑客團夥攻擊 保住政府空陸運輸等重要基礎設施



警方發布《網絡安全報告2025》顯示，雖然香港去年整體的科技罪案及具破壞性的網絡攻擊案件均下降，但網絡安全及科技罪案調查科去年處理的網絡威脅情報按年上升約1,000萬項，當中超過154萬項針對香港，按年增加2.4倍。分析亦發現，有5個惡名昭彰的國際黑客團夥，曾發起針對香港重要基礎設施的惡意活動，幸警方透過情報共享、持續監控及跨機構合作，相關攻擊企圖均能在早期被識別及遏止，避免造成服務中斷或數據損失。報告反映香港持續推動高效網絡安全防禦機制，以及網絡安全生態建設的重要性。

●香港文匯報記者 曾立本

網絡安全及科技罪案調查科去年共處理逾3,500萬項網絡威脅情報，按年升約千萬項，平均每日超過9.6萬項；當中超過154萬項針對香港，按年增加近110萬項。數字反映出網絡威脅的規模與複雜性持續攀升。這些情報包括可疑網站、IP地址、域名、攻擊手法及惡意軟件雜湊值等，主要涉及三大類：系統安全漏洞、網絡釣魚及偵察活動，分別佔34%、27%及17%。

同時，網罪科利用網絡安全行動中心聯盟（SOCA）分享的國際情報進行關聯分析，發現5個在國際間惡名昭彰的黑客團夥，同樣有針對香港重要基礎設施的惡意活動，包括政府、航空運輸、陸路運輸、海運業、銀行及金融服務、廣播、通訊、能源、醫療保健、公共事業，以及其他重要基礎設施。透過情報共享、持續監控及跨機構合作，相關攻擊企圖均能在早期被識別及遏止，避免造成服務中斷或數據損失。

7.8%重要基礎設施有漏洞

網罪科去年對香港重要基礎設施的網絡資產進行逾10萬次網絡安全評估，包括域名及IP地址等，發現當中7.8%存在不同程度的系統安全漏洞。

網罪科深入分析約8,000個系統安全漏洞，當中95%屬中低風險，5%屬極高及高風險，主要包括三大類：**第一**，企業員工系統登入資料外洩或被盜用；**第二**，企業未妥善管理域名，令攻擊者可盜用閒置子域名，建立像真度高的釣魚或詐騙網站；**第三**，雲端儲存服務配置不當，令內部系統意外公開；如企業未有多重認證或登入白名單等措施，便容易被黑客入侵。

●網罪科總警司林焯豪（中）表示，去年有逾154萬項網絡威脅情報針對香港。 香港文匯報記者曾立本 攝

受網絡威脅機構增至36%

為了解本港重要基礎設施營運者及大型機構的網絡安全意識和應變準備，網罪科每年均進行抽樣問卷調查。2025年調查發現，36%受訪機構表示去年曾頻繁受到網絡威脅，較2024年上升16個百分點。

儘管如此，逾八成受訪機構認為自身保持高度警覺並具備充分應變準備。同時，接近八成機構已增加網絡安全預算，另外逾八成已經或正計劃運用AI提升防禦能力。

網絡安全及科技罪案調查科總警司林焯豪表示，結合執法和調查經驗，以及對創新科技發展及網絡威脅形勢的觀察，多位專家整理出以下5個新型技術潛在的網絡安全威脅，包括量子技術、區塊鏈、雲端運算、衛星技術和人工智能。

林焯豪指，網罪科會繼續透過多方面主動措施，包括加強國際合作、強化公私營合作、推動情報與數據共享、強化協作式網絡防禦、完善法律法規、推廣網絡安全意識與教育、推進網絡防禦準備工作。

