回顧 Pawn Storm 二年來的發展

審視這項日益嚴重的威脅

Feike Hacquebord

趨勢科技前瞻威脅研究 (FTR) 團隊

A TrendLabs℠ 研究報告

趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

內容

Pawn Storm 是一個近年來相當活躍、積極、且野心勃勃的網路間諜團體。從該團體的活動即可看出其成立的宗旨主要是從事國內、外網路間諜活動以及影響各地的政治局勢，而非以營利為目的。其攻擊的目標大多為軍事單位、國防機構、新聞媒體、政治團體以及異議分子。

Pawn Storm 的行動最早可追溯至 2004 年[1]，而且在我們 2014 年發表業界第一份 Pawn Storm 相關報告之前[2]，網路上並無太多關於該團體的資料。在第一篇之後，我們又陸續發表了十幾篇 Pawn Storm 的詳細介紹[3]。本文將對該團體的攻擊案例和手法做一番整理和回顧，希望能藉此讓企業更全面地掌握歹徒的做案模式，以及如何加以防範。

Pawn Storm 已成為當今一項日益嚴重的威脅，尤其該團體不再只是單純地從事網路間諜活動。在 2016 年間，該團體曾試圖影響大眾輿論、操弄選情，並且成功地和主流媒體搭上線。目前，全球各大產業和企業都已開始感受到其惡意活動的影響力。在許多國家，就連一般人民都能感受到其威脅，因為 Pawn Storm 會試圖操弄大眾對於國內、外事件的看法。Pawn Storm 甚至已成為其他犯罪團體效法的對象，紛紛仿效其作法來達成各種不同目的。

回顧 Pawn Storm 過去兩年來的活動，我們可以看出該團體越來越懂得利用其竊取到的情報進行剝洋蔥式的爆料，藉此操弄某些事件和大眾輿論。其許多行動都引起了軒然大波，例如美國民主黨全國代表大會 (Democratic National Convention) 遭駭的事件。該團體的網路宣傳手法，也就是透過電子媒體來影響輿論[4]，已經對社會許多層面造成了影響。除了操弄社會大眾之外，該團還會刻意抹黑特定政治人物，或是癱瘓知名媒體。2017 年，不實的新聞與指控如滾雪球般出現，一部分的原因就是歹徒刻意在背後爆料。有媒體已出面證實 Pawn Storm 曾經提供他們獨家爆料情報，其動機很可能是為了扭曲社會大眾對某些特定議題或人物的看法。

在這份報告當中，我們詳細分析了目前所蒐集到的資料，深入剖析該團體所用的各種不同攻擊手法。Pawn Storm 最為人所知的就是高明的社交工程誘餌、高效率的帳號登入憑證網路釣魚、零時差攻擊、獨門漏洞攻擊套件、強大的惡意程式庫、化名行動、以及為了影響政治局勢而操弄輿論的行動。

Pawn Storm 又名 Sednit[5]、Fancy Bear、APT28[6、7]、Sofacy 以及 STRONTIUM[8]，但基本上仍是一個網路間諜團體。他們通常會利用多種管道以及多種方法來試圖入侵同一個目標以達成目的。歹徒大多使用他們所熟悉的技巧，尤其是網路釣魚。Pawn Storm 近年來的許多攻擊，主要都是靠著網路釣魚技巧來騙取受害者的帳號登入憑證，趨勢科技自 2014 年即率先針對該團體進行詳細剖析。

本文第一部分先分析該團體所從事過的一些化名行動，說明 Pawn Storm 如何試圖影響輿論。第二部分介紹該團體攻擊免費網頁郵件 (Webmail) 或企業網頁郵件信箱的各種手法，這絕大多數都是透過精密的網路釣魚技巧。第三部分詳細說明我們這幾年來所追蹤到的一些 Pawn Storm 攻擊行動以及他們所攻擊的目標。緊接著說明他們所偏愛的攻擊方式、共犯，及其所做的安全措施。最後，本文提供了一些原則來教您如何防範 Pawn Storm 攻擊行動。

化名行動

Pawn Storm 會運用各種不同的技巧來滲透其攻擊目標並蒐集資訊，最常見的手法就是登入憑證網路釣魚詐騙。此外，歹徒會將偷來的資訊拿到一些專門交流竊取資料的網站爆料。Pawn Storm 已不止一次偽裝成懷有特定動機的「駭客激進分子」或爆料者。

多重面具

2016 年，就在 Pawn Storm 成功入侵世界反禁藥組織 (World Anti-Doping Agency，簡稱 WADA) 與國際體育仲裁院 (Court of Arbitration for Sport，簡稱 TAS-CAS) 之後，一個自稱為「Fancy Bears」的駭客團體便在其網站上張貼了一些運動員的醫療記錄 (因此資安廠商 CrowdStrike 使用「Fancy Bear」這個名字來稱呼 Pawn Storm 駭客團體)。該團體宣稱他們是為了支持「公平而乾淨的運動競賽」而站出來，但事實上，他們所公開的私密醫療記錄很可能就是 Pawn Storm 所偷來的。這項舉動可能是為了報復 WADA 在 2016 年巴西里約奧運對多名運動員祭出禁賽的懲罰。也或許這是為了弱化 WADA 的地位，影響大眾對禁藥事件的看法。

2015 年，美國陸軍的一些情報被一群自稱為「Cyber Caliphate」的駭客公布在 cyb3rc.com 網站。該團體以伊斯蘭國 (ISIS) 支持者的姿態出現，並意指自己為一個伊斯蘭恐怖主義團體。同年，Cyber Caliphate 也宣稱成功癱瘓了法國 TV5 電視台實況廣播達數小時之久。其支持伊斯蘭國的訊息也出現在 TV5 電視台的 Twitter 和 Facebook 網頁上。此事件對於尚未走出《查理周刊》(Charlie Hebdo) 恐攻陰影的法國來說，尤其是一項沉重打擊。不過，沒過多久 Cyber Caliphate 就被人發現其實就是 Pawn Storm。

法國雜誌《L'Express》提出一些特徵證明 Cyber Caliphate 和 Pawn Storm 明顯有所關聯，隨後法國官方也出面證實這點。TV5 電視台攻擊背後的動機至今仍令人不解。當然，此事件也有可能是 Pawn Storm 當中一些不受控制的分子所為。儘管 Pawn Storm 的行動通常都很有紀律，但過去也曾出現某些 Pawn Storm 分子出現脫軌的行動。

針對政治團體採取行動

2016 年美國民主黨全國委員會 (Democratic National Committee，簡稱 DNC) 據稱遭到 Pawn Storm 入侵，一些遭到竊取的電子郵件隨後外流到維基解密 (WikiLeaks) 網站以及「dcleaks.com」網站，該網域很可能屬於 Pawn Storm 所有。就在 DNC 遭駭事件公開之後，一個名為「Guccifer 2.0」的個人駭客出面自稱發動了這項攻擊。Guccifer 2.0 自稱是一位羅馬尼亞人 (這一點與駭客 Guccifer 相同，此駭客在 2016 年因入侵美國企業高階主管、政治人物和名人的電子郵件帳號而遭判刑)，但是當他與媒體聯絡時卻顯然羅馬尼亞話不太靈光。

根據 ThreatConnect 所做的一份研究顯示[9]，Guccifer 2.0 主動找上新聞媒體並獨家提供密碼給媒體存取 dcleaks.com 網站上用密碼鎖住的內容。該網站確實洩漏了一些來自 Pawn Storm 美國主要攻擊目標的電子郵件內容，其攻擊主要手法就是利用精密的 Gmail 帳號登入憑證網路釣魚。我們蒐集了不少 Pawn Storm 從 2014 年至今許多 Gmail 登入憑證網路釣魚攻擊行動的相關資訊 (請參閱「Pawn Storm 如何攻擊免費與企業網頁郵件 (Webmail)」一節)。由此可見，Guccifer 2.0 很可能是 Pawn Storm 所捏造出來的人物。

此時，自稱為「跨國媒體組織暨相關資料庫」的維基解密網站公布了一些 2016 年來自 DNC 以及土耳其總統埃爾多安 (Erdogan) 所屬「正義與發展黨」(簡稱 AKP) 的電子郵件。我們知道 2016 年 3、4 月間 DNC 遭到了 Pawn Storm 一波猛烈的登入憑證網路釣魚攻擊：在競選期間，數十位政治人物、DNC 人員、演講稿執筆人員、資料分析師、前歐巴馬競選人員，甚至企業贊助者都曾經遭到多次襲擊。此外，Pawn Storm 也曾在 2016 年初對土耳其政府和國會發動網路釣魚攻擊。所以，維基解密所公布的電子郵件非常可能就是 Pawn Storm 先前所竊取的資料。

利用主流媒體

Pawn Storm 過去已有多次記錄利用主流媒體來宣傳其攻擊並試圖影響輿論觀點。許多媒體機構都已證實 Pawn Storm 曾經找上他們表示願意提供獨家新聞。2017 年 1 月，德國信譽優良的《明鏡》(Der Spiegel) 周刊在報導禁藥事件時寫道[10]，有一個叫做「Fancy Bear」的駭客團體和他們接觸了數個月，並且在 2016 年 12 月提供一批 PDF 和 Word 文件以及數百封來自美國反禁藥組織 (United States Anti-Doping Agency，簡稱 USADA) 與世界反禁藥組織 (WADA) 內部的郵件給他們。這顯然就是一個 Pawn Storm 成功利用主流媒體來影響大眾政治輿論的案例。

另一個案例是 2016 年 7 月底左右，美國民主黨國會競選委員會 (Democratic Congressional Campaign Committee，簡稱 DCCC) 遭駭的新聞。我們發現在該事件曝光之前，該網站已經遭駭客入侵長達五星期以上。所有想要捐款給 dccc.org 的人都會先被導到 Pawn Storm 所掌控的網站，也就是說，歹徒有機會駭入民主黨的贊助者。在事件爆發當時，歹徒已經入侵大約一個星期，而且還在持續活動當中。為善盡資訊安全義務，趨勢科技主動向美國主管機關通報，讓問題得以迅速獲得解決。當時我們並未將這個事件公開，因為這樣反而會讓 Pawn Storm 得利，提升他們的影響力，衝擊美國選情。只是，過了五星期之後，該事件最後還是在媒體上曝光。有可能是 Pawn Storm 主動透過主流媒體釋放這項訊息，就像其他案例一樣，他們很可能拿「獨家新聞」來當作誘因。

網路釣魚以及 Pawn Storm 如何利用偷來的資料

2016 年 4、5 月，Pawn Storm 對德國首相梅克爾 (Angela Merkel) 所領導的基督教民主黨 (Christian Democratic Union，簡稱 CDU) 發動了一波波的網路釣魚攻擊。約莫在同一期間，該團體也對德國兩家免費網頁郵件服務發動了網路釣魚攻擊[11]。德國政府後來證實這項攻擊的確是 Pawn Storm 所為。只不過不知道他們是否得逞，因為目前尚未發現有任何 CDU 的電子郵件外流，但之前也曾經發生 Pawn Storm 在過了一年之後才開始將偷來的資料外流的記錄。剝洋蔥式的爆料，是歹徒盡可能擴大影響力的一種手法。

2016 年初，Pawn Storm 也曾架設網路釣魚網站攻擊土耳其政府機關和國會[12]。2016 年 10 月有個針對蒙特內哥羅國會的登入憑證網路釣魚網站很可能也是 Pawn Storm 所為。

Pawn Storm 似乎也曾經利用 cyber-berkut.org 網站來洩漏其竊取到的資訊。該網站背後是一個偽裝成特定激進團體的駭客組織，專門洩漏來自烏克蘭政府的文件。Pawn Storm 與 CyberBerkut 之間的確切關係我們並不清楚，但我們已掌握可靠證據指出 CyberBerkut 曾經發布 Pawn Storm 網路釣魚行動所竊取到資訊。這些文件和電子郵件在公開之前似乎已經有部分遭到篡改。

因此，這批資料的真實性有待商榷，駭客很容易為了達成其目的而竄改資料並透過爆料方式來取信於人。就算不篡改資料，歹徒也可能把竊來的資料藉由斷章取義的方式，製造出對其有利的社會輿論。

從上述案例可得知 Pawn Storm 的動機主要在影響各國的政治局勢，美國總統大選只是其中一個案例。像 Pawn Storm 這樣資源雄厚的駭客集團，有能力長期從事各種行動並應用不同攻擊方法，並且利用同一種攻擊方式 (如登入憑證網路釣魚) 進行長達數年的滲透。在接下來的章節中，我們將詳細說明為何登入憑證網路釣魚對 Pawn Storm 來說非常有效。

