

# 騎劫家居裝置 大規模攻擊美伺服器 黑客「物聯網」播毒 癱瘓科網巨企

美國大選屢傳遭黑客干預之際，全球最大網絡服務供應商之一 Dyn 前日多次遭受大規模「分散式阻斷服務」(DDoS)攻擊，導致多個使用 Dyn 服務的網站癱瘓，包括 twitter、亞馬遜、eBay、Paypal、Spotify、Netflix 等大型科網企業。黑客組織稱是要為「維基解密」創辦人阿桑奇被禁止上網報復。今次網攻的特別之處，在於黑客騎劫數以萬計智能家居網絡裝置來向 Dyn 施襲，使「物聯網」變成播毒網絡。

位於美國東岸的 Dyn 透過官方網站發表聲明，證實旗下域名伺服器先後遭受三波 DDoS 攻擊。第一波始於當地時間早上 7 時，主要影響美東用戶，服務在約兩小時後恢復正常；同日中午左右，黑客再發起第二及第三波攻擊，攻擊來源「更全球化」，伺服器要到當晚 6 時左右才恢復運作，襲擊範圍擴至美國西岸以至歐洲的用戶。亞馬遜旗下的亞馬遜網絡服務公司亦表示，它的網絡服務在當日幾乎同一時間遭受攻擊。

## twitter 戶無法發帖 Paypal 停交易

除了科網企業之外，《紐約時報》、美國有線新聞網絡、網上論壇 Reddit 等運作同告受阻。襲擊波及各類網絡活動，twitter 及 Paypal 等用戶無法發帖、登入網站、下載檔案、看影片、玩網絡遊戲，以及進行零售和金融服務交易。零售業擔心，若攻擊發生在感恩節購物季期間，將嚴重衝擊業績。報道指，黑客控制大量網絡鏡頭和嬰兒監視器等家居聯網設備，再指令它們集體向目標發動 DDoS 攻擊。美國國土安全部和聯邦調查局(FBI)展開調查，暫未知幕後黑手身份。有報道引述高級情報官員指，今次攻擊屬典型網絡破壞行為，相信並非外國政府主導。

## 黑客組織稱為阿桑奇被斷網報復

黑客組織「新世界黑客」在 twitter 上為攻擊承認責任，宣稱是要為阿桑奇報復。「維基解密」近日公開大量不利美國民主黨總統候選人希拉里選情的外洩電郵，導致藏身厄瓜多爾駐英國大使館的阿桑奇被厄方限制上網。「維基解密」呼籲黑客停止攻擊，認為黑客「已表達主張」，又批評美國政府不應利用國家機器阻止對候選人的批評。「新世界黑客」兩名成員透過 twitter 與美聯社通訊，兩人宣稱組織成員大多來自俄羅斯、中國及印度等地，又指組織無意針對美國，今次「只是小試牛刀」，又指攻擊凸顯了網絡保安漏洞，形容自己是在「做好事」。美聯社報道，「新世界黑客」過去曾承認攻擊 ESPN 及英國廣播公司(BBC)網站，並宣稱曾對「伊斯蘭國」(ISIS)發動網絡攻擊。 ■美聯社/法新社/路透社/Politico 網站

## 改襲上游伺服器 恐爆全球性攻擊

近年企業網站屢遭網絡攻擊，但有別於黑客過往主要針對企業本身的伺服器，黑客今次攻擊用於配對網絡域名及 IP 地址的域名伺服器，透過攻擊上游設施，癱瘓下游所有網站。知名電腦保安專家施奈爾警告，過去一兩年類似攻擊愈來愈多，而且規模及複雜性日漸增加，警告網絡攻防戰正趨白熱化。

無意義數字組成的 IP 地址。有專家用地圖及商店比喻 DNS 及網站，黑客攻擊 DNS 就等同撕毀了地圖，雖然商店仍正常運作，但客人卻因為不知店舖位置而無法順利前往。施奈爾指出，近年針對 DNS 等網絡基礎的攻擊愈來愈多，當中不少屬試探性攻擊，即黑客透過不同力度及形式的攻擊，試圖找出網絡保安系統的弱點。施奈爾形容這就像冷戰時期，美軍會派軍機飛越蘇聯領空，迫使對方啟動防空系統，以試探對方的防空能力，懷疑黑客組織正密謀發動更大規模的全球性網絡攻擊，呼籲各國提高警覺。 ■《紐約時報》/《華爾街日報》

