間諜釣魚電郵對華竊密高發

國家安全部：黨政機關網絡成主渠道 軍工企業市政府部門曾受騙

一家郵件系統廠家的運維人員小李，因為貪圖便利經常在電腦上記錄甲方客戶的賬號密碼和系統管理員賬號密碼，被境外網絡間諜鎖定身份，並被竊取了電腦中的客戶賬號密碼表，導致千餘家重點要害單位因郵件系統問題洩密。這是一宗利用「釣魚」郵件實施網攻的典型案例。國家安全部17日發文指出，境外間諜情報機關將中國黨政機關、涉密單位計算機網絡作為竊密主渠道，利用「釣魚」郵件實施網絡攻擊。文章提醒，在工作生活中要時刻保持警惕，提高防範應對能力。

◆香港文匯報記者 趙一存 北京報道

當前，網絡空間已經成為境外間諜情報機關對中國開展間諜活動的重要陣地，網絡安全形勢日趨嚴峻。國家安全部的文章指出，網絡平台早已成為人們工作生活的重要工具，普遍使用的電子郵箱也成為境外間諜情報機關網絡竊密的重點目標。

偽裝官方郵件登錄界面

文章稱，境外間諜情報機關常見手法一般包括假扮官方實施欺詐、個性定制精準竊密，以及竊取賬號冒充身份。其中，假扮官方實施欺詐就是會預先搭建一個與目標電子郵箱高度相似的郵箱登錄界面，並偽裝成郵件服務商，向指定用戶發送虛假的「高風險賬戶警告信息」郵件。待目標對象點擊後，「高仿」登錄界面便會彈出，賬號密碼一旦輸入，便會被境外間諜掌握。2011年，中國某涉密軍工企業工作人員就收到一封偽裝成郵件服務商警告信息的「釣魚」郵件，受誘導點擊後導致工作郵箱賬戶密碼洩露，被竊取了大量敏感工作資料。

定制內容降低防範心理

個性定制精準竊密，即境外間諜情報機關會預先搜集、分析相關電子郵箱用戶信息，篩選出有價值的目標，並根據其關注的熱點事件、工作事項或個人事務，「定制化」設計郵件標題、內容，以降低目標對「釣魚」郵件的防範心理，誘使其下載惡意攻擊性文件，實現「精準」竊密。2019年，某市政府部門工作電子郵箱收到一封偽裝成某縣委辦發來的電子郵件，附件為「幹部年度考核審批」。工作人員出於對轄區機關單位的信任，未加核實便點擊了郵件內偽裝成附件的攻擊性文件，結果造成郵箱中的內部資料被竊。

冒充身份「黑」進社交軟件

此外，竊取賬號冒充身份，即境外間諜情報機關在盜取個人賬號後，「黑」進其電子郵箱或社交軟件，向其好友、聯繫人等發送可能感興趣的「釣魚」郵件，利用熟人「不設防」的心理，達到竊取敏感信息或誘使下載惡意攻擊性文件的目的。2020年，境外間諜情報機關就預先控制了某地黨校教授的郵箱，利用其教授身份向郵箱中的聯繫人發送主題為「某全會精神深度解析」的郵件，相關收件人點擊查看後導致多個郵箱資料被竊。

2022年中企近六成電郵涉網攻

據了解，近年來，中國遭遇境內外黑客和不法分子實施「釣魚」郵件攻擊事件呈高發態勢。據內地知名網絡安全公司奇安信發布的中國企業郵箱安全性研究報告披露，2022年中國企業郵箱用戶共收發各類電子郵件約7,660億封，其中，「釣魚」郵件佔比近六成。不僅如此，中國遭受此類攻擊事件規模愈發龐大，僅2022年上半年就發生十餘宗大型單位及職工遭攻擊事件。

另外，作為在中國經濟發展和社會運行中承擔重要環節的金融、教育、醫療、物流、能源等重點領域的大型企業，其網絡系統因存放大量中國境內用戶、商業甚至國家機密數據，已成為境內外黑客組織和不法分子「釣魚」郵件攻擊的主要目標。

「沒有網絡安全就沒有國家安全。」國家安全部提醒，在工作生活中要時刻保持警惕，提高防範應對能力。公民若發現通過網絡「釣魚」郵件進行竊密活動的可疑情況，應及時撥打12339國家安全機關舉報受理電話，或登錄互聯網舉報平台，或通過國家安全部微信公眾號舉報受理渠道，或直接向當地國家安全機關進行舉報。

◆來源：國家安全部

常見手法一覽

1.假扮官方實施欺詐

也可以叫魚叉式釣魚郵件攻擊，利用預先搭建的與目標電子郵箱高度相似的郵箱登錄界面，並偽裝成郵件服務商，以特定郵箱用戶爲目標，發送定制化郵件，誘騙其輸入賬戶密碼、點擊惡意鏈接、下載帶毒文件等，以獲取重要數據資料。

2.個性定制精準竊密

也可以叫鯨釣，攻擊者鎖定政府高官、企業高管、社會名人等具有較大社會影響力的人物，根據其關注的熱點事件、工作事項或個人事務，冒充其身份向身邊的人發送定制化郵件，以降低目標對「釣魚」郵件的防範心理。此類釣魚方式目標更廣、收效更快。

