AI衝擊波之慎用科技

「龍蝦」四大伏位與解決對策

「數位葬禮」

描述：用戶將開源系統（如「龍蝦」）綁定至重要賬號（如加密貨幣錢包、電子郵件、社交平台等），導致黑客利用系統漏洞竊取憑證，清空資產、竊取隱私，並長期監控受害者的數據。商家隱瞞風險，推銷未經安全加固的產品，涉嫌欺詐與違反消費者保護法。

專家建議：1.避免盲目信任：不要將所有重要賬號與設備綁定，尤其是未經安全驗證的系統。2.選擇安全產品：購買前應查詢產品的安全評價與認證。3.商家責任：商家應提供產品安全保證，並清楚告知風險。4. 用戶教育：提升用戶的安全意識，避免成為「數位自殺」的受害者。

國家安全蟻穴

描述：學生安裝開源系統後，黑客利用其作為跳板，通過家用Wi-Fi滲透家人的辦公電腦，若家人任職公務員或企業高管，黑客就能進一步攻擊政府或重要機構的內網或關鍵基礎設施，威脅國家安全。

專家建議：1.隔離設備。2.提高家庭成員的安全意識，尤其是涉及政府或關鍵基礎設施的工作人員。3. 加強家用路由器的安全配置，啟用網絡隔離功能。4. 商家應對產品的安全性進行嚴格測試，避免成為國家安全威脅的源頭。

用戶隨時淪無意識幫兇

描述：用戶或企業因管理不善，導致開源系統被黑客挾持，成為「喪屍電腦」的一部分，參與DDoS攻擊或生成釣魚郵件。設備擁有者若存在嚴重疏忽，可能需承擔法律責任，並違反網絡公德。

專家建議：1.定期更新系統。2. 設置強密碼並啟用雙重驗證。3. 用戶主動保護設備，避免成為犯罪工具。4. 了解設備管理不善可能帶來的法律後果，履行基本的網絡安全義務。

認清「易請難送」真相

描述：部分開源系統修改了系統底層設定，即使卸載仍留下「數位餘毒」與「持久化威脅」，使得黑客仍能利用殘留漏洞入侵設備。

專家建議：1.徹底清理：需使用專業工具檢查並清除殘留威脅。2. 對於重要設備，建議備份資料後抹除硬碟並重裝系統。3. 避免安裝可疑軟件。4. 商家應提供卸載指南與工具，保障用戶能安全移除產品。

亂用「龍蝦」引狼入室 黑客秒破防私隱盡失

網安專家實測揭逾二千保安漏洞 若無防火牆猶如「網絡裸奔」

人工智慧技術席捲全球，大眾對「AI助理」的需求日益迫切，但便捷背後暗藏資訊安全風險。中小企老闆陳先生早前安裝俗稱「龍蝦」的開源系統「OpenClaw」，隨即連接家庭Wi-Fi、綁定電子錢包等，三天後赫然發現其中一個電子錢包內的20萬元一夜間消失，即使馬上卸除「龍蝦」仍未能把漏洞連根拔起。網絡安全專家龐博文接受香港文匯報訪問時，即場實測共發現2,127個已錄入中美國家漏洞數據庫（CVE）的保安漏洞，其中超級嚴重漏洞多達33個、高危漏洞也有249個，他形容端口防護幾近空白，普通用戶若在未配備防火牆與入侵檢測設備的情況下下載使用，形同「網絡裸奔」，數據可被輕易竊取，主機也會在數分鐘內被黑客完全控制。

●香港文匯報記者　文禮願

受社交媒體對「龍蝦」隨傳隨到私人助理的宣傳影響，陳先生早前出於好奇，一鍵安裝該系統，全程僅耗數分鐘。隨後他將「龍蝦」連接家庭Wi-Fi，且為求便捷，陸續綁定電子錢包、加密貨幣錢包、郵箱及多個社交、購物平台賬號，殊不知已將自身數位安全門鑰親手交給潛在攻擊者。