Pawn Storm 如何攻擊免費與企業網頁郵件 (Webmail)

登入憑證網路釣魚

登入憑證網路釣魚對網路間諜行動來說是一項非常有利的犯案工具。很多網路使用者現在都已從經驗中學到教訓，因此不會輕易落入網路釣魚的陷阱。他們已經學會觀察一些明顯的拼字和文法錯誤，以及不尋常的網址連結，並且會檢查瀏覽器的網址列上是否有安全連線的圖示。不過，專業的駭客集團並不會犯下這麼明顯的錯誤，而且還能想出各種聰明的社交工程技巧。他們的網路釣魚郵件，不論是英文或其他語言，文字都非常流利，而且還能順利躲過垃圾郵件過濾軟體。

基本上，登入憑證網路釣魚攻擊已成為一項既有效又危險的工具，其後果可能相當嚴重。這類攻擊可導致大量敏感資料遭到竊取，而且還可當成歹徒進一步滲透到目標企業基礎架構的跳板。

歹徒可經由登入憑證網路釣魚達成多重攻擊目的，例如：

- 長期潛伏，暗中蒐集資料。Pawn Storm 就是一個最佳範例，根據我們的觀察，他們可以暗中蒐集資料長達一年以上。
- 經由遭到入侵的使用者帳號，滲透受害企業網路。例如利用這些被入侵的帳號發送電子郵件。
- 刻意洩漏敏感的電子郵件內容，破壞受害機構的名聲並影響大眾輿論。
- 從事國內間諜行動，監控特定國家的人民。

這些看似簡單卻精心策劃的登入憑證網路釣魚攻擊，能讓駭客團體蒐集大量資料。以上所列的每一件都是 Pawn Storm 會做的事。2016 年，該團體搜刮資料的對象包括 DNC、希拉蕊競選辦公室以及 WADA。此外，他們也針對許多其他機構發動登入憑證網路釣魚，包括軍事機構、國防企業、新聞媒體等等。

從 2015 年 7 月至 2016 年 8 月，Pawn Storm 很可能掌握了美國布希 (George Bush) 總統時期前國務卿鮑爾 (Colin Powell) 的 Gmail 電子郵件帳號。因為一年多以後 (2016 年 9 月)，dcleaks.com 網站上公布了多封鮑爾的私人電子郵件。而這只不過是 Pawn Storm 洩漏機密資料的眾多案例之一，而且證據顯示，有些案件歹徒持續入侵了相當長的時間。

俄國人民，包括：記者、軟體開發人員、政治人物、大學研究人員以及藝術家，全都曾經遭到 Pawn Storm 的攻擊[13]。許多俄國媒體機構 (包括主流媒體) 和莫斯科的外國領事館都是他們經常攻擊的目標。

許多知名人物的免費電子郵件帳號 (如 Yahoo 和 Gmail)，都是 Pawn Storm 長期鎖定的目標，此外還有烏克蘭的免費電子郵件服務 Ukr.net 以及俄羅斯的 Yandex 和 Mail.ru。除此之外，Pawn Storm 唯有在針對特定目標時才會架設其他免費電子郵件帳號的網路釣魚網頁。我們曾經發現 Pawn Storm 假冒賽普勒斯、比利時、義大利、挪威以及其他國家一些小型電子郵件服務廠商發動網路釣魚攻擊。此外，也曾發現針對愛沙尼亞和俄羅斯大學信箱使用者的攻擊。這些舉動很可能是因為 Pawn Storm 已鎖定了某個重要目標使然。

至於針對 Google、Yahoo 和 Ukr.net 重要使用者的登入憑證網路釣魚攻擊則數量相當龐大。從 2015 年初至今，我們已蒐集了數千封此類網路釣魚郵件，只是並非連續不斷。因為 Pawn Storm 有時候會暫時停止活動，等過一陣子之後再繼續。也有些被攻擊的目標一星期內會收到多次網路釣魚郵件。

針對企業網頁郵件發動登入憑證網路釣魚攻擊

對歹徒來說，企業電子郵件信箱是相當重要的攻擊管道，因為電子郵件本來就是企業防禦最弱的環節之一。過去四年來，Pawn Storm 針對許多企業的電子郵件信箱發動了無數次的登入憑證網路釣魚攻擊。其攻擊的目標遍及全球軍事機構、國防工業、政治團體、非政府組織 (NGO)、新聞媒體以及政府機關。一旦能夠入侵企業機構的電子郵件信箱，歹徒就能取得各種珍貴機密資料，而且可以當成進一步滲透目標機構的跳板。

許多機構都允許員工在離開辦公室之後還能透過網頁介面閱讀工作上的電子郵件。雖然這給使用者帶來很大的方便，但網頁郵件卻可能引來嚴重風險。由於使用者不論從任何地方都能連上網頁郵件，因此歹徒不僅能夠直接試圖猜測密碼來入侵電子郵件信箱，而且還可能運用社交工程技巧來騙取帳號密碼。儘管人們現在對一些較不高明的網路釣魚都能輕易分辨，但真正高明的駭客卻屢出奇招，而且通常外語相當流利。所以在某些情況，也不能完全怪罪受害者上當，因為這些網路釣魚郵件幾乎很難辨別真偽。其中一種非常高明的社交工程技巧就是所謂的「Tabnabbing」(分頁置換攻擊)，後面會詳細說明。

網頁郵件有幾項重要的資安考量：

- 雙重認證確實可提升安全性，但仍無法完全防範社交工程攻擊。所有臨時的認證碼都有可能被駭客攔截。
- 就算使用了雙重認證，駭客只要能夠成功騙取到一、兩次第二認證碼，就能短暫地進入信箱。他們可設定轉寄地址，或者取得可讓第三方應用程式存取帳號的認證碼。
- 企業若硬性規定必須透過 VPN 才能從外部連上企業網路，確實能發揮遏阻作用。但是，歹徒也可能利用網路釣魚來騙取 VPN 登入憑證，我們就看過以騙取 VPN 登入憑證為目標的針對性攻擊。
- 透過實體密碼鎖來認證，就可幾乎完全杜絕登入憑證遭到網路釣魚騙取，除非駭客實際拿到受害者的認證裝置。當企業採用實體密碼鎖時，駭客就只能設法找到認證機制的漏洞，或是偷到受害者的實體密碼鎖和筆記型電腦。
- 除了使用登入憑證的認證方法之外，還有使用生物特徵的認證方法，例如：指紋、虹膜等等。此方法在資料中心門禁系統上的應用已有十年以上的歷史，近來許多筆記型電腦和手機也開始配備生物特徵認證功能。

網路釣魚攻擊目標

本節列出一些曾經遭到 Pawn Storm 攻擊的案例，在某些案例當中，歹徒只挑選了少數特定的員工。

日期	機構	網路釣魚頁面網域
軍事單位		
2013/12/12	智利軍方	mail.fach.rnil.cl
2014/5/15	亞美尼亞軍方	mail.rnil.am
2014/10/23	拉脫維亞軍方	web.mailmil.lv
2015/2/25	羅馬尼亞軍方	fortele.ro
2015/3/25	丹麥軍方	webmail-mil.dk
2015/3/26	葡萄牙軍方	webmail.exerclto.pt
2015/5/13	希臘軍方	webmail-mil.gr
2015/9/4	丹麥軍方	fkit-mil.dk
2015/9/5	沙烏地阿拉伯軍方	mail.rsaf.qov.sa.com
2015/10/16	阿拉伯聯合大公國軍方	mailmil.ae
2015/10/19	科威特軍方	mail.kuwaitarmy.gov-kw.com
2015/10/21	羅馬尼亞軍方	mail-navy.ro
2016/3/4	保加利亞軍方	mail.armf.bg.message-id8665213.tk
國防部		
2014/1/23	保加利亞國防部	mail.arnf.bg
2014/2/11	波蘭國防部	poczta.mon.q0v.pl
2014/4/4	匈牙利國防部	mail.hm.qov.hu
2014/4/30	阿爾巴尼亞國防部	mod.qov.al
2014/5/22	西班牙國防部	mail.mod.qov.es
2014/11/18	阿富汗國防部	mail.mod.qov.af
2015/9/5	沙烏地阿拉伯國防部	mail.moda.qov.sa.com
2016/2/19	波蘭國防部	poczta.mon-gov.pl
外交部		
2015/3/17	南喬治亞外交部	email.mfa.qov.gs
2015/7/16	亞美尼亞外交部	webmail-mfa.am
2015/10/2	阿拉伯聯合大公國外交部	webmail.mofa.qov.ae
2015/10/2	阿拉伯聯合大公國外交部	webmail.mfa.qov.ae
2015/12/10	卡達外交部	mail.mofa.g0v.qa

日期	機構	網路釣魚頁面網域
情報單位		
2014/1/10	保加利亞國安局	dansa.bg
國防產業		
2014/4/24	Academi	mail.academl.com
2014/4/24	Boston Dynamics	mail.bostondynamlcs.com
2014/8/11	Science Applications International Corporation (SAIC)	webmail-saic.com
2014/9/10	Polski Holding Obronny	mailpho.com
新聞媒體		
2014/11/1	New York Times	privacy-yahoo.com
2014/12/1	New York Times	link.candybober.info
2015/1/22	Buzzfeed	account.password-google.com
2015/6/22	The Economist Intelligence Unit	accounts.g00qle.com
2015/8/24	Sanoma Media	mobile-sanoma.net
2016/2/24	Hurriyet	posta-hurriyet.com
2016/3/14	Anadolu Agency	anadolu-ajansi.com
2016/3/15	Anadolu Agency	mail.anadoluajansi.web.tr
2016/5/11	Hurriyet	webmail-hurriyet.com
2016/6/12	Hurriyet	mail-hurriyet.com
2016/11/14	Al Jazeera	account-aljazeera.net
2016/11/14	Al Jazeera	ssset-aljazeera.net
2016/11/15	Al Jazeera	sset-aljazeera.net
2016/11/16	Al Jazeera	sset-aljazeera.com
2016/11/21	Al Jazeera	mail-aljazeera.net
政治團體		
2015/3/1	National Democratic Institute	url.googlesetting.com
2015/4/1	National Democratic Institute	login.accoounts-google.com
2016/1/12	土耳其總理	e-post.byegm.web.tr
2016/1/12	土耳其總理	mail.byegm.web.tr
2016/2/1	土耳其總理	eposta.basbakanlik.qov.web.tr
2016/2/1	土耳其國會	e-posta.tbmm.qov.web.tr
2016/3/1	美國民主黨	myaccount.google.com-securitysettingpage.gq

日期	機構	網路釣魚頁面網域
2016/4/1	美國民主黨	myaccount.google.com-changepasswordmyaccount-idx8jxcn4ufdmncudd.gq
2016/4/22	德國基督教民主黨 (CDU)	webmail-cdu.de
2016/5/6	德國基督教民主黨 (CDU)	support-cdu.de
2016/6/6	美國民主黨	actblues.com
2016/10/20	蒙特內哥羅國會	mail-skupstina.me
2017/3/15	法國總統馬克宏競選團隊	onedrive-en-marche.fr
2017/4/5	德國艾德諾基金會	kasapp.de
宗教		
2015/6/19	東正教美國教會	accounts.g00qle.com
學術機構		
2016/3/4	愛沙尼亞塔爾圖 (Tartu) 大學	mail.university-tartu.info
2016/9/13	俄羅斯貝加爾 (Baikal) 州立大學	mail-isea.ru
政府機關		
2015/5/24	蒙特內哥羅政府	mail-gov.me
2015/9/14	荷蘭安全局 (Safety Board)	vpn.onderzoekraad.nl
2015/9/28	荷蘭安全局 (Safety Board)	sftp.onderzoekraad.nl
2015/9/29	馬來西亞民航局 (Department of Civil Aviation)	mail.dca.qov.my
2015/11/3	蒙特內哥羅政府	mail.g0v.me
能源產業		
2014/12/10	Westing House Nuclear	webmail.westinqhousenuclear.com
國際組織		
2014/6/18	歐洲安全與合作組織 (OSCE)	login-osce.org
2015/4/23	Partnership for Peace Information Management System	mail-pims.org
2016/8/3	世界反禁藥組織 (World Anti-Doping Agency，簡稱 WADA)	mail.wada-awa.org
2016/8/8	世界反禁藥組織 (World Anti-Doping Agency，簡稱 WADA)	inside.wada-arna.org
2016/8/8	國際體育仲裁院 (Tribunal Arbitral du Sport，簡稱 TAS)	tas-cass.org

