

# 侵1300萬電腦 3黑客落網

## 散播「殭屍」盜資料 全球最大宗罪案

【本報訊】綜合外電三日報道：西班牙警方聯同私人電腦保安公司破獲全球迄今最大規模的黑客罪案，拘捕三名男子，指他們利用「殭屍網絡」（Botnet）發動襲擊，令到一百九十個國家逾一千三百萬部電腦受到感染。「中毒」的電腦包括來自逾五百間最大型企業及至少四十家大銀行，黑客遙控受感染的電腦後，肆意盜取信用卡密碼、網上銀行資料及其他個人資料。

被捕的三名疑犯包括外號「凱羅網」及「哈姆雷特1917」的三十一歲集團主腦，以及兩名分別為二十五及三十歲的同黨「Ostiator」和「Johnyleante」，三人都是在上月落網。其中一人被捕時，手頭上擁有多達八十萬人的個人資料。

三名黑客營運的犯罪集團名為「蝴蝶殭屍網絡」，他們向全球個人電腦發放殭屍病毒，以盜取信用卡號碼和其他資料。他們又會向其他黑客「出租」受感染的電腦牟利。

受「蝴蝶」影響的電腦超過一千三百萬部，遍布全球一百九十個國家。受影響的包括住家、學校以及數以百計的政府機構，全球一千間最大企業中也有超過一半「中招」，當中最少包括至少四十間大型金融機構。

### 「蝴蝶工作組」意外破案

西班牙當局周三召開記者會，宣布在一群志願者組成的「蝴蝶工作組」協助下，偵破這個全球最大規模的電腦犯罪集團。相信其他國家將陸續有更多疑犯落網。防衛情報公司、熊貓安全公司以及佐治亞理工學院的研究者是「蝴蝶工作組」的成員。

這些黑客其中一次襲擊是針對防衛情報公司在渥太華的電腦。他們對該公司打擊「蝴蝶殭屍網絡」的努力感到惱火，遂在一月二十五日以每秒九億萬位元的速率把數據傳送給防衛情報公司的伺服器。

防毒公司做了很多出色的工作，發現了某些蝴蝶殭屍的密碼，但是，黑客們非常頻繁地改變他們的軟件——有時每四十八小時就改變一次——使得這些惡意軟件的很多版本都未被發現。公司防衛情報公司總裁克里斯·戴維斯說：「防毒公司描述病毒特徵的速度根本跟不上。」

研究者說，現時仍有很多受蝴蝶殭屍感染的個人電腦，但他們正在與防毒商合作，旨在更有效地偵察和刪除網上惡意程式。戴維斯說，估計一兩個月內，受感染電腦數目「會大大減少」。

戴維斯說，犯罪犯了一個致命錯誤，就是在登記命令及控制網絡時，使用了一個真實姓名。他們可能以為自己是匿名的，因為他們使用了一個私人域名登記者。可是，碰巧該家公司與「蝴蝶工作組」有合作關係。戴維斯說：「他們太過自信和大意，終於被逮個正着。」



### 防不勝防的「殭屍」



多少台電腦中了招？

總數難以得出，但在去年十二月二十三日至今年二月二十三日，就有超過一千一百萬台電腦被「殭屍」入侵。

黑客用它來幹什麼？

「殭屍網絡」是為盜竊資料而設，至今共有上百萬台電腦被其盜去資料，當中除了用戶的個人資料和銀行資料，還有他們在網站上的帳戶資料、帳號和密碼。

它是誰人發明的？

暫時未明。加拿大資料保安公司防衛情報公司表示正與執法部門合力調查「殭屍網絡」是由誰設計。

哪些銀行和企業中了招？

防衛情報公司拒絕透露，只表示已與重要的受害企業和機構聯絡。若閣下想知道自己的企業有否中招，可登上 <http://www.defintel.com/areyou.shtml> 查詢。