電子錢包20萬元一夜消失

安裝僅三天，陳先生赫然發現其中一個電子錢包內的20萬元一夜間消失。他嚇得不知所措，馬上向熟悉網絡安全的專家朋友求救。經調查後發現失款是「龍蝦」系統綁定惹禍，他向香港文匯報說：「專家告知，原來該系統缺乏基本隔離與加密機制，黑客入侵後可輕易通過內存提取（Memory Dumping）獲取所有綁定憑證，實現財產盜取、資訊監控等惡意操作。」

智慧城市聯盟資訊科技管理委員會主席龐博文直指，陳先生的行為形同「數位自殺」。他分析，「龍蝦」系統的設計漏洞，讓黑客無需高超技術，即可輕易實施攻擊：「入侵後不僅能在數秒內令電子錢包歸零，還可通過盜取郵箱重置銀行賬號密碼，將銀行戶口據為己有，甚至利用用戶社交賬號向親友發送詐騙資訊，形成連鎖危害。」

為徹底揭露「龍蝦」系統的安全漏洞，龐博文對今年3月版「龍蝦」系統即場開展模擬攻防實測，還原普通用戶使用場景，若未對系統進行任何額外安全加固，僅依賴其自帶基礎配置，黑客只要搭建常用的Linux攻擊環境，驚險場景瞬間發生：由於「龍蝦」系統默認關閉「登錄嘗試次數限制」，攻擊工具僅用1秒就完成密碼爆破，成功獲取系統最高控制權——螢幕即時顯示，攻擊者可隨意讀取用戶本地檔案、操控設備所有功能，全程毫無阻礙，普通用戶毫無防禦之力。

攻擊者入侵無需複雜操作

進一步端口掃描與漏洞檢測顯示，該版本系統累計存在2,127個CVE認證漏洞，其中33個超級嚴重漏洞、249個高危漏洞直接暴露核心運行模塊，多個端口處於「敞開狀態」，無任何防火牆、入侵檢測機制防護，龐博文形容與「網絡裸奔」毫無差別。他強調，攻擊者無需複雜操作，僅通過自動化掃描工具，即可遠端定位這類無防護設備，快速完成入侵控制，全程僅需數分鐘。

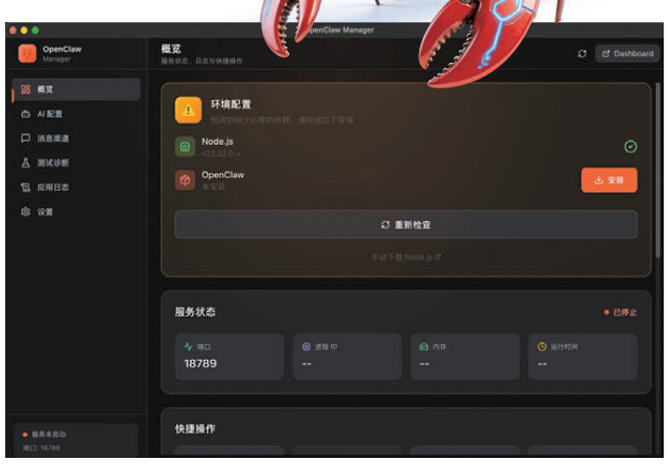
更致命的是，部分「龍蝦」版本設計初衷僅為實驗用途，完全捨棄傳輸層安全協議（TLS），這意味着用戶與系統間的所有指令、對話及敏感資訊，均以「明文」形式在網絡中傳輸。「黑客無論是處於同一網絡環境，還是通過遠端掃描，都能像閱讀報紙一樣，輕易獲取用戶所有隱私，毫無隱秘可言。」龐博文補充道。

全民資安意識務須重建

針對「龍蝦」系統帶來的安全警示，龐博文提出，重建全民資安意識是當務之急，首要任務是打破「科技即安全」的錯誤幻覺。他表示，任何具備聯網功能的設備，本質上都是連接外界的「數位之門」，若缺乏完善的加密機制與認證體系，絕不適合引入私人或私密使用場景。

龐博文建議，政府與教育機構應將資訊保安防禦知識納入市民的基礎生活常識普及範圍，引導市民認識到保護數位身份與保護財產安全同樣重要，從源頭杜絕「因貪圖便捷而放棄安全」的行為，防範類似安全風險蔓延。