表 1：曾經遭到攻擊的組織機構以及相關的假冒網站。

Tabnabbing 登入憑證網路釣魚技巧

所謂的「Tabnabbing」(分頁置換攻擊) 是一種由資安研究人員「Aza Raskin」首次提出的網路釣魚技巧[14]。根據他的說明，此攻擊手法會利用一個簡單的 JavaScript 程式碼在瀏覽器開啟新的分頁或停在某個分頁很久之後，暗中將網址改到網路釣魚的頁面。若使用者若以為這新的網頁是其網路服務的登入頁面，那就很可能受騙上當，重新又輸入一次自己的帳號密碼。

這項技巧利用的就是網路使用者喜歡隨時保持多個分頁開啟的瀏覽習慣。但因為某些服務 (如網路銀行) 在一段時間之後會自動將使用者斷線，因此使用者也習慣很久一段時間不用之後會需要重新輸入自己的帳號密碼。

Pawn Storm 使用 Tabnabbing 的技巧已有一段時日[15]，在這種攻擊手法當中，受害者會收到假冒其可能有興趣的網站所寄來的電子郵件，例如某個他有興趣參加的研討會或是他所訂閱的新聞網站。郵件內含一個連結指向一個看起來相當正常的網址。但當收件人點選該連結時，就會開啟一個新的瀏覽器分頁。這個新的分頁會先連上某個駭客架設的網站，然後再回到的正牌網頁 (例如研討會或新聞網站)，使用者或許會在這個正牌網站瀏覽一陣子。駭客就趁使用者點選連結開啟新分頁到該網站時，暗中執行了一段更換網址的 JavaScript，將原本閱讀信件的分頁導向駭客的網路釣魚網頁。當使用者看完研討會資訊或新聞內容之後，會再回到原先看信的分頁。此時，瀏覽器會顯示連線階段已經逾時，使用者必須重新登入。使用者若不疑有他，就會重新輸入信箱的帳號密碼，而駭客便輕鬆得手。

此一攻擊手法相當簡單，而且不需利用任何軟體漏洞。駭客能否成功，就看其準備功夫是否到位，這項手法相當高明，就連有經驗的資安人員也可能不會察覺，特別是人在外面或沒有特別留意的時候。

表 2 列出一些曾經遭到 Tabnabbing 這項網路釣魚手法所詐騙的機構。

受害機構	網路釣魚頁面網域	惡意網域 (社交工程誘餌)	正牌網域
Academi	mail.academl.com	tolonevvs.com	tolonews.com
拉脫維亞軍隊	mailmil.lv	tusexpo2015.com	tusexpo.com
imperialconsult.com	mail.imperialc0nsult.com	skidkaturag.com	skidkatur.com
匈牙利國防部	mail.hm.qov.hu	aadexpo2014.co.za	adexpo.co.za
匈牙利國防部	mail.hm.qov.hu	itec2014.co.uk	itec.co.uk
匈牙利國防部	mail.hm.qov.hu	sofexjordan2014.com	sofexjordan.com

受害機構	網路釣魚頁面網域	惡意網域 (社交工程誘餌)	正牌網域
匈牙利國防部	mail.hm.qov.hu	eurosatory2014.com	eurosatory.com
西班牙國防部	mail.mod.qov.es	gdforum.net	gdforum.org
保加利亞國安局	mail.dansa.bg	counterterorexpo.com	counterterrorexpo.com
保加利亞國安局	mail.dansa.bg	novinitie.com	novinite.com
保加利亞國安局	mail.dansa.bg	standartnevvs.com	standartnews.com
OSCE	login-osce.org	vice-news.com	news.vice.com
SAIC	webmail-saic.com	natoexhibitionff14.com	natoexhibition.org
Yahoo 用戶	us6-yahoo.com	us6-yahoo.com	youtube.com

表 2：2014 年間遭到 Tabnabbing 網路釣魚技巧詐騙登入憑證的機構。

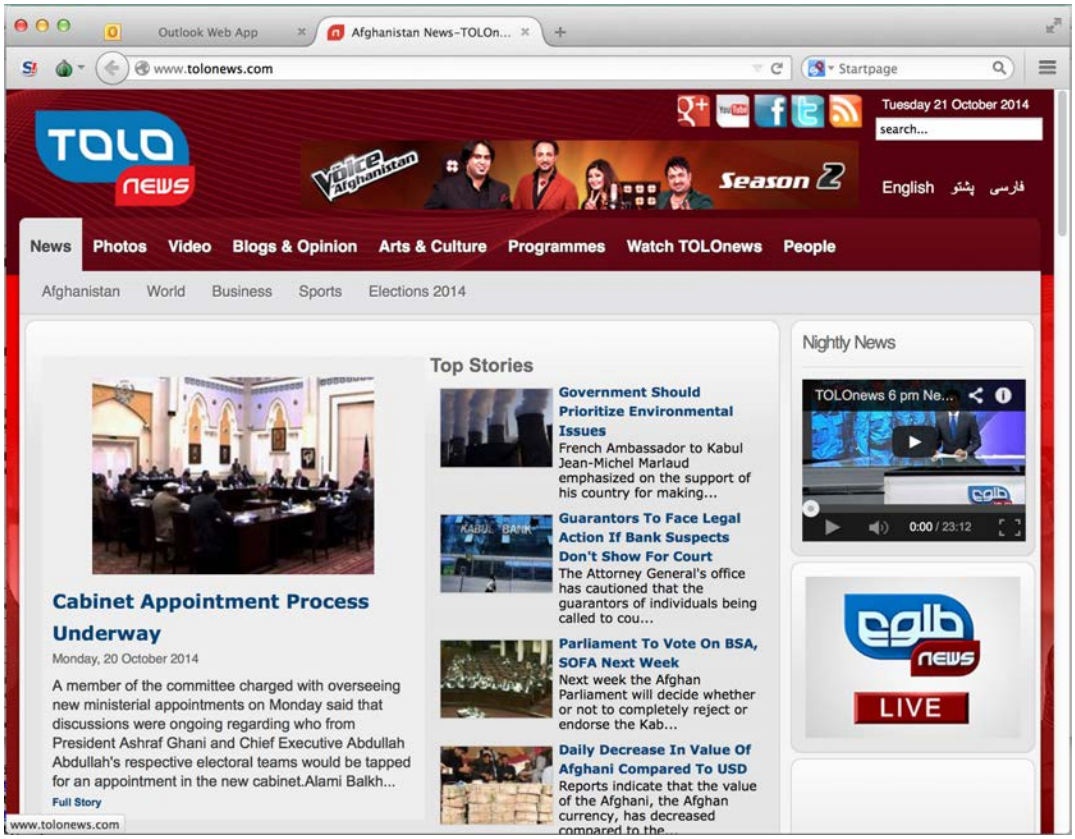

圖 1：受害者點選某個郵件中的連結，並且開啟新分頁連上某個正牌的網站。

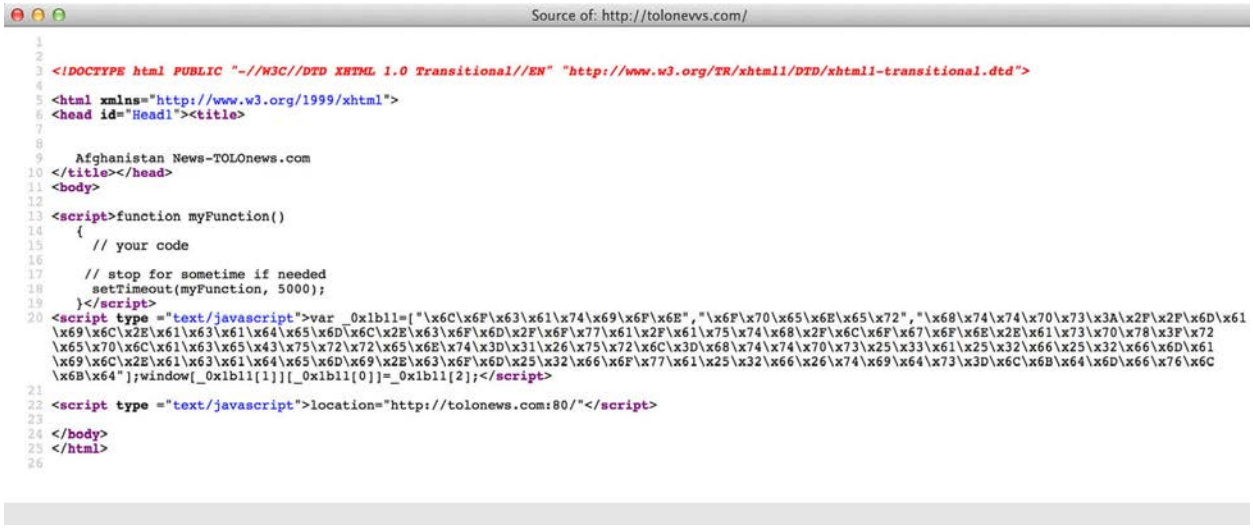

圖 2：就在新分頁連上正牌網頁之前，會先執行一段簡單的 JavaScript 讓舊分頁前往 Pawn Storm 架設的網站，然後才開啟正牌的新聞網站。

這段 JavaScript 並非惡意程式碼，它只是會將其「父視窗」(也就是原本的郵件分頁) 的網址改成指向歹徒的登入憑證網路釣魚網站。

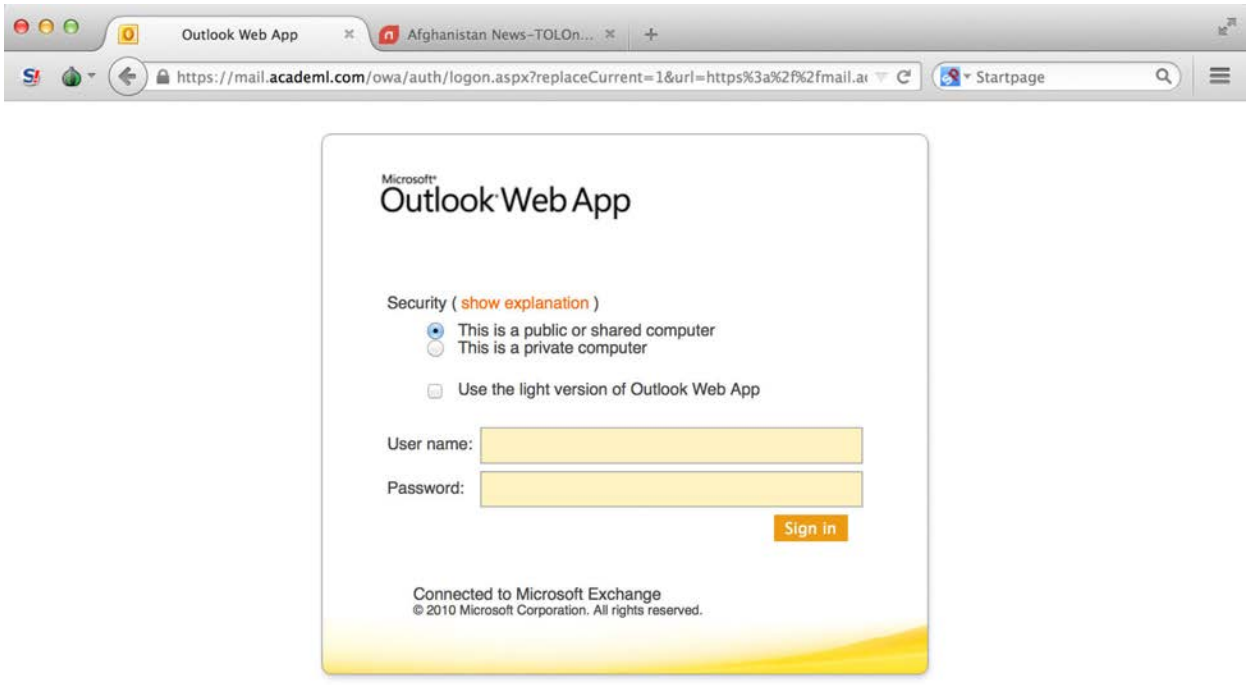

圖 3：瀏覽器分頁的網址遭調包之後顯示的網路釣魚登入頁面。

歹徒的網路釣魚登入畫面做得跟正牌的網頁郵件登入頁面幾乎完全一樣，唯一的差別只有在網域名稱上不是正牌的網域 (但沒仔細看會分辨不出來)。所以，受害者非常容易受騙上當。

篡改 DNS 設定

企業電子郵件系統所面臨的另一個簡單卻危險的攻擊情況是郵件伺服器的 DNS 設定遭到篡改，將郵件伺服器指向某個外部伺服器。這並非什麼新鮮手法，就連知名的廠商也曾發生過 DNS 設定遭到篡改的例子。通常，這是一些有個人目的或其他因素而希望獲得媒體關注的駭客所為。這類駭客入侵的情況通常很快就會被企業發現，並且很快就能修復，尤其當駭客只是希望獲得媒體關注的話。駭客大多只是在駭入的網域上放上一段「哈哈，你被駭了」之類的訊息。當然，高竿的駭客也有能力這麼做，但他們不會這麼張揚。