「殭屍」是如何傳播的？

通過即時通訊程式、USB 盤和點對點網絡傳播。防衛情報公司在分析中發現「殭屍」主要在微軟的通訊程式MSN中散播。

為何許多防毒軟件都探測不到它？

「殭屍」現時共有超過兩百個「品種」，有些會被防毒軟件偵測到，有些不會。網絡保安公司正在與防毒軟件公司合作，讓防毒軟件快速更新，以識別最新的殭屍網絡。

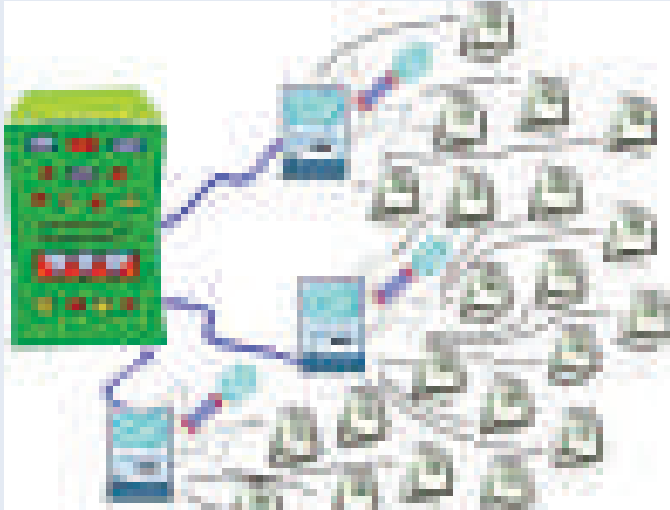
電腦用戶可以怎樣防禦「殭屍」？

可以利用「新威脅」組織（Emerging Threats）提供的 snort 規則或者網絡封包分析軟件 Wireshark 的 plugin 外掛工具。

（資料來源：加拿大防衛情報公司）

西班牙網絡安全負責人宣布破獲全球最大規模的黑客集團（互聯網）

「蝴蝶殭屍網絡」令全球逾一千三百萬部電腦受到感染。圖為互聯網用家（互聯網）



「殭屍」病毒通過即時通訊程式、USB 盤和點對點網絡傳播，以盜取資料（互聯網）

# 不滿英政府削經費 霍金擬遷加國



霍金教授計劃放棄劍橋教席遷居加拿大，以抗議政府削減科學經費（資料圖片）

【本報訊】據英國《每日郵報》三日消息：霍金教授在劍橋大學工作了近五十年後，現在正計劃放棄劍橋教席遷居加拿大，以抗議政府削減科學經費。這位世界上最著名的物理學家，已對日益削減大學預算感到沮喪，他認為此舉會妨礙科學發展。

霍金於一九六二年開始在劍橋工作，他的辭別將對劍橋和英國學術研究構成巨大打擊。六十八歲的霍金，在理論物理學領域取得很多重要突破，而他本人則因為患上運動神經元病而幾乎完全癱瘓。

霍金說，經費的限制將意味着英國科學研究將日益集中於工業應用而不是追求知識和發現。他將於今年夏天到安大略的周邊理論物理研究所待兩個月，而如果一切順利，準備長期待下去。

霍金的發言人二日說，霍金「依然對政府的科學資金政策持嚴厲批評態度」，並說削減科學經費可能會終止英國產生眾多世界級思想家的歷史。為了削減政府赤字，未來三年間英國將削減約十億英鎊的高等教育經費。

霍金的助教薩姆·布拉克伯恩說：「霍金教授正考慮遷居，但一切要看他在周邊理論物理研究所之行是否成功。」

### 名模娜奧美金寶再涉襲人

【本報訊】綜合外電三日報道：有「黑珍珠」之稱的英國名模娜奧美金寶（Naomi Campbell）（見圖）以脾氣暴躁見稱，之前已涉及多宗打人案。但她似乎仍未懂得收斂，日前再遭一名紐約司機投訴，指她從後座突襲，之後逃去無蹤。紐約警方一度通緝她，並考慮是否提出起訴，但最終基於沒有目擊證人，決定不對她提出刑事檢控。娜奧美金寶的發言人事後表示，她會和警方合作。

事發於周二下午約三時，遇襲的司機屬臨時聘用性質，只工作一天。該司機事後向一名交通執法人員投訴，指娜奧美金寶從後座襲擊他，令他的臉部撞落軌盤，右眼下方即時撞瘀。警方接報到場時，娜奧美金寶已不知所終。

該名二十七歲司機告訴警方，他在曼哈頓一間酒店接載娜奧美金寶，要把她載到皇后區的阿斯托里亞錄影廠，但她在車廂中突施襲擊。

警方事後要求會晤三十九歲的娜奧美金寶，以了解事發經過。其發言人事後強調，外界不應過早下判斷，並指她會和警方合作。警方其後表示，由於沒有目擊證人，只把案件列為騷擾投訴，不會提出刑事檢控，因此不會採取拘捕行動。