◀智慧城市聯盟資訊科技管理委員會主席龐博文就「龍蝦」系統進行模擬攻防實測，發現有近二百五十個高危漏洞。香港文匯報記者涂穴　攝



●OpenClaw界面。　網上圖片

各地對OpenClaw規管

地區/平台	限制現況
內地	據報已禁止政府機關、國有銀行、軍隊及軍人家屬安裝使用。多所高校亦已要求教職員及學生必須「徹底卸載」OpenClaw。
香港	數字政策辦公室提醒各政府部門，鑑於OpenClaw存有權限過高、資料外洩及系統入侵等安全隱患，不應在任何連接政府系統的電腦上安裝此工具。
新加坡	發布全球首份《智能體AI治理框架》（Model AI Governance Framework for Agentic AI），專門針對像OpenClaw這種具備自主行動能力的工具。雖然沒有禁止該工具，但要求企業在使用時，關鍵決策（如轉賬、刪除大量文件）必須由人手審核，且企業需為AI智能體的行為承擔法律責任。
Google（Antigravity服務）	今年3月大規模封鎖使用OpenClaw框架連接其AI服務的用戶賬號，以維護運算秩序與系統穩定。

私隱專員警告：代理式AI權限大風險更大

香港文匯報訊（記者 廣濟）「養龍蝦」（OpenClaw）熱潮今年初席捲全球各地，香港特區政府個人資料私隱專員公署就開源系統OpenClaw及其他代理式AI發出警示，提醒機構及市民使用前需留意個人資料私隱及安全風險。個人資料私隱專員鍾麗玲日前接受香港文匯報專訪時指出，代理式AI（又稱AI智能體）與傳統大語言模型有明顯分別，其私隱風險明顯更高。研究顯示在大約一萬個技能中，有超過800個屬於惡意，即是大概每12個技能就有一個已被植入惡意程式。若用戶安裝這些技能，AI智能體可能執行錯誤指令，甚至讓黑客取得整個電腦的控制權。

十二分一技能被植入惡意程式

鍾麗玲在訪問中提及兩宗涉及AI功能的海外個案。第一宗是海外科技公司個案，一名員工向人工智能系統提供公司原始碼，結果構成資料外洩事故，公司即時停止相關AI的運作，並通知員工暫停使用。第二宗是美國連鎖快餐店，店方使用AI語音點餐系統，但在實行前測試不足，推出後因環境雜音導致點餐嚴重偏差，例如顧客只點一個雞餐，系統卻記錄成十個；又或顧客點雪糕，送上的卻是雪糕加茄汁，最終在100個零售點全面停止AI點餐計劃。

鍾麗玲表示，傳統AI主要負責回答問題、做簡單總結或分析，像一個「機械人朋友」，但代理式AI則像一個「私人助理」或「執行者」，可根據指令主動執行任務，例如進行網購、回覆電郵、訂飛機票或繳交水電費。由於需要執行這些任務，代理式AI的權限遠大於傳統AI，往往需要存取用戶的銀行戶口資料、密碼、電郵及文件等。因此，從保障個人資料私隱的角度，代理式AI帶來的風險比一般大語言模型更高。

指令誤解或致電郵誤刪

指令誤解亦會加劇使用風險。例如用戶只想買一張去倫敦的機票，但AI可能誤解為購買頭等艙；或用戶只要求刪除一封電郵，但AI會連同關聯電郵一併刪除。高風險操作時，她建議設定AI每次執行前必須先向用戶確認。

她強調，無論是傳統AI或代理式AI，只要涉及收集、使用個人資料，香港現行《個人資料（私隱）條例》仍然完全適用。同時，公署2023年已推出《使用AI聊天機械人「自保」十招》，並發出《僱員使用生成式AI的指引清單》，以及《人工智能（AI）：個人資料保障模範框架》。公署亦已審視接近90間機構使用AI的情況，並舉辦多場企業內部培訓及推廣活動。

掃碼睇片