警方教路四招防禦網絡威脅

1. 減少可被攻擊的入口。對外開放的系統、VPN、雲端服務、物聯網裝置及第三方程式庫，都可能成為黑客入侵的門口。機構應定期掃描外部攻擊面，優先修補高危漏洞，關閉不必要的端口及舊有協定，並將管理介面與測試環境適當分隔。
2. 管好身份和權限。不少攻擊源於外洩密碼、閒置賬戶、過大權限，甚至利用深偽技術冒認身份。機構應為遠端登入及管理員賬戶採用抗釣魚多重認證，並貫徹「零信任」理念，每次存取都要驗證，權限以「剛夠完成工作」為原則。
3. 做到「看得見、查得到、復原得到」。黑客可能在系統內潛伏一段時間，機構應善用EDR及XDR等工具，配合人工智能更早發現異常。日誌須集中保存並防篡改；備份則要保留不可更改或離線副本，並定期進行還原演練。
4. 把網絡安全變成恒常管理和文化。供應商、外判商及第三方應用程式，都可能成為攻擊者繞道入侵的渠道。機構應將供應鏈風險納入日常管治，每年至少進行一次涵蓋勒索軟件、供應鏈事故及深偽社交工程等情景的演練，員工亦應持續接受培訓，識別釣魚電郵及「深偽」來電。

資料來源：警方網絡安全及科技罪案調查科

去年入侵系統案損失金額飆倍半

綜合數據分析，香港網絡主要存在5大類安全隱患，包括利用人工智能進行網絡犯罪、針對雲端服務攻擊、供應鏈與第三方漏洞入侵、物聯網安全風險、針對互聯網第三代Web3與區塊鏈攻擊；常見風險包括：智能合約漏洞、私鑰被盜、「假充值」等跨鏈漏洞。主要目標是竊取虛擬資產或操縱去中心化應用程式。2025年警方網罪科實際處理的網絡安全事故顯示，大部分受害公司同時存在多個管理及系統設計弱點，令黑客更容易入侵。

去年本港錄得31,571宗科技罪案，當中約87.2%為網上騙案，雖然具破壞性網絡攻擊的入侵系統活動及勒索軟件，只佔整體科技罪案0.3%，但每次網絡攻擊對受害機構均造成非常嚴重後果。

統計顯示，去年全年及今年首季的涉案損失金額俱上升，主要來自幾宗本地金融機構及虛擬資產服務相關平台，因系統入侵而造成大額損失。其中，去年錄得52宗入侵系統活動的案件，損失金額增至6,260萬元，比前年大幅上升145.5%。今年首季則錄得11宗入侵系統的案件，損失由去年同期1,250萬元增至2,120萬元，升幅達69.6%。其中最大一宗入侵系統案件，為今年2月一個加密貨幣交易平台軟件外判商員工，涉嫌利用系統漏洞查看客戶電子錢包資料，將價值2,000萬元加密貨幣轉走。

常見漏洞是遙距登入密碼簡單

網罪科就去年所處理網絡安全事故，歸納出受害機構常見的系統漏洞及弱點，包括對外開放但保護不足的遙距登入服務；例如VPN及遠端桌面存有漏洞的網絡設備；公司或員工使用簡單密碼、重複使用密碼，甚至使用曾外洩密碼，令黑客容易以暴力破解方式登入；員工點擊釣魚電郵內的惡意連結或附件，則導致黑客入侵或加密檔案進行勒索。

警方留意到，不少受害機構沒有完善事故處理機制，即使系統出現警報，亦缺乏分流及升級程序，令監控和偵測形同虛設。部分機構未有集中管理審計日誌，而備份系統亦未有真正隔離，結果黑客能一併刪除或加密備份，令復原和調查更困難。

另外，網上投資騙案損失金額上升，是帶動科技罪案損失金額上升的主因。去年最大一宗投資騙案，受害人為本地一家物業公司董事，他收到騙徒利用新技術假冒加密貨幣礦機製造商的語音通訊，誘騙他將原本用於購買一萬台加密貨幣挖礦機的分期付款，轉入新的加密貨幣錢包，損失1.4億元。

首季長者受騙失財激增近八成

●中銀香港推出「防騙教育號」及「防騙裝甲號」流動宣傳車。圖為主禮嘉賓主持防騙宣傳車啟動禮，並在車前合照。

香港文匯報訊（記者 蕭景源）為加強全民防騙的公眾教育，中銀香港在香港金融管理局及警務處反詐騙協調中心支持下，推出「防騙教育號」及「防騙裝甲號」兩架流動宣傳車，穿梭港九新界以互動形式宣傳防騙及反洗錢資訊。警務處處長周一鳴昨日出席啟動禮時表示，今年首季錄得9,400多宗騙案，較去年同期微跌6%，但損失金額增至18.5億元，受騙群組中包括1,200多名長者或退休人士，較去年同期增加三成，損失金額高達5.3億元，增幅接近八成，警務處將以長者及退休人士作為重點防騙宣傳對象。