駭客只要取得 DNS 管理員的帳號密碼，就能修改 DNS 的 Zone File，但請注意，信譽良好的註冊機構通常會有嚴格的安全管制，DNS 系統管理員要對 Zone File 做任何修改都必須再經過電話確認。駭客只要將受害網域的 MX 記錄指向自己的代理器 (Proxy) IP 位址，就能接收所有寄到該網域的電子郵件。

該代理器可以將所有接收到的電子郵件再轉回受害者原本的電子郵件伺服器。如此一來，駭客就能讀取所有電子郵件的結構資訊 (Metadata) 及內容 (如果未加密的話)。雖然這類攻擊不算什麼高深技巧，但卻可能帶來嚴重後果。我們就曾發現某個東歐國家的外交部遭到 Pawn Storm 篡改網域 MX 記錄長達數個月之久。

當時，我們試圖將此事通報該國外交部，但過程卻困難重重。該國外交部的電子郵件通訊已不可信賴，而且我們對其電話系統的安全性也感到懷疑。因此，為了解決問題，我們用電話和歐洲電腦緊急應變小組 (CERT) 的窗口聯絡。向他們描述了當時的狀況，並且以 PGP 加密電子郵件通知 CERT 西歐總部。該單位發了一封加密電子郵件給該國大使館，大使館將電子郵件解密之後列印出來，接著再利用快遞將印出來的郵件送到該國外交部，最後終於順利解決了問題。

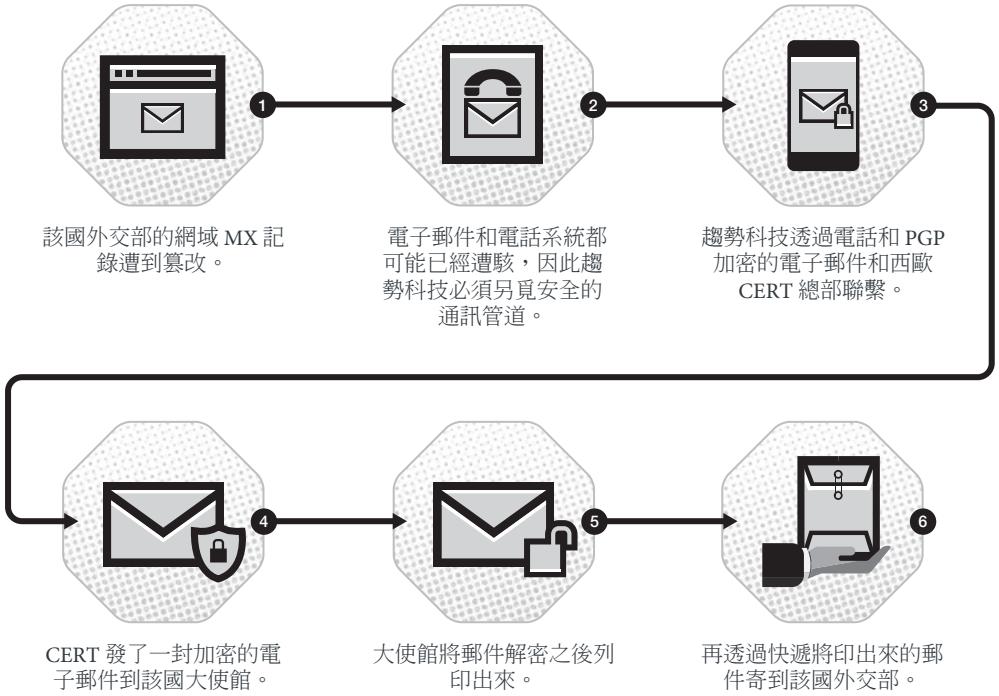

圖 4：趨勢科技通報某國外交部其電子郵件 MX 記錄遭到篡改的過程。

這類攻擊手法突顯了企業機構選擇一家信譽優良的 DNS 廠商以及網域註冊機構有多麼重要，如此才能避免自己的網域輕易遭人挾持。過去至少還有另一起同樣也是西非某國政府機構 DNS 設定遭 Pawn Storm 篡改且長達數個月的案例。

Pawn Storm 網路釣魚行動

登入憑證網路釣魚行動

Pawn Storm 無時無刻都在鎖定一些知名人士並且試圖入侵他們的免費網頁郵件信箱。該集團光是我們所掌握到的網路釣魚行動就有數十波，每一波最多可能鎖定上千位知名人士。儘管其行動當中所使用的社交工程誘餌良莠不齊，但其中有些卻特別危險。

本節將提出幾個攻擊案例來加以說明，我們蒐集了 2015 年 1 月至 2016 年 12 月之間 Pawn Storm 針對一些知名 Yahoo 帳號所散發的登入憑證網路釣魚電子郵件。我們在下圖繪製了 160 起針對 Yahoo 郵件知名用戶的登入憑證網路釣魚攻擊時間分布情況。

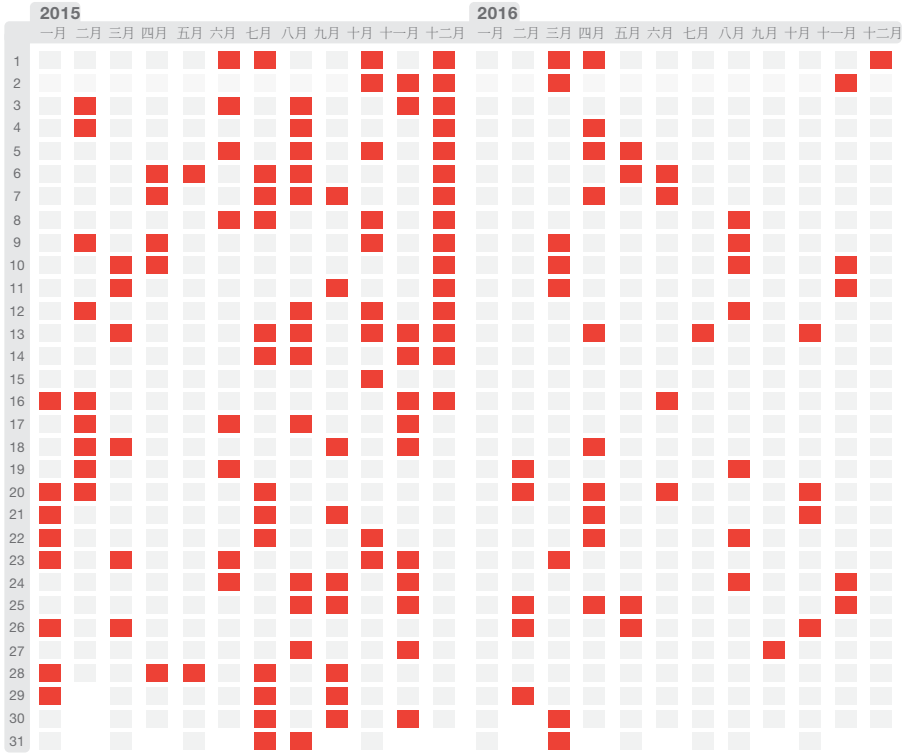

圖 5：Pawn Storm 登入憑證網路釣魚攻擊時間分布情況 (160 起)。

從圖中可以看出，Pawn Storm 在 2015 年底的年節期間休息了好長一段時間。不過，從 2015 年 11 月中至 12 月中，Pawn Storm 卻特別針對一些知名人士加強發動登入憑證網路釣魚攻擊。在這段期間，Pawn Storm 使用了一種特別危險也特別有效的登入憑證網路釣魚手法，我們在以下詳細說明。

歹徒使用了如下圖所示的一封簡單的電子郵件：

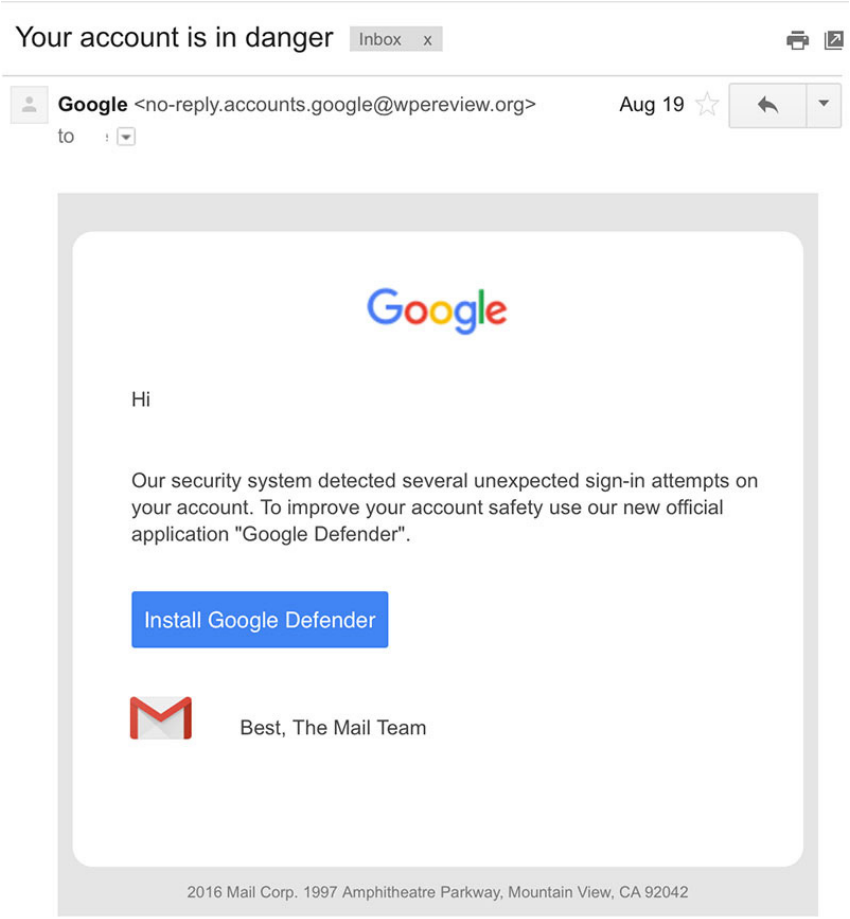

圖 6：要求安裝「Google Defender」不肖應用程式的電子郵件。

該郵件會偽裝成來自 Gmail 的安全通知，要求收件者安裝一個「官方提供的」Google Defender 帳號保護程式。通常使用者對於這類主動要求安裝的應用程式會懷有戒心，但這案例卻很特別，因為其連結點進去之後，會連上真正屬於 Google.com 的一個網頁，如下圖所示：

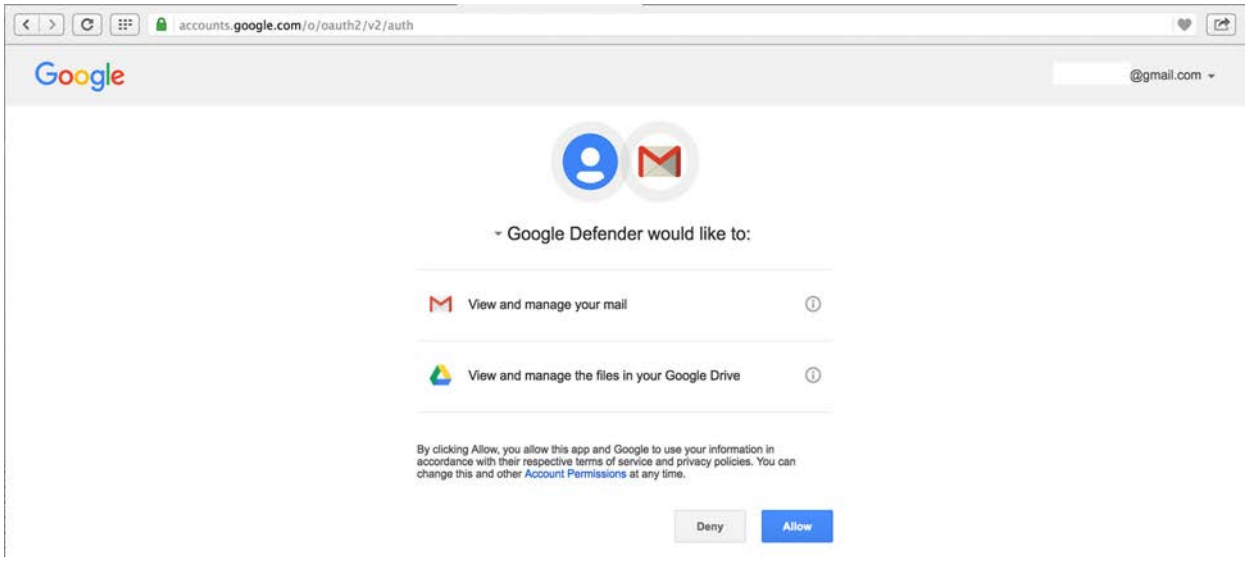

圖 7：看起來真實的網頁要求開放電子郵件存取權限給一個叫做「Google Defender」的應用程式。

從第一眼來看，這像是 Google 的某種服務，因為該網頁就在 accounts.google.com 網域之下，而且也和正常一樣使用加密連線。一般的網路使用者很可能會誤以為一切都是真的。但儘管這是 accounts.google.com 底下的網頁，要求提供權限的應用程式卻不屬於 Google 所有。它其實是 Pawn Storm 所開發的一個第三方應用程式。此攻擊是以 Open Authentication (OAuth) 開放認證機制為幌子，骨子裡卻是社交工程詐騙。後面我們會說明 OAuth 的一般用途為何。

