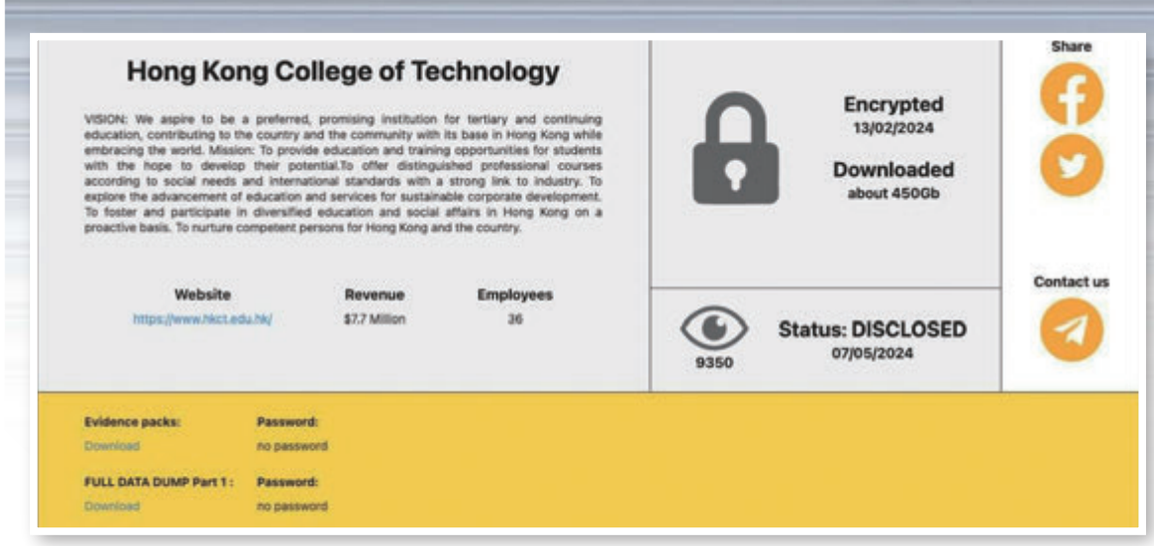
港專約450GB涉學生資料檔案被公開 六福被威脅放售500萬名會員資料

港專六福同遭黑客毒手 釀私隱災難

網絡黑客近期頻密向香港的公私機構發起攻擊，通過網絡入侵盜取個人資料，部分勒索不遂後公開撕票，將成千上萬市民資料在「暗網」拍賣，釀私隱「災難」。近日，香港專業進修學校和六福珠寶遭黑客毒手，港專約450GB檔案遭放上暗網公開，已有近萬人曾查閱資料；有黑客在網上揚言有500萬位六福會員資料出售。兩間機構均已報警和通報私隱專員公署，警方網絡安全及科技罪案調查科接手調查。

◆香港文匯報記者 蕭景源



▲港專約450GB檔案遭放上暗網公開。

►六福集團昨日發表公告，指尚未能確定集團的客戶紀錄是否有任何外洩。 香港文匯報記者鄧偉明 攝

有黑客日前在Telegram發帖聲稱，有500萬位六福的會員資料在「暗網」出售，售價2.5萬泰特幣（約19.5萬港元）。據了解，外洩的資料包括會員的姓名、出生日期、住址、身份證號碼、電郵、賬戶密碼、手機號碼和微信賬號，包括內地和本地客戶的個人資料，懷疑有黑客入侵六福珠寶電腦網絡系統。

六福集團昨日發表公告，形容事件為「潛在數據安全事件」，又披露約在2024年5月7日前後，集團發現一篇由威脅行為者在流行的「暗網」（即地下論壇）上發布的網帖，聲稱能夠訪問集團的客戶紀錄，並邀請對此類紀錄的訪問進行競標。

六福：未確定客戶紀錄是否外洩

公告表示，在發現潛在事件後，集團立即採取行動查明情況，已在一家領先的網絡安全顧問公司的協助下展開徹底調查，包括評估潛在事件的真確性和根本原因，以及全面審查集團系統和伺服器的安全性。調查仍在進行中，尚未能確定集團的客戶紀錄是否有任何外洩，以及其洩露的程度。待調查完成後，該集團會根據有關結果採取適當的進一步行動。

公告表示，集團已向香港警務處及個人資料私隱專員公署報告這宗潛在事件，並將協助調查。該集團將繼續加強資訊系統安全措施，致力保護客戶的資料和私隱，以防日後發生同類事件。

香港專業進修學校前日公布，今年2月下旬遭高階持續性黑客勒索軟件攻擊，資訊科技網絡和檔案伺服器被非法入侵，部分文件檔案被盜取和加密，或涉部分學校文件或個人資料外洩。

