apophasis / June 12, 2014 07:43AM
[青報] 共軍駭客部隊再曝光 主攻美航太 [2014-06-12]
[青報] 共軍駭客部隊再曝光 主攻美航太 [2014-06-12]
更新日期：青年日報 2014-06-12
引用日期：2014-06-12
引用連結：
http://news.gpwb.gov.tw/news.aspx?ydn=026dTHGgTRNpmRFEgxcbfVEV3cQibTDk%2f3zFY4u8tBdAIED8ilUlDamO%2bBjjNxSe%2fZakVsXEmcWxEx5JzWtjTXJjMfL5zbmXS9nASaUMrKw%3d

編譯組 / 綜合外電報導

美國網路安全公司CrowdStrike九日表示，自二○○七年以來，上海的共軍六一四八六部隊，持續針對美國、歐洲與日本政府機構與國防承包商發動網路攻擊，並試圖以瑜珈中心的廣告為誘餌，詐取美國衛星和航太計畫案。這是近一個月來曝光的第二支共軍駭客部隊。

CrowdStrike報告指出，六一四八六部隊駭客主要以Adobe Reader和微軟Office文書處理軟體等「熱門生產力應用程式」為媒介，鎖定美國太空、航太和通訊部門攻擊，並透過針對性的電子郵件攻擊，部署惡意軟體。報告部分內容已獲《紐約時報》查證確認。

CrowdStrike的研究人員說，共軍駭客散布的電子郵件，乍看之下是一家位在「歐洲航太重鎮」法國圖洛斯的瑜珈中心廣告信，但只要使用者一點閱郵件，駭客就能繞過用戶電腦的安全防護竊取資料。遭駭客攻擊的目標有許多是高爾夫俱樂部的會員，CrowdStrike將這些共軍駭客戲稱為「推桿熊貓」。

不到三週前，美國司法部才空前地起訴五名共軍六一三九八部隊軍人，稱他們涉嫌竊取貿易機密。去年另一家網安公司Mandiant也確認包括美國鋁業、西屋電器及美國鋼鐵等公司受到的數以千計網路攻擊，正是出自六一三九八部隊之手。
北京當局對這些指控矢口否認，並宣布加強對美國科技業者的審查以茲報復。CrowdStrike說：「既然中共辯駁這一切都是捏造的，我們就想說不如公布他們無法否認的內容。」

CrowdStrike調查發現，雖然六一四八六部隊利用透過他國網站實施攻擊以隱藏蹤跡，但仍留下包括攻擊者身分與所在位置等痕跡，其中含有與六一三九八部隊成員相同的IP地址。六名接受《紐時》採訪的現任與退役美國國安局官員，也證實這些駭客的身分是六一四八六部隊。

CrowdStrike指出，名為「陳平」（Chen Ping，音譯）的人士登記了數個網域名稱，正好是用在部分網攻行動的網域。陳平的「微博」資料寫著年齡三十五歲，職業是軍人。CrowdStrike在他的網路相簿中，發現他參與軍事訓練、與身著軍裝朋友慶生等照片。在一本名為「辦公室」的相簿中，出現一棟位在上海的白色大樓。

《紐時》實地走訪該處發現，該大樓有士兵管制戒備森嚴，裝有鐵絲網的高牆外，還有一道護城河。牆內茂密的樹林，遮不住軍事衛星訊號接收器的蹤影。

美國與中共近年來因網路間諜活動關係緊張，部分美國官員認為，就算公開指控共軍駭客，他們也不可能踏入美國法庭，反而使得與中共的交涉更加困難。

更完整訊息，請參閱：
http://news.gpwb.gov.tw/news.aspx?ydn=026dTHGgTRNpmRFEgxcbfVEV3cQibTDk%2f3zFY4u8tBdAIED8ilUlDamO%2bBjjNxSe%2fZakVsXEmcWxEx5JzWtjTXJjMfL5zbmXS9nASaUMrKw%3d