## 如遊客失地圖 無法往商店

今次受攻擊的 Dyn 負責提供域名系統(DNS)服務，它就像一本電話簿，儲存了網址及相對應的 IP 地址，讓人們可用易於記憶的網址便能前往想登入的網站，毋須記住由

「Mirai」上月曾攻擊知名電腦保安專家克雷布斯的網站，黑客組織於本月初在網上公開「Mirai」的程式碼，吸引大批黑客下載，專家擔心類似攻擊今後或陸續有來。暫時未知「Mirai」是由誰人研發，「Mirai」一字在日文意指「未來」，而公開程式碼的用戶也利用一個日本動漫角色作為頭像。 ■《衛報》

## 網絡鏡頭保安弱 淪網戰武器

黑客以往一般利用大量受到惡意程式感染的電腦，組成龐大的殭屍網路(botnet)發動 DDoS 攻擊，但電腦專家發現，在今次針對 Dyn 的攻擊中，參與攻擊的裝置大部分是網絡鏡頭及數碼攝影機。專家指，近年愈來愈多電子裝置具備上網功能，但他們的網絡保安功能脆弱，容易被黑客入侵，淪為網戰武器。

## Mirai 程式專門入侵

網絡保安公司 Flashpoint 相信，今次攻擊牽涉一款名為「Mirai」的惡意程式，它能夠入侵閉路電視、網絡鏡頭、數碼攝影機、路由器等裝置，容許黑客遠距操控發動攻擊。跨國電訊服務商 Level 3 Communications 估計，全球有近 50 萬部裝置受到「Mirai」感染，其中 29% 位於美國，比例是全球最多。

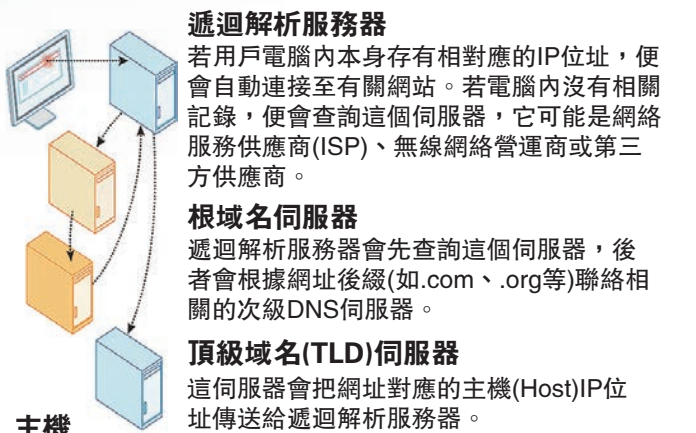
「Mirai」上月曾攻擊知名電腦保安專家克雷布斯的網站，黑客組織於本月初在網上公開「Mirai」的程式碼，吸引大批黑客下載，專家擔心類似攻擊今後或陸續有來。暫時未知「Mirai」是由誰人研發，「Mirai」一字在日文意指「未來」，而公開程式碼的用戶也利用一個日本動漫角色作為頭像。 ■《衛報》



■ Mirai 惡意程式能夠入侵網絡鏡頭，讓黑客遠距操控發動攻擊。

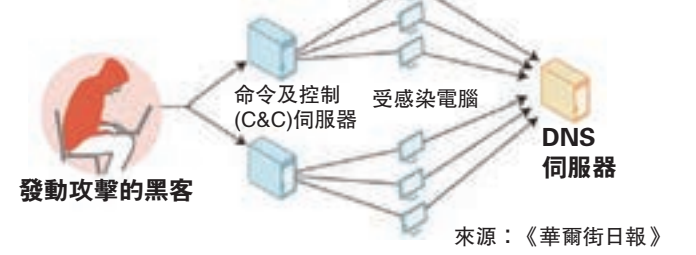
## DNS 伺服器支撐互聯網運作

每個網址都會有相對應的 IP 位址，DNS 伺服器負責把兩者配對起來。假設有用戶想在家中用電腦上網，並在網絡瀏覽器內鍵入「favoritesite.com」：



遞迴解析伺服器 若用戶電腦內本身存有相對應的 IP 位址，便會自動連接至有關網站。若電腦內沒有相關記錄，便會查詢這個伺服器，它可能是網絡服務供應商(ISP)、無線網絡營運商或第三方供應商。 根域名伺服器 遞迴解析伺服器會先查詢這個伺服器，後者會根據網址後綴(如.com、.org等)聯絡相關的次級 DNS 伺服器。 頂級域名(TLD)伺服器 這伺服器會把網址對應的主機(Host)IP 位址傳送給遞迴解析伺服器。