校方表示在得悉事件後，立即採取相應行動，包括報警和主動向個人資料私隱專員公署備案，關閉受影響電腦設備，並在獨立網絡安全專家協助下展開詳細檢視及調查，深入掃除隱患，以及積極配合警方進行調查。

港專發言人譴責任何網絡犯罪行為，強調是次攻擊並非一般性，而是極具針對性和不尋常的網絡攻擊，又對事件造成的不便和困擾深表歉意。校方將為所有受影響者提供為期半年免費「信貸監察服務」和「暗網監控服務」，以加強保護個人資料。

據了解，港專被盜去450GB資料，涉及8,100名學生，包括姓名、身份證號碼、地址等個人資料。根據暗網資料，黑客是在今年2月13日入侵港專電腦系統，盜取相關資料後加密行勒索，因未能取得贖金，於本月7日公開資料。

教育局敦促港專全面調查

特區政府教育局表示，十分關注港專遭黑客入侵，已敦促校方全面調查事件和審視資訊系統保安措施，並按風險為本原則，採取適當措施加強網絡安全，避免同類事件發生，並要求港專完成有關調查後提交報告。

近期黑客網絡攻擊和網絡漏洞洩資料

公布時間	涉事機構	事件經過
2024年5月3日	特區政府公司註冊處	110,000人個人資料外洩，包括姓名、完整護照號碼、完整身份證號碼、通常住址、電話號碼和電郵。處方指承辦商在設計系統時，除了提供查冊相關資料，還將額外個人資料傳輸到客戶端電腦。 查冊者在查冊結果頁面上利用開發者工具（Web developer tool）就會取得額外個人資料，或透過編寫程式（robotic search）查閱資料，或以電子方式提交持牌放債人委任第三方的通知書時，也會出現同樣情況。公司註冊處向當事人致歉。
2024年3月18日	南華體育會	電腦伺服器於2024年3月17日疑遭黑客入侵，個人資料私隱專員公署收到南華體育會的資料外洩事故通報，可能有約70,000人受影響。 由於事故可能涉及個人資料外洩，包括姓名、香港身份證號碼、護照號碼、地址、電郵地址、電話號碼、出生日期和相片，私隱公署建議相關機構盡快通知受影響者，並根據既定程序就事件展開調查。
2023年9月	香港消費者委員會	黑客組織ALPHV獲取並利用消委會一個具管理員權限的賬戶，透過虛擬私有網絡（VPN）進入消委會的網絡。有450人資料外洩。 私隱公署調查發現，消委會5大缺失，包括沒有遠端存取資料啓用多重認證功能、沒有妥善設定用作偵測及攔截網絡安全威脅的網絡安全軟件、欠缺足夠保安措施禁止或防止於測試伺服器內儲存個人資料、資訊保安政策有欠全面及具體、保障個人資料私隱及網絡安全意識不足
2023年8月	數碼港	遭黑客入侵盜取400GB資料，勒索不果後將資料在暗網公開拍賣，共有13,632人受影響，包括近8,000名與僱傭相關人士，其中5,292名求職者和離職者資料保留超過期限，其他受影響者包括數碼港管理人員、酒店職員、實習生、相關業務人士等。外洩的資料包括身份證號碼、銀行戶口號碼、信用卡資料等。 私隱公署指出數碼港5大缺失，包括資訊系統欠缺有效偵測措施、沒有為遠端存取資料啓用多重認證功能、資訊系統保安審計不足、資訊保安政策欠具體，沒有網絡保安框架供員工依循、不必要地保留個人資料

整理：香港文匯報記者 蕭景源

網安情報系統揭攻擊主要來自越南美國荷蘭

香港文匯報訊（記者 蕭景源）網絡黑客攻擊日益猖獗，由居家到企業無孔不入。香港警方與私人機構聯手研發名為「HoneyNet」的「威脅預警及捕獵網絡」，是全球首例由公私合作開發的網絡安全情報系統。「HoneyNet」曾在2021年12月至2022年11月進行測試，其間共記錄1.35億次網絡威脅情報，約17.5萬次為惡意程式攻擊。系統分析數據顯示，黑客攻擊主要來自越南、美國和荷蘭等地。

助警尋「殭屍電腦」IP地址

該套「獵黑客」系統為一個跨機構的網絡安全情報共享系統，可實時收集針對香港不同機構的網絡威脅數據，並透過人工智能和大數據處理技術作出分析，以深入了解網絡威脅的手法和源頭。該系統要利用數據才能加強網絡保護，就好像「引蜜蜂」科技，要先發現黑客入侵，才能提高威脅預警和捕獵網絡黑客。

