港去年網絡威脅44萬項 逾65%涉「釣魚」

網罪科首發表網安報告 揭黑客入侵企業伺服器盜客2100萬元

警方網絡安全及科技罪案調查科（網罪科）今年踏入成立十周年，並發表首份網絡安全報告，涵蓋全球以及香港2024年的網絡安全形勢，報告重點分析香港重要基礎設施面對的網絡安全風險。網罪科表示，本港去年發生逾百宗入侵系統活動及勒索軟件案件，其中涉款最多的一宗入侵系統案件，發生在去年10月至11月間，一間金融服務公司職員發現一名客戶賬戶有不尋常交易，涉及金額2,100萬元，向客戶查詢後獲悉公司伺服器存在漏洞，黑客透過漏洞向自己的手機發出一次性密碼，從而控制有關客戶的賬戶控制權，盜走款項。至於涉款最大的勒索軟件案件，發生於去年9月，一間資產管理公司職員發現電腦內的檔案被加密，黑客留下勒索信息要求支付逾500萬美元贖金，但公司最終無交贖金。

●香港文匯報記者 蕭景源

●左起：網絡安全及科技罪案調查科(網絡安全、法理鑑證及訓練)高級警司梁靄琳，網絡安全及科技罪案調查科總警司林焯豪，網絡安全及科技罪案調查科網絡安全組警司陳純青。 香港文匯報記者郭木又 攝

2024年及2025年首季科技罪案數字

分類	案件宗數（與前一年同期比較）		涉及金額（與前一年同期比較）	
	2024年	2025首季	2024年	2025首季
整體科技罪案	33,903(-0.6%)	7,680(+1.1%)	51.3億元(-6.7%)	14.3億元(-11.7%)
入侵系統活動案件	61(+64.9%)	14(+7.7%)	2,550萬元(+1,114.3%)	1,250萬元(+1,150%)
勒索軟件案件	46(+100%)	15(+15.4%)	0(不適用)	0(不適用)
分散式阻斷服務案件	5(不適用)	0(不適用)	460萬元(不適用)	0(不適用)

資料來源：警方網絡安全及科技罪案調查科 整理：香港文匯報記者 蕭景源

警方對網絡威脅預測和警示

(1)人工智能（AI）網絡威脅及系統安全風險將會持續上升。人工智能是國家安全的重點領域之一，各機構必須實施完善的人工智能安全措施和部署先進的威脅偵測系統。

(2)勒索軟件仍會繼續猖獗。無論機構規模大小，都必須有健全的備份策略、事故應變計劃和安全意識培訓，以應對勒索軟件的持續威脅。

(3)隨着香港致力發展成為全球Web3和虛擬資產樞紐，針對區塊鏈和加密貨幣的攻擊將會越趨頻繁。加強網絡安全協議和監管合規是保持香港領先地位的關鍵。

(4)物聯網安全風險會不斷升級。香港擁有全球最先進的物聯網生態系統之一。在推動低空經濟和大型活動時，必須加強監察電子顯示屏和無人機控制系統中的潛在漏洞。

(5)供應鏈和第三方風險逐漸增加。香港對全球軟件及第三方服務的依賴使我們面臨更廣泛的攻擊面，企業必須加強對第三方服務及整個供應鏈的安全評估。

(6)雲端保安和混合工作模式的風險將會持續升溫。使用雲端服務的企業必須做好嚴格的雲端服務管理，防患於未然。

(7)針對重要基礎設施的攻擊將陸續湧現，對香港的必要服務和公用事業構成重大威脅。必須優先加強電腦系統和運營科技（OT）系統的網絡安全，共同守護大眾市民利益。

資料來源：警方網絡安全及科技罪案調查科

網罪科對2024年共44萬項針對香港的網絡威脅情報分析，發現有超過65%、即超過28萬項與網絡釣魚有關，通常有四種手法。最常見手法是黑客利用網絡釣魚手法製造入侵電腦系統的入口，例如發送釣魚電子郵件或短訊，誘使受害者或機構員工點擊惡意連結，目的是引導受害人下載惡意軟件，或輸入企業系統或雲端服務的登入資料。

勒索軟件成網絡罪犯主要牟利工具

其次是殭屍網絡，由攻擊者控制的一個受感染設備網絡，用於執行網絡攻擊，例如分散式阻斷服務攻擊或濫發電郵。此外偵察活動，即黑客收集有關目標系統、網絡或機構的資訊，以識別系統安全漏洞，策劃潛在攻擊也十分常見。再其次是惡意軟件，包括病毒、蠕蟲、勒索軟件和間諜軟件。

當中，勒索軟件已成為全球網絡犯罪分子的其中一個主要牟利工具，並演變成龐大的地下產業，包括「勒索軟件即服務」（RaaS）的興起及數據洩露網站的出現。

網罪科警司陳純青指出，透過剖析去年的網絡安全事件，發現不同受害機構中被重複利用的系統安全漏洞，包括存取控制和配置不足的問題。自2020年在家工作普及化，企業需要透過虛擬私人網絡（VPN）及遠端桌面協定（RDP）連接讓員工在家工作，但企業在存取控制和配置方面存在不足之處，例如未有及時修補已被公開披露的漏洞，或者欠缺措施抵擋攻擊者利用憑證攻擊，即是撞密碼，令攻擊者更容易遙距入侵企業的電腦網絡。