3.竊取賬號冒充身份

也可以叫商業電子郵件欺詐，攻擊者利用盜取的個人賬號「黑」進目標對象的電子郵箱或社交軟件，向其好友、聯繫人等發送「釣魚」郵件，利用熟人「不設防」的心理進行誘騙。

何謂釣魚郵件

話你知

「釣魚」郵件是一種常見的網絡攻擊手段，攻擊者通常會僞造發件人地址和郵箱賬號，誘使目標用户點擊惡意鏈接或下載惡意文件，竊取用户憑證和數據資料等敏感信息，甚至入侵控制相關終端設備。

區別於傳統意義上對網絡服務器的攻擊，「釣魚」郵件直接以人作爲攻擊對象，利用「人性」的獵奇心理和防備鬆懈等實施欺詐、誘騙行爲，這種攻擊手段無須大費周章地突破系統防火牆、入侵防禦系統、入侵檢測系統等縱深防禦措施，便可輕鬆獲取賬户資料信息或植入惡意程序。

民眾也可成目標 AI助攻更易上釣

專家解讀

內地安全專家接受香港文匯報訪問時表示，事實上不僅是黨政機關、涉密單位等特定對象會成為「釣魚」郵件實施網絡攻擊的目標，普通民眾也可能會成為被「釣」目標，比如軍事發燒友、攝影愛好者，甚至喜歡旅行的人等等，「境外間諜情報機關為了得到想要的信息無所不用其極。」亦有專家指出，當前，還須防範利用生成式AI製作的新型「釣魚」郵件，此類郵件更具欺騙性和迷惑性，較之傳統「釣魚」郵件更加難辨真偽。

軍迷成間諜案高危群體

國家安全部此前曾發文指出，軍事發燒友近年來已成為涉軍領域間諜、竊密、洩密案件的高危群體。他們出於個人喜好、吸引流量等各種目的，熱衷於搜集、整理涉軍敏感信息，或在自媒體、社交媒體賬號、各類軍事論壇發布，極易造成軍事秘密廣泛傳播。

此外，隨着大數據等前沿科技的運用推廣，地理空間信息數據被廣泛收集，有關敏感信息數據洩露的風險也隨之增加。國家安全部指出，有個別境外地圖公司利用採集地圖數據換取虛擬貨幣獎勵的方式，誘使境內人員購買並使用專用設備進行地圖「打卡」，非法採集敏感地理空間信息數據，並實時上傳至境外服務器，甚至針對特定區域開出高額獎勵，吸引「採集者」進行重點採集。

防範意識淡薄易被利誘

「境外間諜情報機關為了得到想要的信息無所不用其極，」內地安全專家盧興盛向香港文匯報表示，普通民眾也可能會成為被「釣」的目標，究其原因，是一些人的國家安全意識淡薄，缺乏法律、保密、防範意識，同時受到通過愛好賺錢的形式所誘惑，不知不覺給國家安全帶來隱患，甚至造成危害，個人也承擔嚴重的法律後果。

大數據國家戰略計劃聯盟發起人、360集團信息保安專家鄔玉良則向香港文匯報表示，近兩年來，以ChatGPT為代表的生成式人工智能技術掀起了全球熱潮，也為黑客製作網絡武器化的「釣魚」郵件提供了便利，民眾更須時刻警惕利用生成式AI製作的新型「釣魚」郵件。他表示，此類郵件技術門檻低，僅需簡單文字描述便可生成語法合理、邏輯通順、文字精練、格式規範的高仿真「釣魚」郵件，更具欺騙性和迷惑性，較之傳統「釣魚」郵件更加難辨真偽，「這就要求我們時刻提高警惕，增強辨別力。」

專家教路防駭 線下反覆查證

網絡「釣魚」作為境外間諜情報機關實施網絡攻擊竊密的主要手段之一，有着成本低廉、手法隱蔽、危害性強的特點。國家安全部17日發文指，在當前網絡竊密多發高發的態勢下，民眾在工作生活中要時刻保持警惕，提高防範應對能力。內地專家亦向香港文匯報表示，要對每一封郵件保持懷疑態度，仔細檢查發件人信息。對於AI製作的「釣魚」郵件，更須利用線下確認和電話查證方式反覆核對。

增強網安知識 完善安防舉措

文章稱，要增強安全意識。隨着網絡「釣魚」方式不斷更新，民眾要學習應知應會網絡安全知識，增強網絡安全風險意識，善於識別網絡攻擊手段，避免「咬餌上釣」。同時，還要提高甄別能力。在工作生活中要注意甄別虛假信息，對於無法確定來源、疑似仿冒、索要賬號密碼等可疑郵件，不要輕易點擊或打開其中的附件、鏈接。

此外，要完善安防舉措。個人應設置具有較高安全性的登錄密碼並定期更新，配置並使用二次認證、異常登錄報警等安全防護功能。相關單位要強化網絡安防措施，啟用有效的安全防護策略。同時，應安裝並及時更新電腦、手機等終端殺毒軟件，定期進行全盤體檢殺毒。

大數據國家戰略計劃聯盟發起人、360集團信息保安專家鄔玉良告訴香港文匯報，企業單位也應落實好網絡安全和數據安全防護主體責任，要定期對員工開展安全培訓，宣傳「釣魚」郵件防範內容，提高企業和員工整體安全防護意識，降低遭受大規模攻擊的風險。他還提醒，民眾不要在任何互聯網網站上隨意輸入賬戶密碼，不發布任何敏感信息。如果遭遇「釣魚」攻擊，應第一時間斷網，並將相關情況匯總上報給企業管理者或相關安全部門，盡可能降低影響，避免擴大危害。