該系統不但可助警方找出「殭屍電腦」的IP地址進行淨化來源行動，更可為特區政府有關電腦安全資訊提供發放資料平台提早作出防禦，及將攻擊數據給資訊安全公司，以增強防毒軟件能力。只要使用者經常更新防毒軟件，就能防範黑客入侵。

「HoneyNet」最初有6個「HoneyPot」測試點，警方希望能有更多機構包括學校、中小型企業、大型企業和網絡營運商參與，使收集數據更龐大，截擊網絡攻擊更加全面。

議員倡引入強制性資料外洩通報

香港文匯報訊（記者 蕭景源）立法會資訊科技及廣播事務委員會主席葛珮帆昨日在接受香港文匯報查詢時，表示對事件感到震驚，認為大量個人敏感資料外洩，一旦遭盜用後果嚴重。近日個人資料外洩事故頻繁，除反映社會整體對網絡安全意識不足外，亦反映《個人資料（私隱）條例》猶如「無牙老虎」，以致部分機構對網絡安全和保障個人私隱掉以輕心，故有必要提升社會整體的網絡及資訊安全意識。

葛珮帆建議特區政府盡快修訂《個人資料（私隱）條例》，引入強制性資料外洩通報，加重罰則，以及加入行政罰款機制，以達阻嚇作用，如政府部門或公營機構出現個人資料外洩事故，有關部門或機構的首長及資訊科技項目主管必須問責。

同時，特區政府應在所有資訊科技項目中引入「隱私數據評估和審計」，及未來「數字政策辦公室」須密切監察網絡攻擊的趨勢和保安威脅，適時發出警報通知，並提高各政府部門網絡及資訊安全的即時應變能力和防範意識。

她又建議加強香港網絡及資訊安全的教育和推廣工作，以提高社會整體網絡及資訊安全的意識。私人機構應評估所收集的個人資料是否必要，避免收集過多個人資料，及時刪除不必要的個人資料。同時，市民應謹慎提供個人資料，了解機構保留其資料的期限和相關安全措施。

對於有機構可能因擔心損害聲譽，而未有主動公布資料外洩事故，她認為此舉對當事人不公道，因為有關機構未必可以通知全部當事人，因此應該盡快對外公布，讓可能受影響者提高警覺。

專家之言：應定期做網絡安全檢查

電腦安全研究員賴灼東昨日接受傳媒查詢時表示，根據公開資料，雖然香港暫時並非十大網絡攻擊對象，但近年不時出現勒索攻擊，連具有標誌性的機構數碼港也遭入侵，估計會讓黑客留意到香港存在網絡安全風險，香港「已經到了一個階段不止金融行業，只要有個人資料、付款資料或會員資料，這些系統都必須保護」。

賴灼東認為，黑客攻擊手法始終如一，當發現有漏洞便會入侵，竊取資料勒索，因此企業切勿心存僥倖，建議做好保安監察，利用軟件監察系統異常狀況，強調系統的安全設置非常重要，需要有專業人員持續更新、測試和監察系統。

他指出，坊間的防火牆已經相當成熟，可有效偵察和攔截多次嘗試登入資料庫的活動，黑客可以隨時入侵系統反映情況嚴重，故建議大型商場或零售業店舖等所有涉及儲存個人資料、登記會員或儲積分的網站和程式，都要定期做網絡安全檢查。

有網絡安全專家表示，網絡安全是一場永不休止的「攻防戰」，因防禦技術提升時，黑客入侵技術也在提高，甚至往往「易攻難守」，故網絡安全必須引起全社會重視，可能有機構覺得花巨資提升網絡保安後，一直沒有遭到攻擊；或者在提升網絡保安後仍不能百分百保證安全，故對投資網絡安全不夠重視，但始終不能心存僥倖，一旦中招，招致的損失難似估量。

◆香港文匯報記者 蕭景源

黑客五類常用網絡攻擊「武器」

1.木馬程式
◆其偽裝成正常軟件並下載到電腦中，試圖竊取使用者的敏感數據並可以從後門侵入系統

2.掘礦軟件
◆竊取電腦的部分算力，妨礙系統正常運作

3.網絡掃描工具
◆搜查指定IP地址和開放端口

4.清除日誌軟件
◆清除日誌使電腦管理員難以追查黑客行蹤

5.密碼爆破工具
◆以不同方法進行密碼爆破攻擊

資料來源：網絡安全及科技罪案調查科
整理：香港文匯報記者 蕭景源