八達通系統遭攻擊 共涉約3萬客戶商戶資料

香港文匯報訊（記者 蕭景源）續有企業和機構網絡系統遭受非法入侵外洩資料。八達通卡有限公司公布，昨晨偵測到系統受到網絡攻擊，事件涉及約7,500名客戶的個人資料，包括姓名及相片，其中部分資料亦可能涉及自動增值服務資料，包括銀行編號及自動增值金額，但不涉信用卡或銀行戶口資料。此外，約22,000名商戶的一般資料同受影響，包括公司聯絡人姓名、職位、電郵地址及電話號碼。八達通現正全面調查事件，已通知有關部門，會因應調查進展適時更新有關評估。

八達通主要服務運作如常，客戶可如常使用八達通卡、手機八達通及八達通銀包。截至目前，八達通未發現有客戶蒙受財務損失，卡內及錢包內的餘額亦繼續受到嚴格保障。因應已採取的預防措施，有少數功能或會暫時受到影響。八達通提醒客戶提高警覺，留意戶口有否出現異常活動，並提防可疑來電、短訊、電郵或連結。八達通已特設查詢熱線，解答疑問並提供支援。

「康體通」及AEON信貸財務同失守

同日，康文署公布，11月26日接獲外判承辦商通報，供市民預訂康文署轄下康體設施及參加康樂活動的「SmartPLAY康體通」「重新啟動Leisure Link賬戶」功能被黑客非法進入，涉及約9萬名Leisure Link賬戶的個人資料，包括出生日期、電話號碼、地址、性別及電郵地址，以及其中約1,500名用戶的姓名。是次事件不涉身份證明文件的資料，SmartPLAY沒有儲存任何信用卡或其他付款的資料。SmartPLAY已取消「重新啟動Leisure Link賬戶」功能，並將全面移除當中的資料。

SmartPLAY的「忘記用戶編號或密碼」功能亦被黑客非法使用，以致系統向被觸及的用戶發出載有驗證碼的電郵，事件不涉個人資料。用戶如沒有使用此功能而收到由系統發出的電郵驗證碼，請不要理會，如因忘記密碼而需要更改密碼，可攜帶香港身份證到設有「智能自助服務站（3S）」的康樂場地或區內康樂事務辦事處辦理。

SmartPLAY已停止「忘記用戶編號或密碼」功能，功能恢復後會另作公布。承辦商已即時採取措施防止黑客，確認系統可繼續正常運作。康文署已向警方報案，同時向保安局、數字政策辦公室及個人資料私隱專員公署通報。由於過去數天黑客接連非法進入康文署轄下的URBTIX及SmartPLAY資訊系統，康文署會請警方檢視是否涉及嚴重的不法行為。

另一方面，AEON信貸財務（亞洲）有限公司發出自願性公告指，11月18日發現若干面向客戶的系統出現異常回應延遲及逾時情況。其後識別到未經授權存取其後端系統的情況，已限制所有進一步未經授權存取，並加強公司系統安全控制措施，已委聘獨立第三方專家協助調查事件，並就進一步的遏止及補救措施提供建議。

該公司已通報個人資料私隱專員公署及警方，並已採取多項措施，包括通知可能受該事件影響的客戶、調整信用卡交易限額、更換可能受影響的信用卡、加強交易授權機制及監控，以及優化欺詐偵測等措施等。



●八達通卡有限公司公布，昨晨偵測到系統受到網絡攻擊。圖為市民使用八達通卡乘搭港鐵。 資料圖片

兩月處理30宗網安事故 當中11宗涉應用程式界面漏洞

警揭黑客藉機構漏洞取「密鑰」盜資料

香港近月頻密爆發網絡安全和資料外洩事故，不同行業都成為黑客目標。警方由今年10月1日至11月26日已處理30宗網絡安全事故，有11宗涉及應用程式界面（API）漏洞，揭露涉事機構將API密鑰直接編寫到手機應用程式或網頁原始碼內，黑客破解程式碼便輕易取得API「鑰匙」，藉此越權存取系統內客戶資料，換言之API失守，機構資料庫也會失守。另外，黑客利用人工智能掃描系統漏洞，令攻擊速度加快，本月有連鎖零售店網站及應用程式遭入侵，短時間被盜取過百萬項客戶資料，而騙徒可利用資料進行「精準詐騙」。警方呼籲企業加強網絡系統保安和監察。

