警方研發系統 防入侵「獵黑客」

可搜出「殭屍電腦」盼更多企業學校加入擴大數據庫

網絡黑客攻擊日益猖獗，由居家到企業無孔不入，市民私隱和錢財隨時被盜。香港警方與私人機構聯手研發出名為「HoneyNet」的「威脅預警及捕獵網絡」，這是全球首例由公私合作開發的網絡安全情報系統。過去一年，「HoneyNet」發現了逾億個網絡威脅，而發起黑客攻擊最多的國家包括美國。測試更發現黑客入侵智能家居電器，盜取和偷窺市民私隱。這套「獵黑客」系統，不但可助警方找出「殭屍電腦」，也可協助網絡安全公司完善防毒軟件，提高市民電腦的防火牆功能，有望全港更多企業學校加入系統，擴大數據庫，以預警來自不同國家或地區、不同方向、不同網站的黑客攻擊威脅。

◆香港文匯報記者 蕭景源

◀網罪科與研科院合作研發「HoneyNet」系統，以提升收集黑客攻擊情報。 香港文匯報記者廖傑堯 攝

▲黑客可用惡意程式入侵家居智能產品。 香港文匯報記廖傑堯 攝

警方昨日公開「HoneyNet」的運作原理，表示該系統是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，並透過人工智能及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，使用的技術在世界處於領先位置。

攻擊多來自越南美國荷蘭

網絡安全及科技罪案調查科署理高級警司范俊業表示，「HoneyNet」由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。

他指出，該系統透過分析2,048種惡意程式，發現其中40種為新發現的變種惡意程式，並發現該些惡意攻擊來自35.88萬部有關可疑的伺服器或電腦，其中1,218部是位於香港的「殭屍電腦」，警方已透過網絡供應商通知用戶及協助將之清除。

香港應用科技研究院應科院網絡安全與分析高級經理梁偉基指出，研發的「威脅預警及捕獵網絡」在測試中發現，網絡攻擊一般有三個步驟，第一步是以漁翁撒網方式向使用者「敲門」，若有反應就會進行第二步攻擊掃描。黑客會有一套「清單」針對較弱防護使用者，例如使用較簡單及常用的密碼，就很容易被入侵。

第三步，黑客會在電腦或家居電腦產品，例如路由器WiFi連接的多項家居產品，該些智能家居裝置較少安裝防毒軟件。黑客會利用微型電腦連接路由器，再傳送木馬或惡意軟件至家居產品，例如智能電視、電腦或IPcam（家居閉路電視），造成破壞或盜取資料。使用者可能被勒索。

奪取權限 偷用電腦「挖礦」

系統測試又發現了一種新的趨勢情報。黑客除輸入勒索、病毒軟件外，還會利用入侵電腦奪取權限，進入電腦中央處理器透過該電腦進行虛擬貨幣「挖礦」，使用者可發現個人電腦的中央處理器佔的數據量突然變大。

梁偉基表示，系統數據不單是統計，還可以向警方提供調查案件的資料，又或找出「殭屍電腦」的IP地址進行淨化來源行動，亦可為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。

香港應用科技研究院行政總裁葉成輝表示，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，才能提高威脅預警及捕獵網絡黑客。目前，「HoneyNet」共有6個「HoneyPot」測試點，其中兩個在應科院，另外4個在警方網罪科和電訊公司及大學等地點，希望能有更多機構包括學校、中小型企業、大型企業及網絡營運商參與，使收集數據更龐大，截擊網絡攻擊更加全面。

用高強度密碼 破解「1秒變5年」

特稿

普遍黑客都會「取易不取難」。不少市民購買電腦產品後，由於貪方便不更改原廠設定密碼，又或使用簡單的密碼設置，因而容易被黑客攻擊。網絡安全及科技罪案調查科署理高級警司范俊業昨日表示，其實安全密碼可有效提升網絡的防禦能力，可能是「1秒」與「5年」之差。

范俊業指出，很多在設置電腦產品密碼時會選用較簡單或易記的密碼，例如過往最多人使用的「admin」，黑客只要透過攻擊掃描，1秒鐘就可以破解其密碼入侵其電腦，但如果使用較強且複雜的密碼，例如「Iwoke@PAQ」，由於包含了大小寫及字符組合，黑客可能要花上5年以上才能破解。