Pawn Storm 還有一些針對 Yahoo 用戶的類似攻擊。例如 2015 年底左右就出現了一個以 McAfee Email Protection 電子郵件防護軟體為誘餌的攻擊：

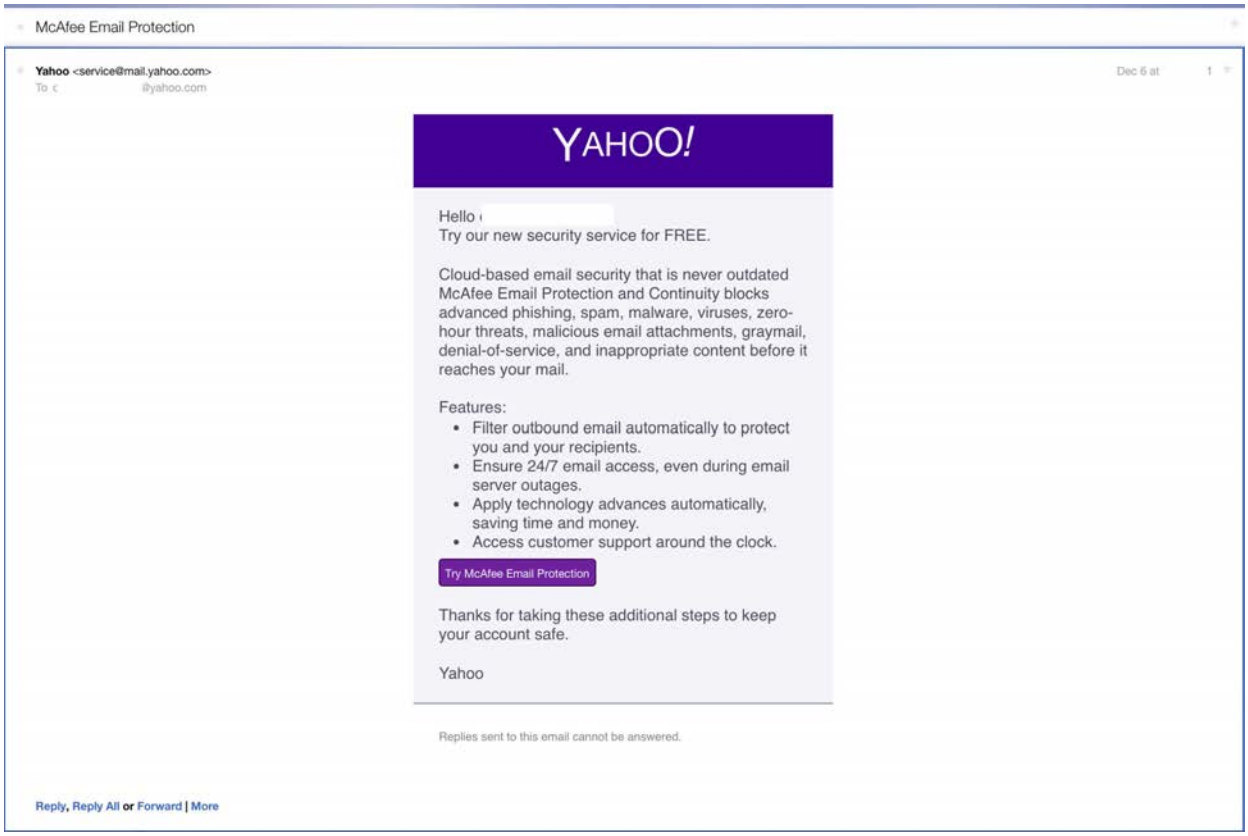

圖 8：針對知名 Yahoo 用戶的網路釣魚攻擊。

使用者若點選了網路釣魚連結，就會連上真正 Yahoo 網域 (api.login.yahoo.com) 底下的一個網頁。該網頁會詢問使用者是否要授權給「McAfee email protection」應用程式存取其電子郵件信箱。如果使用者同意，Pawn Storm 就能完全進入其信箱。

此案例的社交工程誘餌與之前 Gmail 的案例很像，這類誘餌之所以特別危險，就在於網路使用者可能不會意識到這些應用程式其實並不屬於郵件服務廠商所有，而且也未經過他們審查。

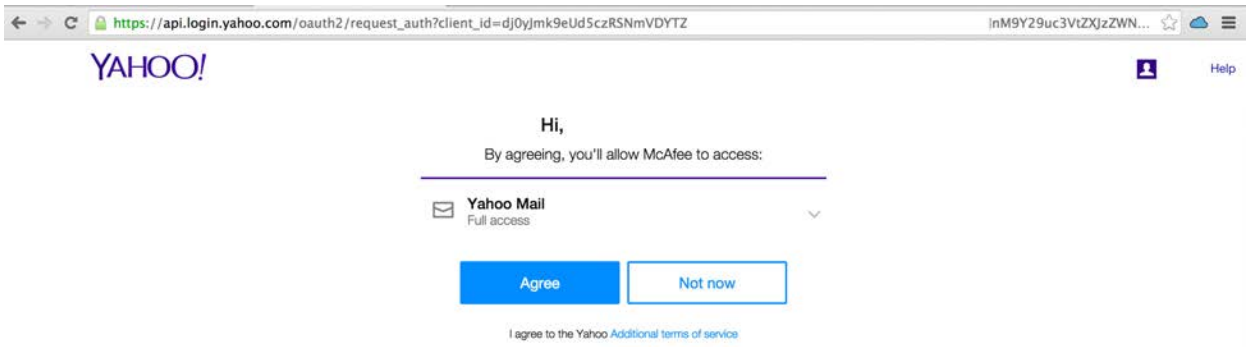

圖 9：2015 年底左右，Pawn Storm 利用 Open Authentication 開放認證機制來誘騙 Yahoo 使用者。

這項社交工程誘餌利用了 OAuth 這項開放認證機制。OAuth 是網路服務 (如電子郵件) 授權第三方應用程式存取使用者網路帳號的一種機制。此機制最大的優點是，使用者不需提供帳號密碼給第三方應用程式。而第三方應用程式拿到的是一個認證碼，利用此認證碼就能通過服務廠商的認證。

OAuth 機制確實能提升網站使用者的體驗，例如，允許社群網站存取您的網頁郵件通訊錄可以更方便找到同樣有在使用該社群網站的好友。另一個 OAuth 常見的應用是將多個免費的網頁電子郵件帳號整合在一起。

儘管 OAuth 確實能夠帶來方便性，但卻也會讓使用者暴露於危險，尤其是像前述這類高明的社交工程詐騙手法，假使服務廠商未針對使用 OAuth 機制的應用程式嚴加審查的話就更加危險。許多免費的網頁郵件服務都只要求一個電子郵件地址和一個網站，就允許第三方應用程式使用 OAuth。也正因如此，OAuth 才很容易遭到歹徒濫用，所以才會讓 Pawn Storm 這樣的駭客團體利用 OAuth 來從事登入憑證網路釣魚詐騙。

這類攻擊雖然不會騙取使用者的登入憑證，但其造成的結果卻是相同。這種手法的詐騙方式很簡單：

- 歹徒先撰寫一個不肖的應用程式並且將應用程式送給某個支援 OAuth 的網路服務供應商審查。
- 該應用程式通過網路服務供應商的基本安全審查，廠商會確認該程式是否為冒牌程式。
- 駭客開始製作電子郵件，利用前述使用 OAuth 認證的不肖應用程式為社交工程誘餌。

- 收件人或許對一般的網路釣魚郵件都已相當熟悉，但對這類利用 OAuth 機制的網路釣魚並不熟悉。即使是受過良好資安教育的使用者也很可能受騙上當。
- 一旦受害者提供了 OAuth 授權，歹徒就能隨時存取受害者的帳號，直到其取得的認證碼被撤銷為止。就算受害者變更了帳號密碼，歹徒還是能夠經由 OAuth 認證碼進入受害者的信箱。然而受害者卻可能以為更換密碼就沒事了。

我們曾經和兩家允許第三方應用程式使用 OAuth 認證的大型網頁郵件服務廠商私下反映過這項問題。其中一家後來修改了申請使用 OAuth 機制的應用程式審核程序。現在，新申請的應用程式必須通過更嚴格的審查才能使用 OAuth 機制。根據我們的觀察，Pawn Storm 從 2015 年末期之後就不再散發利用該廠商 OAuth 機制的網路釣魚郵件。Pawn Storm 又改回傳統的登入憑證網路釣魚手法，當然，這方法效率較差。

魚叉式網路釣魚行動

Pawn Storm 會試著利用含有惡意附件檔案或漏洞攻擊連結的電子郵件來對目標發動魚叉式網路釣魚攻擊。魚叉式網路釣魚電子郵件通常會以目標對象可能有興趣的近期新聞事件為誘餌。Pawn Storm 經常使用直接取自 CNN、半島電視台 (Al Jazeera)、Huffington Post、Military Times 等新聞網站上的標題。

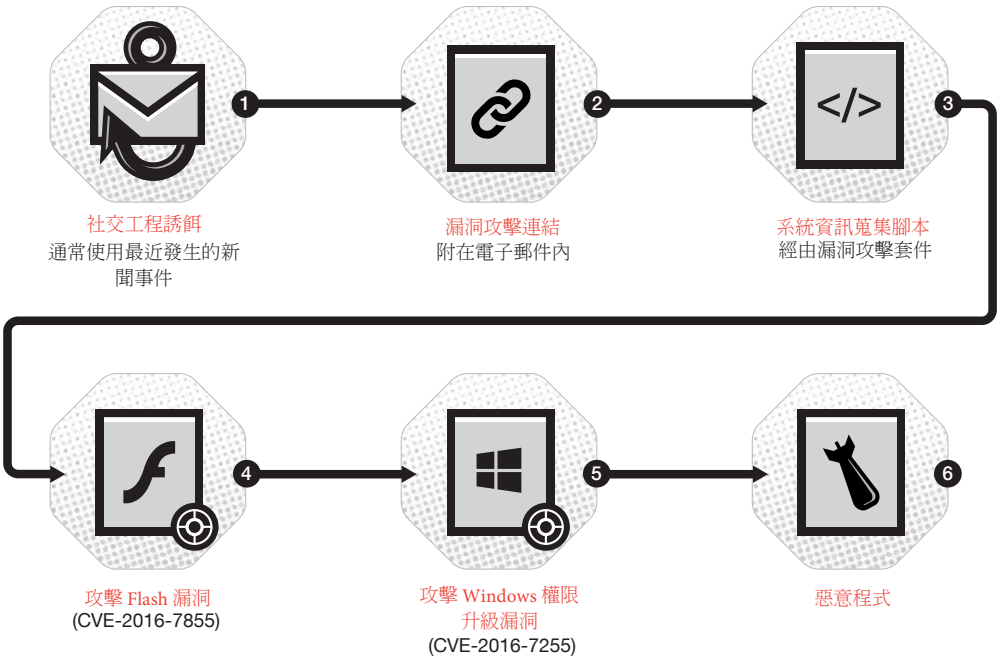

圖 10：Pawn Storm 魚叉式網路釣魚攻擊的一般流程。

在 2015 和 2016 年間，趨勢科技攔截了數十起這類針對知名人物的魚叉式網路釣魚攻擊。以下列舉一些內含 Pawn Storm 獨門漏洞攻擊連結的魚叉式網路釣魚郵件標題及日期。

