黑客網釣攻擊 呃公司8000萬元

扮生意夥伴寄電郵誘過數 科技罪案首10個月1.3萬宗涉款24億

受疫情影響，企業經營及個人生活「網絡化」成為新常態，科技罪案亦隨之急升。今年首10個月香港警方已錄得逾1.3萬宗案件，損失金額高達24億港元，中小企更成為「重災區」，有公司被黑客入侵騙取千萬美元，也有公司電腦被盜用作加密貨幣「挖礦」，有家庭電腦網絡攝影機（webcam）被控制而私隱盡露，再被迂迴入侵公司電腦行騙。警方網絡安全及科技罪案調查科聯同國際刑警及互聯網業界，展開代號「碩將行動」，移除數以千計殭屍電腦伺服器及釣魚網站，以淨化本港網絡，並廣傳網絡安全貼士，提升企業和個人應對網絡威脅及防禦網絡攻擊的能力。

●香港文匯報記者 蕭景源

警方網絡安全及科技罪案調查科高級警司林焯豪昨日表示，2020年全球因為網絡犯罪造成的經濟損失高達1萬億美元，預計今年相關損失金額將會增加15%，至2025年損失更有可能高達10.5萬億美元。今年首10個月，香港電腦保安事故協調中心共接獲6,457宗網絡安全事故報告，同期警方亦錄得13,163宗科技罪案，包括11,349宗網上騙案、1,041宗網上勒索案及117宗不當使用電腦等，損失合共約24億港元，較去年同期上升24%。

3個月揪出殭屍電腦2486部

其中損失最大一宗案件，為一間內地公司誤中網絡釣魚攻擊後，於今年5月下旬收到黑客假扮其生意合作夥伴的電郵，要求過數1,000萬美元（近8,000萬港元）貨款，職員不虞有詐過數，其後始知受騙報案。

今年9月至11月，網罪科與國際刑警、網絡安全公司及互聯網服務供應商協作，分別進行數據分析及情報交流，並收集約200萬項與網絡安全有關的情報及數據，進行研究、整合及全面分析，搜尋網上黑客攻擊蹤跡。網罪科經130次實地檢查，發現15個具備指揮及控制功能的殭屍電腦伺服器（C2 Servers）、2,486部已被操控的殭屍電腦設備（Bots）及1,075個釣魚網站（Phishing Websites），其中釣魚網站涉及674宗案件，損失合共約7.8億港元。

同時，警方共發現12萬部有潛在漏洞的裝置（Vulnerable devices），已修正大量有潛在風險及漏洞的裝置，並聯絡230間互聯網服務供應商協助通知裝置有潛在漏洞的用戶，提供一系列安全建議，適時進行系統更新或重新設置。

警方又發現不法分子透過惡意程式入侵電腦，進行秘密挖掘加密貨幣的挾持事件急升，有研究顯示2021年全球涉及加密貨幣的挾持事件，較去年上升4倍，其中企業高性能電腦系統成為目標。警方發現有私人機構的網頁伺服器被植入惡意挖礦程式，秘密挖礦長達3個月。這類惡意程式，可以導致受害人公司電腦效能下降，增加電力成本，嚴重可拖垮全公司資訊科技系統。

●警方網絡安全及科技罪案調查科展開代號「碩將行動」，移除數以千計殭屍電腦伺服器及釣魚網站，以淨化本港網絡。 香港文匯報記者 攝

林焯豪強調，警方主要目的是想取締一些殭屍網絡及相關潛在網絡安全漏洞的裝置，為香港提供一個更加安全及潔淨的網絡環境。

「智能家居」恐成網安漏洞

香港文匯報訊（記者 蕭景源）物聯網（Internet of Things，簡稱IoT），是用互聯網龐大網絡結合數以千計電腦裝置及智能裝置，即是將所有東西都連入網絡；近年普及的智能家居，因把家電及家居連入網絡，成為物聯網的一個應用場景。惟很多家居智能電器等裝置，由於設計時未有考慮網絡安全問題，容易成為網絡保安漏洞。

今年首三季，有電腦安全公司偵測到本港網址（IP Address）遭千萬次惡意攻擊，而網罪科在「碩將行動」發現2,486部已被操控的殭屍電腦設備中，發現有網絡攝影機鏡頭、網絡儲存裝置、家用路由器、溫度監測儀、影印機等智能裝置被黑客攻擊，受害人可能被盜取個人及銀行賬戶等重要資料，家中私隱也會被公開，但黑客入侵家居的最終目標是，利用所控制的裝置作橋樑，攻擊有關連的公司、機構及政府部門等，然後進行網上勒索或網上騙案。

此外，市民的智能電話其實也是一部流動電子通訊裝置，電話內有電子銀包、公司、他人及個人等重要資料，其實都有被黑客攻擊的風險，一旦遭入侵導致資料外洩，同樣可造成「火燒連環船」的巨大損失。網絡安全專家呼籲市民，不要隨便下載可疑軟件或登入可疑連結，並定時提升及更新防毒軟件，如果發現電腦效能突然變得緩慢、智能電話無故發熱或停用時耗電量仍很快，便要提高警覺。

「守網者」網頁揪出釣魚電郵

警方在網上設置「守網者」一站式平台，為網民提供全面網絡安全、資訊保安及科技罪案防罪資訊，並有連接網絡安全公司工具讓市民免費進行一次防毒更新，以測試個人電腦有否中病毒及檢查裝置保安強弱程度，更嶄新推出「釣魚詐騙搜尋器」，提供市民搜查可疑釣魚網站及電郵，減低受騙風險，令市民成為醒目數碼公民；「守網者」網址https://cyberdefender.hk/。

網絡安全貼士

家用路由器(router)

- 更改路由器的出廠賬戶密碼
- 關閉所有不常用或不必要服務
- 留意所用產品相關保安警告
- 不要安裝開放源碼組織所提供的韌體(firmware)
- 定期更新路由器韌體(firmware)
- 應使用有生產商提供支援服務的型號

網絡攝影機(webcam)

- 透過官方渠道購買網絡攝影機
- 更改出廠預設密碼
- 密碼應定期更改並符合複雜要求
- 切勿在公共網絡中連接網絡攝影機
- 僅從官方應用商店下載相關手機應用程式
- 定期檢查網絡攝影機的設定
- 切勿將網絡攝影機設置在私人或敏感區域
- 更新韌體(firmware)至最新版本
- 無論使用任何連接方式，都應啓用認證功能
- 不使用時關閉網絡攝影機
- 應使用有生產商提供支援服務的型號
- 留意所用產品的相關保安警告

網絡儲存裝置(NAS)

- 如有需要經互聯網存取裝置，請使用虛擬私人網路
- 修改預設的管理員密碼或建立一個新的管理員賬戶
- 不要安裝或開啓不必要的附加功能
- 定期進行檔案備份
- 保持設備的系統更新
- 留意所用產品的相關保安警告
- 應使用有生產商提供支援服務的型號

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