防火牆未修補及舊版系統成攻擊目標

其次是系統過時並且未被修補的問題。未修補的防火牆和舊版系統是攻擊者的兩個主要攻擊目標。不論企業或公眾，都應該及時更新電腦保安系統，如防火牆、防毒軟件、電腦操作系統。一些已過時的電腦系統亦因欠缺更新，存在大量已被公開披露的系統安全漏洞，企業及公眾亦應避免繼續使用。

最後是欠缺威脅偵測機制，例如保安資訊和事件管理（SIEM）系統及端點偵測和回應（EDR）解決方案。一旦攻擊者成功入侵受害機構的電腦系統而未被發現，攻擊者就可以潛伏於系統之中進行廣泛的偵察、尋找敏感及機密資料或關閉網絡保安控制，直至時機成熟就會進行最後的攻擊，例如執行勒索軟體加密系統資料以換取贖金。當遏制資料外洩事故的時間愈長，修復其破壞的成本愈高。因此，企業必須部署強大的威脅偵測機制，以縮短攻擊者潛伏時間並減輕對機構的潛在損害。

警方年測9萬重要網絡資產 揭5%存安全漏洞

香港文匯報訊（記者 蕭景源）警方網罪科首份網絡安全報告，涵蓋全球以及香港2024年的網絡安全形勢，報告重點分析香港重要基礎設施面對的網絡安全風險。去年網罪科檢測超過9萬個重要基礎設施的網絡資產，發現約5%存在不同程度的系統安全漏洞和弱點，當中11%屬於極高及高風險，一旦被攻擊者利用，極可能嚴重影響重要基礎設施的正常運作。警方遂對今年網絡威脅作出七項預測，包括人工智能網絡威脅及系統安全風險上升，以及針對重要基礎設施的攻擊陸續湧現，警方網罪科將繼續透過主動措施，強化網絡安全防禦能力，提高公眾及業界的網絡安全意識。

網絡安全及科技罪案調查科總警司林焯豪在接受香港文匯報訪問時表示，面對全球網絡安全威脅持續上升，去年全球因網絡犯罪而導致全年經濟損失估計高達9.5兆美元，預料今年更可能高達10.5兆美元。

警利用自動化技術應對黑客

香港亦未能置身事外，去年警方共錄得33,903宗科技罪案，當中包括網上騙案及其他具破壞性的網絡攻擊。然而，香港所面對的網絡威脅不只科技罪案，去年網罪科處理超過2,500萬項網絡威脅情報，即平均每日處理超過6.8萬項情報，2,500萬項中又有超過44萬項情報是針對香港，當中涉及黑客利用人工智機（AI）技術自動掃描可能存在的安全漏洞或發起攻擊，警方也利用自動化技術應對。

網絡安全報告整合威脅者的幾種網絡攻擊形式及手法，包括：透過網絡滲透活動竊取敏感資料；透過供應鏈漏洞大規模入侵系統；利用人工智能提升網絡攻擊的破壞；利用社交工程手段騙取個人資料及內部系統登入資料；以及使用勒索軟件加密數據以索取贖金牟利。警方強調對香港重要基礎設施的網絡資產風險評估，是防範性措施。

系統弱點中11%屬極高及高風險

網罪科高級警司梁靄琳分析，去年網罪科檢測超過9萬個重要基礎設施的網絡資產，包括URLs、域名及IP地址等，約5%存在不同程度的系統安全漏洞和弱點，當中近九成被歸類為中低風險，11%屬於極高及高風險，第一類是企業員工的系統登入資料外洩或被盜用，令攻擊者可藉此輕易入侵關鍵電腦系統；第二類是企業未做好域名管理，讓攻擊者可盜用閒置的子域名，構建像真度極高的釣魚或詐騙網站；第三類是企業雲端儲存服務配置不當，令設置雲端服務的內部系統意外被公開，假如企業未有做好網絡安全措施，如多重認證、登入白名單，會非常容易被黑客入侵。

警方即時通報 及時採補救措施

梁靄琳表示，這些高風險漏洞一旦被攻擊者利用，將極可能嚴重影響重要基礎設施的正常運作，但透過警方即時通報，所有重要基礎設施已及時採取補救措施。為提高香港整體網絡防禦能力，網罪科採取多項主動措施，包括轄下網絡安全中心全年24小時無間斷運作，除了收集網絡威脅情報及發出網絡安全警示，亦會監察重要基礎設施系統的正常運作及全天候提供不同等級的網絡防禦及行動支援。

其次，她指去年成立名為「網絡安全行動中心聯盟」(SOCA)的核心網絡威脅情報交流平台，通過分析來自各個來源的情報，深入了解針對香港的網絡安全威脅，並適時發出預警及應對。