分散式阻斷服務(DDoS)攻擊 DDoS 攻擊牽涉黑客操控大量受感染電腦，同時向目標發送大量查詢要求，導致目標伺服器負荷過重，使得其他用戶無法享用服務。



來源：《華爾街日報》

## 美恐黑客狙擊大選日

距離美國總統大選投票日只有半個月左右，有政治評論員擔心今次攻擊只是前奏，黑客可能正準備在投票日發動規模更大的網絡攻擊。目前美國 31 個州及哥倫比亞特區

允許海外軍人及僑民在網上投票，選舉科技顧問西莫斯擔心，一旦黑客針對投票系統發動 DDoS 攻擊，可能導致大量選民無法投票，在選情緊湊的搖擺州影響尤其顯著。 ■《紐約時報》

## 特朗普「結案陳詞」 談執政百日大計

美國共和黨總統候選人特朗普因為接連捲入醜聞，選情流血不止，他定於當地時間昨早在賓夕法尼亞州蓋茲堡發表演說，闡述上任總統後首 100 天的執政大計及願景。特朗普競選團隊形容，這次演說將是他本屆大選對選民的「結案陳詞」。

說會在「特別的地方度過特別的一天」。蓋茲堡對共和黨別具意義，該黨首位總統林肯 1863 年便是在此發表著名的《蓋茲堡演說》，但特朗普與林肯發表演說的地點並不相同。 特朗普前晚在賓夕法尼亞州拉票時又表示，一旦當選總統，便會在賓夕法尼亞州等地建造 3 艘新戰艦，並承諾會採用「美國鋼鐵」。



■ 特朗普希望透過闡述願景展示正面形象。 美聯社

特朗普在競選期間傾向貶低美國現狀，又多次警告美國前景堪憂，給予外界黑暗及負面的形象。特朗普團隊透露，他在演說中會採取另一風格，希望透過闡述願景展示正面印象，預料演說內容會集中國家安全、法律與秩序、就業、貿易政策、改革、經濟刺激措施等話題，貫徹他的競選主軸。

希拉里總部收粉未信 一度疏散 民主黨總統候選人希拉里位於紐約布魯克林的競選總部，昨日收到含有可疑白色粉末的信件。警方接報到場後疏散總部內的人，經初步檢查證實粉末並無傷害性，正調查屬於什麼物質，以及發送者的身份。 ■法新社/彭博社/美國有線新聞網絡

## 擬建 350 戰艦 承諾用美鋼鐵

特朗普前晚接受霍士新聞訪問時，拒絕披露更多有關演說的詳情，只實關于

## fb 放寬審查 新聞價值先行

全球不少網民透過社交網站 facebook(fb)分享新聞及圖片，令 fb 具備媒體功能，但創辦人朱克伯格一直不承認 fb 是「媒體公司」。在各界呼籲下，fb 前日終於決定放寬審查尺度，容許「具新聞價值」的圖片在頁面上出現。有分析認為，fb 已正式採納傳統新聞業的編輯準則，以新聞價值為先，意味朱克伯格已成為全球最具影響力媒體的「總編輯」。

## 朱克伯格拒刪特朗普排外言論

fb 過去的審查標準引起不少爭議，最轟動是早前以涉及兒童色情為由，刪除挪威報章發佈的「燒夷彈女孩」經典越戰照片。fb 其後承諾與發佈者會晤，探討在「表達自由」及「保障社區安全」之間取得平衡。有意見認為，雖然 fb 仍未詳細披露將來如何作出編輯決定，但相比以往較保守的做法，今次已屬一大進步。 《華爾街日報》報道，fb 員工早前曾試圖刪除美國共和黨總統候選人特朗普在 fb 發佈禁止穆斯林入境的言論，但遭朱克伯格否決。雖然朱克伯格承認有關言論違反 fb 禁止仇恨言論的準則，但認為「這可能是上任美國總統言論一個重要部分」。 ■《衛報》/《華爾街日報》