●香港文匯報記者 曾立本



●警方聯同持份者呼籲企業及市民做好網絡安全措施。 香港文匯報記者曾立本 攝

近兩個月，香港警方共處理30宗網絡安全事故，包括14宗勒索軟件和16宗黑客入侵事故，尤以零售業錄得7宗佔最多。在16宗黑客入侵事故中，有11宗涉及應用程式界面漏洞，包括9宗手機應用程式及兩宗網站入侵。

AI加劇保安漏洞風險

網絡安全及科技罪案調查科警司許綺惠昨日表示，現時市民無論在購物、日常事務甚至預訂行程等，會使用網上服務及向不同機構提交個人資料。換言之，本港不同機構都會保存市民的數據，包括個人資料或交易詳情，而市民日常到網站或用手機App進行一些交易或查閱資料時，背後是依靠API到資料庫。

由於API是直通資料庫的鎖匙、橋樑，一旦API失守，企業的資料庫也會失守，客戶的資料同樣失守。許綺惠指出，企業API出事的原因，是將API密鑰直接編寫在手機App或網頁的原始碼；黑客只需破解App原始碼，便可以取得API密鑰，就可看到資料庫背後儲存的客戶數據格式，若系統沒有再次核對使用者身份，黑客便可直接在查詢指令內不斷改動編號，短時間內取走大批客戶信息。

企業API密鑰有很多漏洞，包括正常測試系統後沒有離線或企業本身防火牆保安措施設定鬆散等，而人工智能加劇了保安漏洞的風險，許綺惠表示，一旦黑客用自動化工具代替以往人手進行改動編號，便可以短時間內取得大批資料。以本月發生的一宗個案為例，有機構被黑客在短時間入侵取得逾百萬名客戶個人資料。騙徒在取得客戶資料後，包括姓名、電話號碼、購物紀錄、送貨地址等的資料，便能很有說服力地進行精準詐騙，如根據訂單資料假冒客服，訛稱貨品出現問題提出理賠，誘使市民提供銀行資料、驗證碼或轉賬等。

建議機構採取「零信任」安全原則

根據香港警方數據顯示，今年首10個月，全球接獲共約3,310萬宗網絡威脅情報，按年升14.6%；其中約148萬宗屬針對本港的網絡威脅情報，按年增約24%，當中針對香港的網絡偵測及惡意軟件情報數量分別大幅上升252.8%及616.1%。許綺惠表示，網絡偵測是不法分子在網絡攻擊前的「踩線」活動，以收集網絡上系統資料，包括系統有什麼漏洞，目的是為後續的攻擊鋪路，同一時間，黑客也可以利用惡意軟件突破防線，直接在系統偷取數據。由於網絡犯罪分子利用AI將網絡偵測或編寫惡意軟件自動化，大幅加快攻擊的速度；近期全球發生一些非常矚目的網絡攻擊事故。

許綺惠表示，機構的測試系統未妥善處置或防火牆規則不足，同樣會引致網絡安全事故，即使機構將IT服務外判，但企業在保障客戶資料上責無旁貸，建議機構採取「零信任」安全原則，存取要求時均要核實身份及權限；市民切勿盡信來電，應立即收線並向官方核實；切勿透露銀行密碼、驗證碼或點擊不確定連結；更改涉事及重用密碼、啟用雙重認證；留意銀行交易、設定轉賬或交易金額上限；善用「防騙視伏器」、「防騙視伏App」或致電防騙易18222。

網絡安全保護措施及防騙貼士

機構：
一）全面保護系統和API
1）盤點系統及資料
掌握有哪些系統，包括API、誰負責、處理什麼資料等
2）保護敏感資料
按照資料敏感程度及風險採取適當保護措施，包括為儲存中及傳輸中的敏感資料進行加密
3）最小權限
管好權限、核實身份、限速及監控，只讓必要的人和系統存取，並定期檢視
4）更新及測試
不用即離線、數據脫敏、及時修補漏洞，並定期做保安測試
5）持續監察
留意異常存取及大量下載，及早發現問題
6）減少資料
只收集及保存所需資料，萬一外洩影響較小
7）防火牆
加強保安，登入失敗即鎖、限制嘗試次數、自動封鎖
二）處理網絡安全事故步驟
1）即時遏止
暫停受影響的相關系統、API及賬戶，阻止資料繼續外流
2）評估影響
確認外洩的資料類別、數量及受影響人士，並保留紀錄
3）專業服務支援
HKCERT網絡安全方案「一站式」平台——「網絡安全服務供應商聯動計劃」
4）通報及溝通
通知私隱專員公署及受影響人士
市民防騙貼士：
1）切勿盡信來電，立即收線並向官方核實
2）切勿透露銀行密碼、驗證碼或點擊不明連結
3）更改涉事賬戶及重用的密碼，並啟用雙重認證
4）密切留意銀行交易紀錄，設定轉賬及交易金額上限
5）善用「防騙視伏器」或致電18222求助

