廿一世紀駭客網絡
駭客教學、犯罪一條龍

駭客破解視窗7可無限使用

提款卡駭客半天環球偷7300萬　入侵RBS偷密碼　港拘兩「提款員」

駭客襲Hotmail　Gmail　萬用戶密碼被公開。

「駭客」（Cracker）不再僅是犯罪小說裏的專有名詞，駭客技術更非少數電腦精英的專利，在網上有成千上萬的「駭客教學」網站，病毒程式任人下載，青少年要成為年輕駭客，已非難事……

記者・黃愛琴　張寶晶　編輯・王菁卉　攝影・王菁卉

個案一：小五已學會做駭客

十六歲的老子（網名），自小學五年級起就從網絡學會駭客技術，如社群、論壇都有教程及討論，後來他更自購電腦保安書籍來鑽研：「那些課程是公開的，正如你在書局可以買到中學的教科書一樣。」更甚的是網上有各式各樣的病毒程式任人下載：「每當國內外有新病毒，都會有人把病毒的樣本放上網。」

十三歲時，老子成立網上組織「一日小駭（Crack）」，實行「有理無理，每天來一小駭」。他指，該組織會員以中學生為主，在高峰時期，會員數目更達至七百多人。零七年，由於有傳媒報道「一日小駭」公然於網上教授各種入侵電腦系統的知識，引起警方關注，因此，老子唯有把該組織的網站關閉。他表示自己知道錯了，決心改過，另成立香港破曉黑客文化及資訊安全協會，希望透過這個組織加強大眾的網絡保安意識。

老子承認曾經入侵了不少網站和電腦，例如電郵戶口、學校伺服器和企業網站，所及地區包括台灣和中國。他也曾經試過不斷找尋有漏洞的網站，然後提醒管理員去修補漏洞：「如果對方是學校網站，我可能會在公告欄以校長的名義或是盜用網絡管理員的帳戶留個言，讓他們知道存有漏洞及其嚴重性。有時候，可能只會發個電郵告訴他們，要視乎找到哪些可以聯絡網管的方法。」

老子表示，最初只是為了追求快感，想嘗試一下學習到的新「招數」，無聊地看見有保安漏洞，就進去留言。直到後來，則是為了挑戰自己，追求難度。「或者，也可以理解為年少時看多了武俠小說，便在網上用這種自以為是大俠的形式達到夢想吧！」

老子考慮到當時入侵的對象都不在香港，而跨境駭客活動較難追查，故毫不擔心自己的駭客活動會被警方發現：「老實說，在這個圈子中（駭客圈），你一定會很熟悉相關的案例和法律，駭客都是很精明的傢伙。」老子續稱，有些駭客更會留意到政治局勢有助便利入侵活動：「台灣就曾經追查一名電腦入侵者，但由於該入侵者在中國，結果就不了了之。」

個案二：為求報復 入侵電腦

現年二十多歲的家威（化名）乃香港中文大學電腦工程碩士生，初中開始學習駭客技術，經常到網上找別人所寫的入侵軟件（cracking software）研究。試過有同學激怒家威，他就萌起報復之心，匿名傳送一幅附帶病毒程式的圖片給那同學：「當他看那幅圖片時，病毒程式就會在電腦中運作。」家威後來聽說那位同學的電腦硬件和底板都報銷，更沾沾自喜：「那一刻，我知道自己成功了！」

家威初時只在網上下載入侵程式，成功入侵同學的電腦後，更開始學寫入侵程式：「我會覺得自己懂而別人不懂很威風，而且做駭客就好像刺客一樣，沒有人知道你在做甚麼，別人在明、你在暗，覺得很刺激。」

家威表示網上駭客技巧不難，甚至可作不法用途，只是如今不似年輕時意氣用事：「如果你問我懂不懂得如何偷取別人的信用卡密碼，我是懂的，但是我不會這樣做。」

黑客駭客　孰正孰邪？

一般人會把黑客（Hacker）視為電腦罪犯，但這個專有名詞其實是指那些檢查電腦系統有何漏洞、發現後再去修正或通知系統管理員的「俠客」，故黑客很多時也是電腦保安工作程式編寫員。黑客必須熟悉網絡程式的運作及應用原理，例如資料庫、病毒、密碼學、網絡保安等。所以在老子眼中，「Bill Gates也是黑客」。