要有效防止黑客攻擊，在使用高強度密碼的同時，更應定期更新電腦系統，以修補系統漏洞；定期使用防毒軟件為電腦掃描；切勿點擊不明來歷的網址。

今年9，網罪科推出了一站式的「防騙伺服器」，協助公眾辨識詐騙及網絡陷阱。市民可按網上要求輸入相關可疑的電腦IP地址，伺服器就會即時評估網絡安全的風險。

平台測試結果會有四種不同顏色顯示，紫色代表「未有紀錄」、黃色代表「提防中伏」、橙色代表「疑似有伏」及紅色代表「高危有伏」。

◆香港文匯報記者 蕭景源

警設顧問小組 加強應對網罪

香港文匯報訊（記者 蕭景源）為應對不斷上升的科技罪案，以至未來更多新型的網絡威脅，香港警務處前日成立「網絡罪案警政顧問小組」，委任了12位來自多個界別的網絡安全專家及領袖，協助警隊制定短、中、長線策略方向，以加強在應對網絡罪案方面的數碼警政能力。

警方昨日表示，「網絡罪案警政顧問小組」的12名小組成員來自學術、教育、商會、金融、資訊科技、電訊、公營機構等的專家及領袖。警務處處長蕭澤頤前日主持了顧問小組成員的就職典禮，並向他們頒授委任狀。

警方期望透過融匯專家和領袖的專業知識和視野，加強在應對網絡罪案方面的數碼警政能力。

另外，警方網絡安全及科技罪案調查科首次主辦的「網絡攻防菁英培訓2022/23」網絡安全活動，將於明日在香港都會大學舉行啟動禮。該大型網絡安全推廣活動以粵港澳大灣區青少年為對象，旨在透過網上互動遊戲及網絡防衛比賽，提升青少年的網絡安全知識，推廣網絡安全「零信任」（Zero Trust）的概念，加強大灣區人才及組織在網絡安全領域的協作，發掘網絡安全人才，為有志投身網絡安全的青少年提供「職業生涯規劃」。香港特區政府警務處處長蕭澤頤、澳門特區政府司法警察局局長薛仲明，及內地網絡安全公司奇安信集團副總裁劉進會以視像形式參與啟動禮。

渣打：1%信用卡賬戶受盜用事件影響

香港文匯報訊（記者 蔡競文）渣打信用卡疑遭大規模盜用事件備受各界關注，渣打發言人昨日表示，該行就可疑信用卡交易即時實施的監測措施已見顯著成效，問題交易量已大幅下降，又透露事件中僅有1%信用卡賬戶受影響。

渣打發言人表示，是次事件為不法分子隨機的信用卡小額測試，並無證據顯示銀行出現個人資料外洩。

該行已啟動信用卡退款保障機制，由下周一起陸續安排退款，預計可於一周內完成。

放「正印」涉起底落網 「小三」私隱上網

香港文匯報訊（記者 蕭景源）《2021年個人資料（私隱）（修訂）條例》於去年10月刊憲生效，將起底罪行刑事化，令私隱專員公署變身「有牙老虎」，打擊起底致網上公審霸凌的歪風。私隱專員公署昨日在港島區拘捕名一名35歲已婚女子，懷疑因不滿丈夫有婚外情及反擊「小三」，涉嫌起底「小三」資料放上社交平台「唱衰」報復，披露的資料包括對方姓名、出生年份及工作地點等個人資料，涉嫌違反《個人資料（私隱）條例》第64（3A）條的規定。

連同該宗個案，至今已經有12人涉嫌觸犯相關罪行而被拘捕。香港文匯報在整理有關的個案後發現，情財糾紛和個人仇怨是目前觸犯「起底」罪行的主要動機。

私隱專員公署早前接獲相關舉報及經調查，顯示該宗起底案涉及一段婚外情。被「起底」的女事主與被捕女子的丈夫，於2019年至2021年間曾有感情關係，但最後兩人分手。女事主疑不忿這段婚外情未有開花結果，將這段關係曝光給女疑犯「示威」。

由2021年11月至2022年5月期間，有人在一個社交媒體平台的群組上先後發布了3條包含女事主個人資料的訊息，並對女事主作出負面的評論及指控。被披露的個人資料包括女事主的中英文姓名、別名、出生年份、居住地區、工作地區，以及她的職業和照片。私隱專員公署根據舉報及經調查後，昨日拘捕涉案的「正印」。被捕的女子35歲，已獲准保釋，案件仍在調查中。