另外，網罪科會為重要基礎設施定期進行「網絡資產安全評估」(IFAA)，及早洞悉及修補潛在的系統安全漏洞。網罪科亦積極參與關鍵基礎設施網絡安全相關立法工作，包括今年3月19日通過保護關鍵基礎設施(電腦系統)條例草案。

警方已邀請多位專家，在報告中總結出七個對網絡威脅的預測（**見表**），建立全面的網絡安全策略並採取主動防禦措施。網罪科亦會透過網絡防禦機制進行適時通報及攔截，引領網絡安全生態發展，與持份者共築網絡安全防線。

7賊謀爆竊珠寶店 遇警埋伏一網打盡

香港文匯報訊（記者 蕭景源）螳螂捕蟬，黃雀在後。一個爆竊團夥，昨日清晨圖向馬鞍山新港城中心商場二樓一間珠寶店埋手，詎料警方早已收到風聲布下天羅地網。在他們趁珠寶店開門營業前準備落手時，迅將合共7名疑犯一網成擒，當場檢獲一批爆竊工具及兩輛用作犯案的私家車，被捕疑犯包括一名年僅19歲青年和一名外籍人士，警方正追查眾人背景以及過往是否干犯同類罪行。

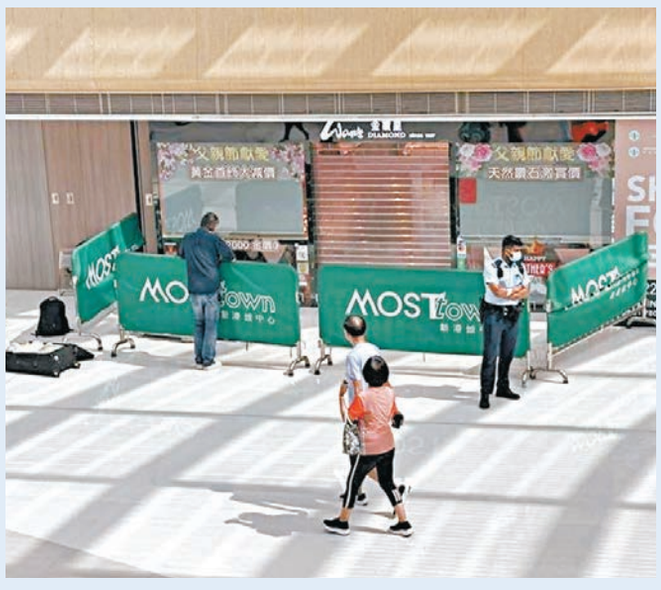
被捕者最細19歲

昨日清晨約5時，七人駕乘兩輛私家車到達上址商場附近後，分頭準備落手爆竊之際，埋伏監視及跟蹤的探員認為時機成熟，一聲令下採取拘捕行動。先在商場外截停並拘捕4名涉案男子，其後再截停兩輛涉案私家車，以及拘捕多3名涉案男子。

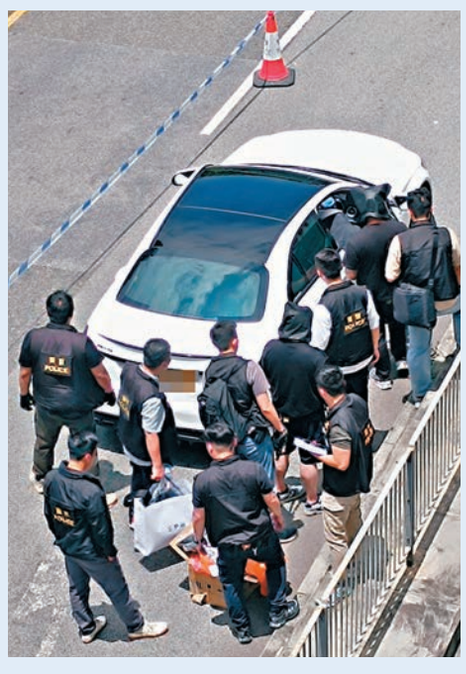
據悉，被捕的7名男子中，6人（19歲至44歲）是本地人，另一人是41歲外籍人士，所有被捕人涉嫌企圖爆竊被扣查。行動中，探員在他們身上檢獲一批爆竊工具，包括一把石屎釘槍、一把木槌及三支螺絲批，另在涉案兩輛私家車內則檢獲熔金爐、電子磅及手套。案件現由新界南總區重案組繼續跟進。

由網上圖片可見，大批探員在商場外的鞍祿街截停涉案兩輛私家車搜證，其中兩名被捕歹徒則被黑布蒙頭在一輛涉案的寶馬房車旁協助搜查。至於案中成為爆竊目標的珠寶店在警方採取行動後，一度被圍封及有警員在場駐守，該珠寶店並無任何損失。

其後，警方安排拖車將兩輛涉案私家車拖走繼續扣查，而涉事珠寶店亦解封如常營業。



●成為爆竊目標的珠寶店一度被圍封及有警員在場駐守。 網上圖片



●其中兩名歹徒被黑布蒙頭協助搜查涉案車輛。 網上圖片