周一鳴表示，長者受害人勤勞一生，被騙去安享晚年的血汗錢，除蒙受金錢損失，同時承受心理創傷。層出不窮的騙案手法，顯示反詐騙工作仍路途遙遠。有關宣傳計劃要持續到位，走進社區，為達至精準防騙，已將長者及退休人士群組，以及投資騙案分別定為今年的重點宣傳對策及項目，宣傳工作包括製作防騙粵劇，與電訊商合作教育長者安全使用智能電話，向提取退休金人士作出防騙宣傳，以及邀請財經界KOL在節目中加入投資騙案的資訊等。

投資騙案升幅較高

金管局助理總裁陳景宏表示，香港的詐騙情況仍然嚴峻，投資騙案上升幅度較高，長者被騙令人痛心。為了加強銀行客戶自我保護能力，所有零售銀行已推出「智安存」服務，讓銀行客戶將部分存款「鎖起」。金管局早前聯同警務處和證監會推出多項打擊投資騙案的措施，亦已向銀行發出相關指引，要求銀行偵測和評估客戶是否墮入投資騙案，並提供一系列建議查問方法，增強銀行偵測和阻截投資騙案的能力。

中銀香港副董事長兼總裁孫煜表示，中銀今年首季防騙工作成效持續提升，有效管控可疑戶口及交易通道。針對近期經常發生的投資騙案，亦進一步優化防騙預警邏輯，保障客戶資產安全。

他強調，中銀在防騙及反洗錢領域投入大量資源，不斷提升智能防控及防欺詐管理水平，全力配合金管局、警務處及銀行公會推進多項措施，保障客戶存款，提升可疑活動識別與交易監控能力。

黑客歸還Canvas客戶資料 專家：付贖金如飲鴆止渴

香港文匯報訊（記者 蕭景源）網上教育平台Canvas遭黑客組織ShinyHunters攻擊，全球約2.75億用戶資料外洩，影響遍及全球逾9,000間機構，總量達3.65TB。Canvas母公司Instructure早前發聲明表示，已與黑客達成協議，對方已向公司歸還所有數據，並收到銷毀數據的數碼憑證，但未有提及是否有交付贖金。香港資訊科技商會榮譽會長方保僑表示，從營運現實來看，公司停擺每小時都是金錢與聲譽的損失，絕對可以理解，但支付贖金往往是飲鴆止渴。

倡撥資源加強網絡韌性

方保僑認為，現實中，支付贖金既不保證能拿回完整數據，更無法確保黑客沒留後門；一旦開了先例，公司會被標籤為「優質客戶」，招致更頻繁的攻擊。面對系統癱瘓，最實際的做法是將該筆「贖金」轉化為「搶救資金」，即時聘請專業團隊進行系統重建與數據清洗。建議企業應該將資源放在加強網絡韌性，以專業的應變方案向客戶展示公司有能力保護數據，這才是真正止蝕並保護長遠聲譽的做法。

就Canvas系統遭入侵事件，香港警方截至本月12日共接獲兩宗求助個案。一宗由本地教育機構主動通報，該機構因本身使用Canvas，從新聞得悉平台遭入侵後主動報案，並未發現有系統數據外洩問題。

另一宗為本地市民指有騙徒冒認Canvas平台技術支援人員，試圖誘騙其透露個人資料及進行匯款；該市民識破騙局後，主動向警方提供相關情報。

警方提醒使用第三方平台服務的機構，應加強第三方風險管理，包括定期檢視權限設定，嚴格限制第三方平台可存取的資料範圍；制定事故應變及數據備份方案，以確保業務持續運作；同時，應加強員工的網絡安全意識，尤其要警惕數據外洩後可能衍生的針對性釣魚攻擊，並建立內部通報機制，以便員工在發現可疑情況時能即時上報。

此外，警方呼籲市民提高警覺，留意騙徒可能冒認第三方平台員工發動釣魚攻擊。防範釣魚騙案應遵循「一停、二諗、三核實」的原則，對任何來歷不明的訊息保持警覺，切勿隨意點擊連結、下載附件或輸入個人資料。

凡涉及金錢或敏感資訊的要求，務必透過官方渠道核實對方身份。