聲稱遭騙財 網爆事主資料

前日，私隱專員公署落案起訴另一名36歲女子，涉嫌從事網上買賣活動期間因金錢糾紛，違反《個人資料（私隱）條例》第64（3A）條「在未獲同意下披露個人資料」共14項罪行。

調查顯示，女被告從事網上買賣活動，被起底的事主曾是其供應商，兩人由商業夥伴關係其後演變成金錢糾紛。

2021年12月期間，有人在一個社交媒體平台約14個不同的群組上發文，聲稱有人騙財，文中披露了事主與其丈夫的個人資料，包括中文姓名、電話號碼及相片。私隱專員公署於2022年7月26日拘捕被告，案件將本月12日在沙田裁判法院首次提堂。這是在「起底」刑事化後，私隱專員公署第四宗落案起訴的個案，其中一宗已定罪。

起底案多涉情財糾紛

據香港文匯報根據私隱專員公署拘控的12宗個案中整理顯示，起底罪行的犯案動機涉及市民生活中的各種糾紛，包括「貼街招」追債、情侶分手、工作結怨、財務糾紛、業主租客衝突和婚外情等，最終的目的都是為了報復。

這些起底一般是指透過網上搜尋器、社交平台及討論區、公共登記冊、匿名報料等方式，將目標人士或其相關人士（如家人、親友等）的個人資料搜集起來，並在互聯網、社交媒體或其他公開平台（例如公眾地方）發布。

在法例修訂前，這種歪風在網上盛行，引發網民公審和評論，並引發網上欺凌，隨着私隱專員公署根據法例賦予執法權，相信有助遏止歪風。私隱專員提醒市民，起底屬嚴重罪行，違例者一經定罪，最高可被處罰款100萬元及監禁5年，而《私隱條例》同樣適用於網上世界，市民在網上或社交媒體平台發布或轉載起底訊息前都要三思，以免觸犯法例。

起底刑事化後被拘控案件

感情糾紛

- 35歲女子疑不滿「小三」與其丈夫有婚外情，在一網上社交平台發布該「小三」的姓名、出生年份、相片及工作地點等個人資料。
- 27歲男子與女友分手後，在不同社交媒體平台冒認舊愛開設賬戶，披露對方個人資料，致不少陌生人聯絡受害人意圖交友。男子承認7項控罪，是起底刑事化首宗定罪案件。

租務糾紛

- 59歲女業主疑因租金糾紛，於今年3月在社交媒體平台群組中，發布租客的個人資料包括照片。
- 36歲男子因租務糾紛在社交媒體平台，發布了大學生女租客的個人資料，並對事主的父母作出負面評論及指控。

僱傭糾紛

- 48歲男中介疑與臨時僱員就薪金及工作編配發生糾紛，涉披露對方的身份證副本等個人資料，並備註「永不錄用」。

財務糾紛

- 37歲男子因外傭無法來港工作，而就合約事宜與外傭中介公司有金錢糾紛，在社交媒體平台披露中介人個人資料及作出負面的評論及指控。
- 46歲男子與商業夥伴因金錢糾紛而拆夥，在對方公司大廈外牆及周邊貼大字報，披露對方姓名、照片、公司名稱等個人資料。
- 36歲女子與網購商業夥伴因錢反目，於社交媒體平台約14個不同的群組上發文披露對方與其丈夫的個人資料，並聲稱受害人騙財。
- 41歲男子疑涉商業糾紛，在不同社交媒體平台上披露3人的全名、別名、電話號碼、任職公司及公司職位等個人資料。
- 31歲男子因金錢糾紛在社交媒體平台兩個不同群組上披露兩人的姓名、手提電話號碼、職業、住址及僱主名稱等個人資料。

工作糾紛

- 31歲男子與受害人因工作結怨，最終被公司解僱，在網上披露受害人的姓名、手提電話號碼、居住屋苑名稱及私事等。

煽仇煽暴

- 23歲男子在社交媒體平台披露警務人員及70位立法會議員以及其家人的個人資料，包括出生日期、身份證號碼和住址等。

製表：香港文匯報記者 蕭景源 資料來源：個人資料私隱專員公署