日期	郵件標題
2015/2/3	Pro-Russian rebels launch new offensive
2015/3/18	NATO's role in conventional arms control
2015/3/25	Open Skies Consultative Commission
2015/3/26	News: Exercise Ramstein Dust I 2015 is underway in Italy
2015/4/1	News: Yemen air strikes kill 23 in factory: residents
2015/4/1	National Armaments Directors
2015/4/1	Heavy clashes on Saudi-Yemeni border
2015/4/6	North Korea declares no-sail zone, missile launch seen as possible - reports
2015/4/6	What does Russia's President Putin really want?
2015/4/6	Ukraine Today: Russian-backed militants appeal to Merkel
2015/4/6	Ambassador of Ukraine to Jordan Dr. SergiyPasko held talks with Director of the European Department of the MFAE of Jordan Mr. Daifallah al-Fayez
2015/4/8	Petro Poroshenko congratulated Muhammadu Buhari on his election as President of the Federal Republic of Nigeria
2015/4/15	News: Obama, in 'therapeutic' meetings with U.S. Jewish leaders, stresses how much he cares
2015/4/21	China, Japan and South Korea hold renewed talks
2015/4/22	News: Foreign Ministry denies any suspected incidence of corruption in Tunisia's embassy in Amman
2015/4/30	News: Tragedy in Nepal
2015/5/5	News: Chimerica in Decline?
2015/5/7	Diplomatic Access: The United States
2015/5/12	News: Can China and the EU Cooperate on International Security?
2015/5/13	News: Kerry: Now is 'Critical Moment' for Ukraine Conflict
2015/5/15	Russian soldiers quit over Ukraine
2015/5/20	Foreign Minister Szijjarto: NATO must respond to new threats
2015/6/17	Ambassadors RSG Wolfsbos bezoeken Europees Parlement
2015/6/19	Pew Survey: Irredentism Alive and Well in Russia
2015/7/3	For Your Information: Latest from OSCE Special Monitoring Mission (SMM) to Ukraine
2015/7/8	For Your Information: Latest from OSCE Special Monitoring Mission(SMM) to Ukraine

日期	郵件標題
2015/7/9	For Your Information: ANNUAL MEETING & EXPOSITION 12-14 October 2015
2015/7/9	Iran nuclear deal: Snapping back sanctions
2015/7/10	CNN Politics:What the Iran deal is really about
2015/7/23	NATO Won't Establish Permanent Military Bases In Poland Amid Russia Tension, US Diplomat Says
2015/8/27	Russia to increase wheat supplies to Egypt, says Putin
2015/9/8	Iraq Puts New F-16s Into Action Against ISIS Jihadists
2015/9/9	Bulgaria Bars Syria-Bound Russian Planes as NATO Fears Grow
2015/9/16	Russia gives Assad firepower, spurring US strategy adjustment
2015/9/17	Burkina Faso: an attempted coup?
2015/9/18	Croatia closes road border crossings with Serbia after migrant influx
2015/9/21	US, Russian Defense Heads Talk about Syrian Military Buildup
2015/9/21	Tsipras returns as PM in decisive Greek election
2015/9/22	Foreign Information Policy
2015/9/22	THE FIGHT AGAINST ISIS
2015/9/22	Despite Attention to Islamic State, Al-Qaida May Be Bigger Threat
2015/9/23	US military reports 75 US-trained rebels return to Syria
2015/9/24	Assad is Moscow's pawn in regional power stakes
2015/9/24	Russia Warns of Response to Reported US Nuke Buildup in Turkey
2015/10/1	Russia rejects claims its 'anti-sisl' airstrikes hitcivilians and other rebels
2015/10/5	Israel launches airstrikes on targets in Gaza
2015/10/12	Suicide car bomb targets NATO troop convoy in Kabul
2015/10/12	Syrian troops make gains as Putin defends air strikes

表 3：2015 年 Pawn Storm 魚叉式網路釣魚郵件 (資料來源：趨勢科技 Smart Protecting Network)。

從這些標題可明顯看出 Pawn Storm 都是利用一些最新且具新聞價值的活動資訊來誘騙受害者點選連結。儘管這些都屬於針對特定對象的針對性攻擊，但有些在當時卻引起了相當大的關注，而且在 2015 年至 2016 年間相當頻繁。絕大多數的攻擊都沒有太多媒體關注，但有些卻也成功登上新聞版面。

2016 年，在趨勢科技和其他資安廠商不斷披露之後，社會大眾對這類攻擊的意識開始逐漸上升。例如，2016 年 9 月，德國多家主要報紙報導了有關德國政治人物在 2016 年 8 月遭到 Pawn Storm 攻擊的事件。趨勢科技也確實看到 Pawn Storm 以德國相關議題為社交工程誘餌的網路釣魚電子郵件。

然而這些電子郵件其實只是某個規模更大且牽涉許多其他國家的行動之一。德國媒體所報導的網路釣魚郵件一點也不稀奇，這只不過是 Pawn Storm 集團每日的例行公事而已。然而，這也顯示歹徒從 2016 年起開始對入侵政治團體特別有興趣。

儘管 Pawn Storm 的某些魚叉式網路釣魚攻擊引起相當的關注，但他們在感染受害對象時都會小心翼翼。首先，他們的漏洞攻擊網址會針對每個對象而精心特製，而且內含一個針對每個對象獨一無二的參數。當目標對象點選了漏洞攻擊網址時，首先會執行一段蒐集其系統特徵的 JavaScript 程式碼，但這並非惡意程式本身。這段 JavaScript 會將系統資訊上傳到歹徒的漏洞攻擊伺服器，包括：作業系統版本、語言設定、安裝的瀏覽器附加元件以及系統所在的時區等等。漏洞攻擊伺服器會根據這些資訊來判斷該以什麼方式發動攻擊，包括：舊漏洞、零時差漏洞，或者利用社交工程誘餌[16]。很多時候，使用者除了被重導到某個正常的新聞網站閱讀社交工程誘餌當中所說的新聞訊息之外，並不會發生什麼事。Pawn Storm 是否會發動零時差攻擊，還要看這個零時差漏洞是否寶貴。因為，零時差漏洞一旦曝光，廠商就會開始進行修補，讓漏洞失去價值。

2016 年，我們發現就在某個 Windows 權限升級漏洞被揭露之後，Pawn Storm 趁著廠商還沒釋出修補更新之前特別加強攻勢，並擴大其攻擊的政府機構人員。他們結合了才剛釋出修補更新的 Flash 零時差漏洞與這個仍未修補的 Windows 權限升級漏洞來發動攻勢[17]。

不過，就算受害目標真的感染了惡意程式，其感染的也是較為單純的第一階段惡意程式。Pawn Storm 會利用這個程式來刺探目標對象是否值得進行更深入的行動。若值得，駭客就會在系統上安裝一些第二階段的惡意程式，如 X-Agent 和 X-Tunnel。接下來，Pawn Storm 會試圖深入網路基礎架構，希望能進一步控制受害者網路上的更多節點。

2016 年，Pawn Storm 開始利用內嵌 Flash 檔案的 RTF 和其他 Office 文件。該 Flash 檔案會將受害者的系統資訊上傳至遠端伺服器。我們已證實這個遠端伺服器可能利用一連串的漏洞攻擊、零時差攻擊、權限升級攻擊來感染受害的電腦。這樣的感染方式最早是由 Palo Alto Network 研究人員所提出，並且將它命名為「DealersChoice」[18]。

Pawn Storm 偏愛的攻擊方式、資源及工具

水坑式攻擊

Pawn Storm 會入侵其目標可能瀏覽的網站來發動所謂的「水坑式攻擊」(Watering Hole)。在這類攻擊當中，駭客必須守株待兔，隨時觀察有誰連上這個已被入侵的網站。Pawn Storm 會在這些網站上植入一些腳本來幫他們達成目的。我們曾經看過 Pawn Storm 在某個正常網站上植入名為「Browser Exploitation Framework (BeEF)」瀏覽器漏洞攻擊架構[19] 的軟體套件。此外，也曾看過 Pawn Storm 在網站上植入一些指向其獨門漏洞攻擊套件的連結。BeEF 的運作方式正如其名，也就是從瀏覽器對網路使用者發動攻擊。合法的滲透測試人員也會使用 BeEF 工具，因此這類工具算相當普遍。這類套件包含了許多工具模組，包括情蒐偵察、社交工程、主動式漏洞攻擊等等。

對駭客來說，BeEF 最有用的情況是遇到那些喜歡在背景保留許多分頁的使用者。當使用者開啟一個瀏覽器分頁，並且連上一個含有 BeEF 漏洞攻擊套件的網站，駭客就有充分的時間可以仔細偵察目標系統，並嘗試各種不同的攻擊手法，直到分頁被關閉為止。這些攻擊甚至可能結合社交工程攻擊、密碼擷取或漏洞攻擊。

我們曾經看過某個烏克蘭國防企業的網站遭駭客植入一個指向遠端 BeEF 漏洞攻擊套件的連結。因為會瀏覽該網站的使用者很可能就是 Pawn Storm 想要攻擊的對象，而且可能已遇過各種攻擊。除此之外，歐洲和非洲某些國家的外交部網站也被駭客植入過 BeEF 漏洞攻擊套件。

早期在 2014 年時，Pawn Storm 即曾經入侵波蘭政府網站以及波蘭能源交易所 (Power Exchange in Poland) 的網站。瀏覽這些網站的使用者很可能就會感染 Pawn Storm 的獨門漏洞攻擊套件。

正如先前提到，Pawn Storm 在 2016 年 6 月曾經入侵 DCCC 的網站。任何經由 dccc.org 網站捐款的人都會被導向 Pawn Storm 的某個網站。Pawn Storm 很可能是希望入侵美國民主黨的捐助者並暗中加以監控。可惜我們尚未找出其確切的感染過程。

零時差漏洞

Pawn Storm 已知會使用多個零時差漏洞[20]。例如，2016 年 10 月底，Pawn Storm 曾經利用一個 Flash 零時差漏洞來搭配某個 Windows 權限升級漏洞。就在廠商修補了這個 Flash 漏洞 (CVE-2016-7855) 之後，Pawn Storm 馬上擴大其攻擊目標，希望能在所有使用者都完成修補之前發揮漏洞的最大利用價值。2016 年 10 月 28 日，歹徒發動了一波引起相當關注的行動，使用了多份 RTF 文件來攻擊使用者。

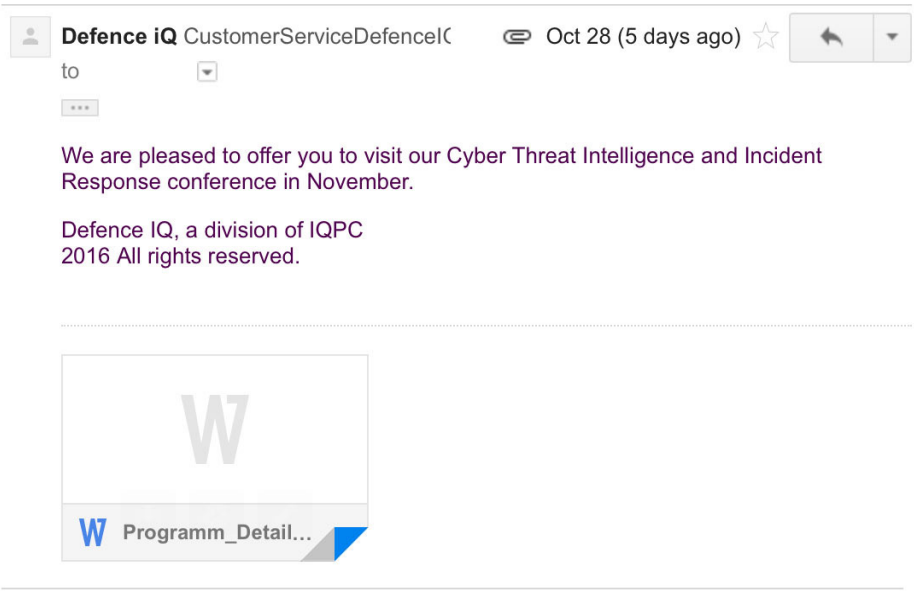

圖 11：使用 RTF 文件的 Pawn Storm 魚叉式網路釣魚郵件。

該 RTF 文件含有一個內嵌的 Flash 檔案，這是一個單純的檔案下載程式。我們曾見過它先從遠端伺服器下載一個加密的 Flash 漏洞 (CVE-2016-7855) 攻擊程式。接著再下載另一個可讓 Microsoft Word 當掉的檔案。在其他案例當中，第二個下載的檔案曾經出現 Pawn Storm 的第一階段惡意程式。

2015 年 7 月，趨勢科技發現駭客利用一個 Java 零時差漏洞來搭配另一個權限升級漏洞，藉此避開 Java 的點選播放 (click to play) 保護機制。