娜奧美金寶的臭脾氣早有前科，她因為毆打家傭，又在倫敦希斯路機場襲擊兩名警察，屢遭檢控。



## 日產全球回收近 54 萬輛車



紐約國際車展上的日產 Armada 款汽車（資料圖片）

【本報訊】據法新社東京三日電：日產（Nissan）汽車公司宣布在全球回收近五十四萬輛車，指煞車腳掣和油錶有問題，當中大部分受影響的問題車在美國市場銷售。要回收的車款包括二〇〇五至二〇〇八年出廠的 Titan、Armada、Infiniti QX56s、Frontier 小卡車、Pathfinder 及 Xterra SUV 等車款。

其中煞車腳掣有問題的車款在美國有十七萬九千輛，中東、加拿大、俄羅斯及其他國家的則佔兩萬六千輛。這些車的腳踏活塞容易鬆脫，導致煞車力度減低。但日產強調，並無接獲因為腳踏活塞鬆脫，導致有人受傷或車輛的報告。它呼籲車主若發現腳踏鬆脫，可以聯絡代理商。

此外，燃油錶問題也影響日產在美國的四十一萬九千架車，以及在其他地方的五萬三千架車。問題車油缸的感應器出問題，車內的燃料儀表板會在油箱已空的情況下，顯示仍有四分一燃油的訊號。

日產表示，將會通知須召回的車主何時應將車輛送至

當地經銷商維修。同時，日產也希望顧客在其車輛接受檢查之前，盡量維持油箱半滿以上的狀態。

日產表示，目前所有正在出售的車輛都沒有上述兩項問題。日產北美發言人周二表示：「我們為了預先防範而採取這一行動，對於給顧客造成的任何不便，我們深感抱歉。」

在日產宣布召回行動之前，美國通用汽車周二也宣布因動力轉向故障問題，將召回一百三十萬輛 Chevrolet 和 Pontiac 車種。上個月，日本本田車廠因安全氣囊恐造成暴衝的問題，召回數百萬台車輛。

日產汽車宣布展開召回行動的同日，正有報告顯示日產汽車銷售量年增長率冠於亞洲車廠。日產二月份銷售量較去年增加百分之二十九，遠高於本田百分之十三的年增率與韓國現代汽車百分之十一的年增率，而受召回事件打擊的豐田汽車二月銷售量則較去年同期下滑百分之八點七。

### 美堪薩斯州首府暫名「谷歌」

【本報訊】據美國廣播公司三日報道：美國堪薩斯州首府托皮卡市（Topeka）將在本月暫時更名為「谷歌（google）」。這項市名更改決定已在一日的市議會上獲得批准，托皮卡市的市長比爾·波頓隨後宣布，整個三月份托皮卡市都將名為「谷歌」。

波頓解釋了更名的理由，是因為該市被谷歌公司選為測試超高速寬頻的試點，托皮卡市因此成了美國的「光纖之都」。根據測試，谷歌的超高速寬頻將比目前的互聯網速度快一百倍。

目前該市路標和市政府網站也已經用谷歌標誌取代了原有標誌。波頓更在官方網站上，歡迎訪客來到「谷歌之城」。



美國堪薩斯州首府暫時更名為谷歌（互聯網）

## 紐約州法庭小火災 疑為恐襲虛驚一場

【本報駐美記者黃曉敏紐約二日電】二日上午十一時許，毗鄰紐約華埠、位於中央街一百號的紐約州法庭的地下室突然冒出濃煙。法庭的法警以為紐約又遭到恐怖攻擊，馬上知會紐約警方和聯邦反恐部門。

反恐部門和警方在五分鐘之內將法院附近的幾條街全部封鎖，並馬上進行人群疏散工作，將法庭裡面的法官、檢察官、律師、評審團、證人，以及聽審的群眾等相關人士快速疏散，並用大型囚車把囚犯從法院的另一通道運走。

經過消防人員的檢測，排除恐怖攻擊，初步認定是由於電線短路引起的小火災。

雖然虛驚一場，不過聯邦反恐部門和紐約市警方的反應迅速，配合緊密，井然有序地疏散工作，令附近的居民高度讚許。



火警後人群迅速疏散（互聯網）