資料來源：警務處、香港網絡安全事故協調中心
整理：香港文匯報記者 曾立本

資料外洩頻發 民記倡立法會下周緊急討論

香港文匯報訊（記者 蕭景源）香港近期接連發生網絡個人資料外洩事故，涵蓋航空、醫療、零售、大專院校及城市售票網相關系統，涉及旅遊證件、信用卡及醫療紀錄等極度敏感資料，引起社會高度關注。民建聯主席、立法會保安事務委員會委員陳克勤昨日致函保安事務委員會主席，建議於12月1日會議上臨時加入緊急議程，討論「加強網絡安全防禦及遏止大型資料外洩引發的詐騙風險」。

冀政府交代遏「二次詐騙」部署

陳克勤表示，過去兩個月內，香港連續發生接近20宗網絡資料外洩事故，受影響人次高達300多萬。涉事機構及外判承辦商在事故後未見全面堵塞保安漏洞，令大量市民資料仍暴露於極高風險之中，隨時被不法分子用作精準行騙，引發連鎖網絡詐騙及「二次詐騙」，對市民財產安全構成即時威脅。他期望特區政府在12月1日的會議上，清楚交代最新執法及調查進展、遏止「二次詐騙」的即時部署，以及協助公私營機構全面排查保安漏洞的緊急應變措施，以維護本港網絡安全及保障公眾利益。

民建聯副主席、香港執業律師、立法會議員周浩鼎表示，在要求執法部門盡快交代連串事故的調查進展的同時，他建議政府檢視《個人資料（私隱）條例》，從制度層面堵塞漏洞，例如，香港社會各界均關注研究引入「強制性資料外洩通報機制」及現有《私隱條例》並未直接規管外判商等「資料處理者」的情況，政府應交代將如何修改法例，以及稍後處理的時間表，以助增強法例阻嚇力，同時有效督促公私營機構及外判商切實履行保護個人資料的責任。

私隱署今年接330宗外洩通報 近半涉黑客入侵

香港文匯報訊（記者 蕭景源）香港私隱專員公署2025年共接獲246宗資料外洩事故通報，較2024年增加21%。今年截至11月25日，公署已接獲330宗資料外洩事故通報，較去年同期223宗增加近五成，其中涉及黑客入侵的資料外洩事故通報有156宗，佔整體資料外洩事故通報47%，較去年同期75宗上升超過一倍。在今年330宗資料外洩事故通報中，有113宗是在10月後接獲，佔整體34%，反映近期資料外洩事故加劇。

私隱專員公署高級個人資料主任（合規及查詢）文靄怡表示，資料外洩事故除可能影響資料當事人及導致造成損害外，同時會令機構聲譽受損，若機構未有採取足夠安全措施保障持有的個人資料而導致資料外洩，更有可能違反私隱條例的資料保障原則。

籲加強第三方服務供應商管理

她強調，外判資料處理不等於外判資料保障的責任，如果機構聘請第三方處理個人資料，需要採取合約規範或其他方法，以確保轉移的個人資料安全。

倘發生資料外洩事故，機構應該立即收集重要資料，包括事發時間、地點、涉及系統、受影響個人資料種類和範圍等，並即時採取控制措施，遏止事件擴大，例如隔離被入侵系統、重設賬戶、修補保安漏洞等，同時評估事件可能造成的風險，盡快向受影響的資料當事人和公署通報，完整記錄事故的經過，從中汲取教訓改善處理個人資料做法。公署在接獲通報後，會向機構提供協助和建議，以減低外洩事故的損害。

文靄怡提醒機構各方要提高網絡安全意識，適時採取對資料的保安措施，包括定期進行保安漏洞評估和滲透測試，並加強第三方服務供應商的管理，聘用前作準則審查，合約訂明保安和資料外洩事故通報要求，並定期監察和審核是否履行相關責任。此外，機構應制定資料外洩事故應變計劃，確保一旦發生事故時可以迅速處理和通報。公署亦提醒市民，如果收到不明來歷或可疑的來電、短訊、電郵等，要提高警覺，不要開啟、點擊連結或披露個人資料。