圖 12：Pawn Storm 曾經使用的獨門零時差漏洞 (在漏洞修補之前)。

除了這些零時差漏洞之外，Pawn Storm 對於 Hacking Team 外洩事件當中曝光的漏洞也都非常迅速地採取了對應行動。

第二階段幕後操縱 (C&C) 伺服器

我們從 2013 年年底開始，都一直持續監控該團體的第二階段 C&C 伺服器。2013 年底左右，該團體活躍中的 X-Agent C&C 伺服器大約有5台。2016 年 10 月初，我們掌握到活躍中 X-Agent C&C 伺服器數量就有 26 台。這強烈顯示 2016 年是 Pawn Storm 相當活躍的一年。

還有另一個高峰期是在 2014 年秋天，可能原因是趨勢科技當時發表了有關 Pawn Storm 的第一份報告，使得該團體對其基礎架構進行一番修正。

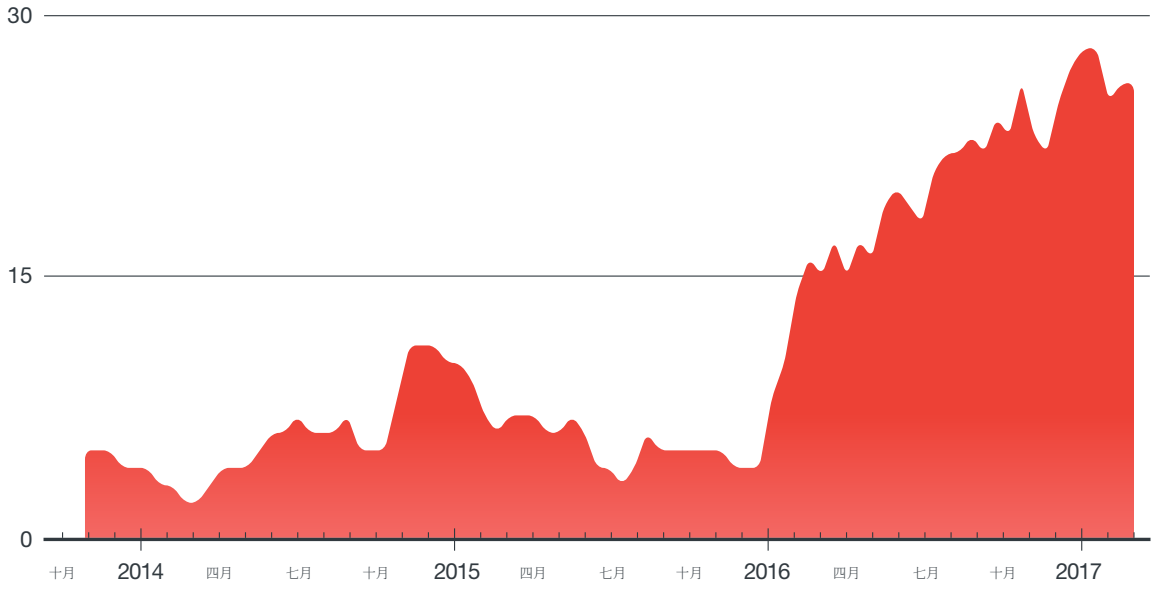

圖 13：2013 年 10 月至 2017 年 2 月 X-Agent C&C 伺服器數量變化。

2016 年耶誕節前後，活躍中的 X-Agents C&C 數量稍微增加至 27 台。2017 年 1 月，該數字達到高峰，共有 28 個活躍中的 X-Agent IP 位址。在 2016 年歲末佳節期間，Pawn Storm 並未放長假。我們發現就在耶誕節過後的隔天 (2016 年 12 月 26 日)，Pawn Storm 就恢復其魚叉式網路釣魚行動。2017 年 1 月，登入憑證網路釣魚行動也恢復正常。

共犯

很明顯地，Pawn Storm 特別偏愛使用某些網站代管服務廠商和網域註冊機構。其偏愛程度有時已經到了情有獨鍾的地步，因此甚至有些新註冊的網域都還沒用於攻擊當中就被發現。不過，近幾個月來，Pawn Storm 所使用的 IP 範圍似乎較有所變化，使得某些活動變得不易追蹤。

一般來說，Pawn Storm 的網域都位於網路基礎建設發達的國家，如：美國、英國、法國、荷蘭、拉脫維亞、羅馬尼亞及德國。在這些國家，政府的情治單位通常能夠輕易且合法地攔截歹徒幕後操縱伺服器的連線、(魚叉式) 網路釣魚郵件的來源、以及 Pawn Storm 在其境內架設的漏洞攻擊網站。不過，不論是網站流量或電子郵件流量，只要透過傳輸層 (TLS) 加密連線，這些合法攔截行動的效果就會大打折扣。

例如，Pawn Storm 在發送登入憑證網路釣魚郵件時，就不必擔心執法機關的問題，除非執法機關能夠實際掌握他們發送郵件的伺服器。下表列出 2015 年 Pawn Storm 用來發送 Yahoo 登入憑證網路釣魚郵件的伺服器。就我們所知，2015 一整年，Pawn Storm 僅用到一個位於德國的 IP 以及一個位於荷蘭的 IP 來發送網路釣魚郵件。

日期	發送端 IP	伺服器名稱	後端 IP	伺服器名稱
1/15	80.255.3.94	ubuntu	46.166.162.90	Henry-PC
2/15	80.255.3.94	ubuntu	46.166.162.90	Henry-PC
2/15	193.169.244.35	security.service-facebook.com	46.166.162.90	Henry-PC
3/15	80.255.3.94	ubuntu	46.166.162.90	Henry-PC
3/15	193.169.244.35	security.service-facebook.com	46.166.162.90	Henry-PC
4/15	193.169.244.35	security.service-facebook.com	46.166.162.90	Henry-PC
4/15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
5/15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
6/15	80.255.3.94	set121.com	46.183.217.74	Henry-PC
7/15	80.255.3.94	set121.com	46.183.217.74	Henry-PC
8/15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
9/15	80.255.3.94	set121.com	46.183.217.74	Henry-PC
10/15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
11/15	193.169.244.35	security.service-facebook.com	46.183.217.74	Henry-PC
11/15	193.169.244.35	security.service-facebook.com	185.82.202.102	WIN-17MK2DLAHLN
11/15	80.255.3.94	exua.email	無	無
11/15	193.169.244.35	security.service-facebook.com	87.121.52.145	Hans-PC
12/15	193.169.244.35	security.service-facebook.com	87.121.52.145	Hans-PC
12/15	193.169.244.35	security.service-facebook.com	185.82.202.102	WIN-17MK2DLAHLN

表 4：2015 年 Pawn Storm 用來對知名 Yahoo 用戶發送登入憑證網路釣魚郵件的伺服器。

2016 年，Pawn Storm 開始使用像 GMX 和 Yandex 這類合法的電子郵件服務廠商，並經由 IPVanish 之類的 VPN 伺服器來發送登入憑證網路釣魚郵件。C&C 伺服器 (如 X-Agent) 的實際通訊資料都會經過加密，因此，就算攔截到其通訊資料，除非知道解密的演算法，否則亦無法解讀其內容。Pawn Storm 顯然不在乎情治單位是否知道其受害者的身分。

當我們發現其許多 X-Agent C&C 伺服器已活躍數個月之後，這一點就更顯而易見。就三年來所觀察到的資料來看，其 X-Agent C&C 伺服器的活躍時間平均大約在 6 個月左右。其中有 10 台 X-Agent C&C 伺服器甚至活躍長達 12 月以上。如此可看出，Pawn Storm 相當厚顏無恥，因為他們並不在意是否哪天可能失風被逮。這或許算是其行動上的安全漏洞，但也代表受害者對於 Pawn Storm 的攻擊有點束手無策。在許多攻擊當中，駭客不管怎樣都能得到他們想要的。

下圖顯示 2013 年 11 月至 2017 年 2 月歹徒第二階段 X-Agent C&C 伺服器在各國的分布情況。從圖中可清楚看出這三年來活躍中的 C&C 伺服器的分布情況。

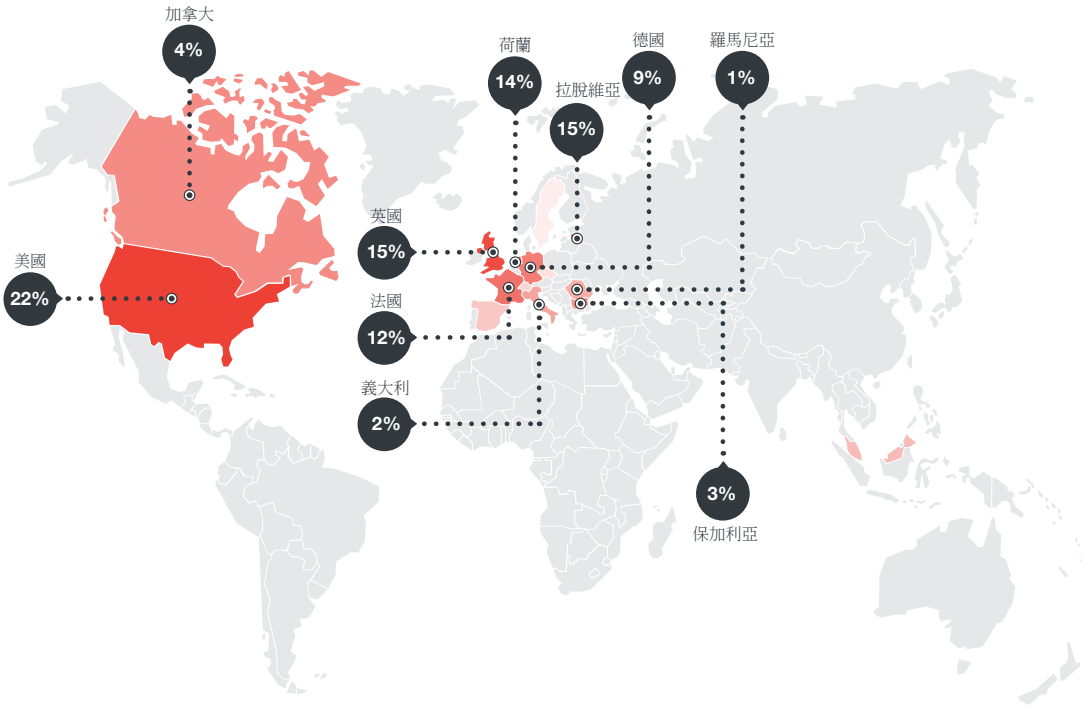

圖 14：過去三年來活躍中的 X-Agent C&C 分布情況。

安全措施

此處所謂的「安全措施」是指歹徒為了避免其活動及行蹤暴露所做的預防措施。Pawn Storm 的安全措施做得相當不錯，因為雖然 Pawn Storm 在許多行動當中顯然並未刻意隱藏行蹤，但我們很難找出其行動與地下網路上的哪些人有所關聯。許多網路犯罪集團至少都有某些成員在地下網路上的代號已經曝光。但 Pawn Storm 集團的成員在這方面的保密做得相當不錯。Pawn Storm 明顯偏愛使用某些代管服務廠商、DNS 服務廠商以及網域註冊機構。只要監控這些服務廠商，研究人員就能輕鬆發掘歹徒是否又架設了新的基礎架構。透過這樣的方式，Pawn Storm 的很多基礎架構都很早就被發現，有時甚至是在駭客實際發動攻擊之前。

這看來似乎又是另一項該團體在安全措施上的漏洞。然而 Pawn Storm 也會使用匿名註冊的網域，這時他們會選擇截然不同的服務供應商。經由這些網域的攻擊或許就不容易被發現，因此也無法算在 Pawn Storm 頭上。

除此之外，Pawn Storm 所偏好的服務廠商通常提供較好的匿名性，一個原因就是這些廠商都接受比特幣付款。關於這點，Pawn Storm 反倒是利用了西歐網站代管服務廠商較重視客戶隱私的特點。我們不曉得這些代管服務廠商對於其服務遭網路犯罪與網路間諜集團利用是否知情，不曉得他們是否有額外收取費用。但某些網站代管服務公司過去確實與所謂的「防彈主機」代管服務廠商有所關聯。我們在 2016 年曾經在一篇文章當中提到一個荷蘭代管服務廠商的案例[22]。我們發現 Pawn Storm 經常利用 VPN 伺服器來連上免費的網頁郵件信箱，並且散發魚叉式網路釣魚郵件來攻擊鎖定目標。某些 C&C 伺服器或許只是負責將流量轉送至中間代理器 (Proxy) 並且經由多次轉跳將竊取到的資料轉送回真正的後端伺服器。其實，歹徒只要多繞幾台代理器，就能大幅提升行動的安全性與匿名性。