相反，利用公共通訊網路，在未經許可的情況下，入侵他人電腦系統，並作出攻擊的人應稱為駭客（Cracker）。家威概括：「Hack（黑）是做好事，而Crack（駭）就是做壞事。」

個案三：為所欲為 偷看私隱

香港中文大學物理系三年級生子超（化名），中六時很喜歡與班裏的朋友一起研究駭客技術，希望藉此了解網絡如何運作，提升自己的電腦技能。

為求刺激和確認自己已學會駭客技術，子超與朋友嘗試入侵同班同學的電腦。他們會一起上線，找尋目標同學的IP位址（網際協定網址，是在網絡上給主機的編址），然後利用自己編寫的駭客程式進入他們的電腦系統，偷看到目標同學的私隱：「看的主要是同學的功課，最有趣的是MSN紀錄！」

子超升讀大學後因學業繁重，再沒有時間從事駭客活動。但回想昔日做駭客，偷看朋友的私隱便感滿足：「當你寫一個電腦程式出來，然後做到你想做的事，你會很滿足。」

網上駭客教學氾濫 網絡罪行難追究

警方去年一至十一月，共接獲一千三百七十八宗與電腦有關的罪行，較去年全年的七百九十一宗大增七成四，當中涉及「非法進入電腦系統」的案件，更由去年的四十六宗，大幅增至今年的四百一十宗，升幅接近八倍。在去年四百多宗個案裡大部分涉及網上電郵戶口被盜用，當中包括罪犯利用偽冒電郵及虛假網站盜取電郵戶口資料。根據電訊條例不獲授權而利用漏洞入侵他人電腦，即使不作出破壞，也要負上刑責。如果有犯罪或不誠實意圖而取用他人電腦資料，可判監五年；在未獲授權下取用電腦資料，即可罰款二萬元。

三位年輕駭客表示，網上到處都有駭客技術的教學和駭客軟件下載，如被中國防毒軟件商列為病毒榜首的遠程控制軟件「灰鴿子」，曾在其官網供網民隨意下載，後因零七年中央電視台將事件曝光後才被逼停發，但網民現時仍可透過非法途徑如BT點對點下載。

雖然如此，家威認為，一個駭客的技術夠好，警方難以追查：「他們或者可以找出一些線索，但是所需的時間一定很長。好像破解一個十個位的密碼般，警方要試過所有的機率，可能要試一百二十年才能夠試到。」香港電腦保安事故協調中心經理古煒德也認同，要追查駭客的身分和所在地區很難，駭客對法律漏洞往往瞭如指掌，加上網絡是國際性的，跨國調查有難度。他以近年流行的網絡詐騙「釣魚網站」（phishing website）為例，指出追查原兇困難重重：「誰寫這些程式和網頁，誰想出策略，甚至誰拿了錢，一連串的過程，就如供應鍊般。雖然警方找到了中間某些機構，但始終很難追查原兇。」

警方發言人表示，警方已採多管齊下的措施對付網上罪案，除加強執法外，科技罪案組已於去年十月增加人手，由四十五人增至七十一人，以加大電腦法理鑑證、調查及防止罪案的力度，又會繼續與海外執法機構加強合作，以更有效跟進境外網上罪行。

電腦保安意識由個人做起

香港電腦保安事故協調中心經理古煒德提醒，大部分受病毒感染的電腦都是個人或家用電腦：「很多時候在大機構出現網絡問題，都和個人保安做得不好有關，例如員工家中的電腦中了病毒，把帶有病毒的檔案帶回公司，使公司損失。」他又指，新科技產品如Facebook、MSN、iPhone等，雖然已漸被廣泛使用，但其保安發展卻未完善，容易成為駭客的入侵目標。

子超及老子都認為，防毒軟件只能夠防止大規模散播的電腦病毒，阻隔一些不明來歷的網絡地址，如果駭客有意入侵的話，防毒軟件未必能夠發揮效用。也有一些軟件如Hacker Eliminator是專防駭客攻擊和木馬病毒的，彌補普通防毒軟件和防火牆的不足，但用家往往會嫌麻煩，連打開Microsoft Office也得通過其允許。所以老子認為，更重要的是培養保安意識：「如果你見到一個.exe的檔案，你應質疑它是不是一個病毒，或者是一個木馬程式。.exe檔是最有可能含有病毒的檔案類型，這就是意識問題。」