就算 Pawn Storm 的基礎架構很快就被發現，但在受害者察覺異樣之前，歹徒已經將大量的資料傳送至國外伺服器。還有許多案例是受害者在遭到感染或入侵之後數個月才發現，有些案例甚至超過一年。

Pawn Storm 的絕大部分行動，基本上都會引起各國情治單位的注意。然而一般的警政單位所做的調查最後都無疾而終，因為網路間諜案件[23] 通常必須交由層級更高的政府單位來處理，而非刑事調查機關。有時候，同一國家或不同國家之間的執法機關也無法溝通順暢。因此，或許某個國家的情治單位已經掌握了 Pawn Storm 在其國內或另一個國家的行動，但卻無法及時通知對方，讓 Pawn Storm 更容易得逞。

不難想像，Pawn Storm 集團其實還蠻感激資安研究人員剖析並報導其攻擊行動 (反正他們的目標已經達成)。因為大眾傳播媒體可能會找到這些文章並加以刊登，這對歹徒來說等於是免費宣傳，不僅彰顯其能耐，更讓受害的機構遭受二次打擊。一般的網路犯罪集團通常不喜歡獲得媒體關注，甚至在其行動遭到曝光或報導時會暫停一下避避風頭。但這對 Pawn Storm 來說卻一點也不影響。事實上剛好相反，從 2014 年秋天至今已經有很多關於 Pawn Storm 的報導，但其活動卻反而越來越大膽，也越來越頻繁。

結論：如何防範 Pawn Storm

在經過仔細的分析之後，我們對於 Pawn Storm 的活動、規模與技巧，都有明確的掌握，也了解到該團體的真正動機和能耐。在掌握了 Pawn Storm 的未來動向以及過去的發展歷史與行動之後，希望所有可能受害的目標未來都能有效防範這項威脅。在本文最後，我們希望提出一些防範 Pawn Storm 的建議。

防範像 Pawn Storm 這樣的駭客集團是一項艱難挑戰。他們的資源充裕，可以執行長達多年的攻擊行動，而且對於攻擊對象的挑選似乎也有明確的方向。我們已見識到就連最小心的網頁郵件使用者也可能落入其登入憑證網路釣魚陷阱當中，也見識到其精密的攻擊手法。2015 和 2016 年 Pawn Storm 已不只一次使用零時差漏洞，此外，他們的手法也相當純熟，包括：分頁置換攻擊、篡改 DNS 設定、水坑式攻擊以及進階社交工程技巧等等。同時，他們也不乏一些巧妙運用各種技術的新技巧。

Pawn Storm 的攻擊不僅涵蓋多個層面，而且當發掘某個高價值目標時還會投入更多資源。就算曾經多次擋下其攻擊，也不代表未來就能高枕無憂，因為駭客只要成功一次，就能達到目的。

儘管如此，您還是可以透過下列方法來提升自身的防禦能力：

1. 盡可能縮小攻擊面，某些不需暴露在外的系統，就不要讓人經由網際網路存取。
2. 要求遠端工作人員必須經由公司的 VPN 伺服器連上您的系統。
3. 盡可能減少您所使用的網域名稱數量，並且將郵件伺服器集中。
4. 防範您網域的 DNS 設定遭到篡改，挑選信譽良好的註冊機構，此外，您的 DNS 系統管理帳號必須採用雙重認證。透過註冊機構來凍結您的網域設定，避免您的網域遭到未經授權的變更。例如，您

可以要求註冊機構在 DNS 設定有任何變更時，打電話給您授權的 DNS 系統管理員來確認是否真有這項變更。

5. 在公司的網頁郵件實施雙重認證，或者使用實體金鑰 (如 USB 隨身碟) 來進行認證。
6. 教育員工妥善保護其免費郵件帳號與社群媒體帳號，要求他們不要將這些帳號用於工作用途。
7. 當您的員工出國出差或參加會議時，借一台乾淨的電腦給他們使用。在出差回來之後，將電腦上的資料全部清除，然後重灌作業系統。
8. 外包廠商也可能成為資料洩密的來源，因此請務必挑選信譽良好的服務廠商。
9. 教育員工如何養成良好的電子郵件和電子郵件帳號使用習慣，特別是，千萬不要將未經加密的敏感資訊保存在信箱內，切勿經由電子郵件傳送未經加密的敏感資訊。
10. 找一家信譽良好的廠商定期幫您的網路進行滲透測試。此外，也做一下社交工程詐騙測試。
11. 隨時修補並維持軟體更新。

參考資料

1. TrendLabs。(2004 年 7 月 22 日)。*趨勢科技威脅百科 (Threat Encyclopedia)*。「TROJ_SCONATO.A」。上次存取時間 2017 年 3 月 8 日： http://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/troj_sconato.a.

2. L.Kharouni、F. Hacquebord、N.Huq、J. Gogolinski、F.Mercês、A.Remorin 與 D. Otis。(2014 年 10 月 22 日)。*趨勢科技*。「Pawn Storm 攻擊行動：轉移目標以躲避偵測」(Operation Pawn Storm: Using Decoys to Evade Detection)。上次存取時間 2017 年 3 月 12 日： http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf.

3. TrendLabs。(2016 年 1 月 16 日)。*趨勢科技*。「Pawn Storm 攻擊行動重點摘要與最新發展」(Operation Pawn Storm: Fast Facts and the Latest Developments)。上次存取時間 2017 年 2 月 20 日： https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts.

4. TrendLabs。(2017 年 3 月 10 日)。*趨勢科技*。「網路宣傳初探」(Cyber propaganda 101)。上次存取時間 2017 年 3 月 13 日：https://www.trendmicro. com/vinfo/us/security/news/cybercrime-and-digital-threats/cyber-propaganda-101.

5. Eset 研究人員。(2016 年 10 月 20 日)。*ESET*。「Sednit 間諜集團剖析」(Dissection of Sednit Espionage Group)。上次存取時間 2017 年 3 月 17 日：https://www.eset.com/int/about/newsroom/research/dissection-of-sednit-espionage-group/.

6. FireEye 威脅情報。(2014 年 10 月 27 日)。*FireEye*。「從 APT28 看俄羅斯網路間諜行動」(APT28: A Window into Russia's Cyber Espionage Operations?)。上次存取時間 2017 年 3 月 16 日：https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

7. R. Benchea、C. Vatamanu、A. Maximciuc 及 V. Luncaşu。*Bit Defender*。「檢視 APT28 駭客集團：竊取情報與政府資訊」(APT28 Under the Scope: A Journey into Exfiltrating Intelligence and Government Information)。上次存取時間 2017 年 3 月 13 日：http://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf.

8. Microsoft 資安情報。(2015 年 11 月 16 日)。*TechNet Microsoft*。「Microsoft 資安情報報告：Strontium」(Microsoft Security Intelligence Report: Strontium)。上次存取時間 2017 年 3 月 15 日： https://blogs.technet.microsoft.com/mmpc/2015/11/16/microsoft-security-intelligence-report-strontium.

9. ThreatConnect 研究團隊。(2016 年 8 月 12 日)。*ThreatConnect*。「熊脫逃？」(Does a Bear Leak in the Woods?)。上次存取時間 2017 年 3 月 3 日：https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/.

10. R. Buschmann、L. Eberle、C. Henrichs 與 G. Pfeil。(2017 年 1 月 15 日)。*Der Spiegel*。「對抗運動禁藥的絕望內幕」(Inside the Desperate Battle against Sports Doping)。上次存取時間 2017 年 3 月 16 日： http://www.spiegel.de/international/world/sports-doping-and-the-difficult-fight-to-prevent-it-a-1129918.html.

11. Feike Hacquebord。(2016 年 5 月 11 日)。*趨勢科技*。「Pawn Storm 攻擊德國基督教民主黨」(Pawn Storm Targets German Christian Democratic Union)。上次存取時間 2017 年 3 月 13 日：http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/.

12. Feike Hacquebord。(2016 年 3 月 7 日)。*趨勢科技*。「Pawn Storm 攻擊行動將土耳其列入攻擊名單」(Pawn Storm Campaign Adds Turkey To Its List of Targets)。上次存取時間 2017 年 3 月 10 日：http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-adds-turkey-list-targets/.

13. Feike Hacquebord。(2015 年 8 月 18 日)。*趨勢科技*。「揭發 Pawn Storm 國內間諜行動；烏克蘭與美國成為全球首要目標」(Pawn Storm's Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets)。上次存取時間 2017 年 3 月 13 日：http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/.

14. AzaRaskin。*Aza Rask.in*。「Tabnabbing (分頁置換攻擊)：網路釣魚新手法 」(Tabnabbing: A New Type of Phishing Attack)。上次存取時間 2017 年 3 月 7 日： http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/.

15. Feike Hacquebord。(2014 年 10 月 24 日)。*趨勢科技*。「Outlook Web Access 使用者面臨 Pawn Storm 攻擊風險 」(Operation Pawn Storm: Putting Outlook Web Access Users at Risk)。上次存取時間 2017 年 2 月 15 日： http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-putting-outlook-web-access-users-at-risk/.

16. Feike Hacquebord。(2015 年 4 月 16 日)。*趨勢科技*。「Pawn Storm 活動升高，NATO 與白宮成為目標」(Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House)。上次存取時間 2017 年 3 月 16 日：http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/.

17. Feike Hacquebord 與 Stephen Hilt。(2016 年 11 月 9 日)。*趨勢科技*。「Pawn Storm 趁零時差漏洞修補之前升高魚叉式網路釣魚攻擊」(Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched)。上次存取時間 2017 年 3 月 17 日： http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/.

18. Robert Falcone 與 Bryan Lee。(2016 年 10 月 17 日)。*Research Center Paolo Alto Networks*。「Dealers Choice 為 Sofacy 的 Flash Player 漏洞攻擊平台」('Dealers Choice' is Sofacy's Flash Player Exploit Platform)。上次存取時間 2017 年 3 月 2 日： http://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/.

19. The Browser Exploitation Framework Project (瀏覽器漏洞攻擊架構專案)。上次存取時間 2017 年 3 月 8 日： http://beefproject.com/.

20. Brooks Li 與 Feike Hacquebord。(2015 年 7 月 11 日)。*趨勢科技*。「Pawn Storm 最新消息：趨勢科技發現新的 Java 零時差漏洞攻擊」(Pawn Storm Update: Trend Micro Discovers New Java Zero-Day Exploit)。上次存取時間 2017 年 3 月 16 日： http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-trend-micro-discovers-new-java-zero-day-exploit/.

21. Jack Tang。(2016 年 12 月 2 日)。*趨勢科技*。「一個位元掌控整套系統：CVE-2016-7255 漏洞分析」(One Bit To Rule A System: Analyzing CVE-2016-7255 Exploit In The Wild)。上次存取時間 2017 年 2 月 20 日：http://blog.trendmicro.com/trendlabs-security-intelligence/one-bit-rule-system-analyzing-cve- 2016-7255-exploit-wild/.

22. Feike Hacquebord。(2016 年 4 月 21 日)。趨勢科技。「荷蘭網路攻擊共犯分析」(Looking Into a Cyber-Attack Facilitator in the Netherlands)。上次存取時間 2017 年 3 月 15 日：http://blog.trendmicro.com/trendlabs-security-intelligence/looking-into-a-cyber-attack-facilitator-in-the-netherlands/.

23. Roman Dobrokhotov。(2016 年 11 月 8 日)。*Aljazeera (半島電視台)*。「在俄羅斯遭到監控」(Under surveillance in Russia)。上次存取時間 2017 年 3 月 12 日： http://www. aljazeera.com/indepth/opinion/2016/11/surveillance-russia-161107133103258.html.

作者：

TrendLabs

趨勢科技全球技術支援與研發中心

趨勢科技

趨勢科技是全球雲端安全領導廠商，致力為企業和消費者開發網際網路內容安全與威脅管理解決方案，建立一個安全的數位資訊交換世界。身為伺服器安全的先驅，擁有 20 多年經驗，我們專門提供符合客戶及合作夥伴需求的頂尖用戶端、伺服器及雲端安全防護，更快攔截新的威脅，保護實體、虛擬及雲端環境內的資料。我們領先業界的雲端運算防護技術、產品及服務皆以趨勢科技 Smart Protection Network™ 基礎架構為後盾，能在威脅出現的來源，也就是網際網路，直接攔截威脅，並且還有全球 1,000 多位威脅情報專家在背後支援。如需更多資訊，請至：www.trendmicro.tw

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.tw