無檔案惡意軟體滲透全球 40 個國家的銀行、政府和電信業

無檔案惡意軟體 Meterpreter 感染了超過 140 家企業和政府機構遍及全球 40 個國家。殭屍網路 Mirai 開始擴大感染 Windows 裝置。波蘭超過 20 家銀行受到駭客攻擊，攻擊來源竟然是國家金融監督局。

無檔案惡意程式橫行全球 40 個國家

駭客破解領務局外館聯繫信箱密碼規則，上萬筆民眾個資外洩

外交部領務局近日出面表示，多數領務局與外館聯繫信箱密碼遭駭客破解，造成信箱內容的資料外洩，估計有 15,000 筆曾利用出國登錄系統的民眾個資外洩。領務局根據 SOC 系統的 Log 中發現，郵件系統在去年 10 月就出現大量不屬於外交部網域的 IP，存取駐外使館聯繫信箱。因為外館聯繫信箱密碼具有規則性，所以駭客僅取得一、兩個信箱密碼後就能夠破解 117 個所有外館的聯繫信箱。外交部目前已通知受影響民眾，建議民眾更換信箱密碼，避免駭客利用民眾個資，竊入信箱。此外，外交部找資安專家調查，初步判斷領務局內部電子郵件主機、文件、護照作業系統等相關主機則無入侵跡象。行政院資安處也在 2 月 3 日介入調查表示，駭客利用具匿蹤功能的洋蔥網路(TOR)入侵，無法查證真實的攻擊來源 IP。

開啟含巨集惡意程式的 Word 文件，駭客即能操控 Mac OS 電腦

資安公司 Synack 研究總監 Patrick Wardle 近日發現，有一支惡意的巨集程式藏在 Word 文件專門感染 Mac OS 電腦。受害者同意開啟惡意巨集後，會將巨集內建的惡意軟體安裝至 Mac 電腦，駭客就能侵入竊取受害者電腦的內部資料、瀏覽紀錄和密碼等，以及操控視訊攝影機。此外，Patrick Wardle 檢驗了樣本發現，文件標題為「U.S. Allies and Rivals Digest Trump’ s Victory - Carnegie Endowment for International Peace.docm」。駭客可能偽裝非政府營利組織或基金會名義寄發惡意文件，誘騙受害者開啟該文件。Wardle 指出，使用者若不同意開啟該文件巨集，就不會被感染。

勒索軟體 DynA-Crypt 鎖定被害者螢幕，每 5 分鐘隨機刪除電腦資料

資安公司 GData 惡意軟體分析師 Karsten Hahn 發現，最近出現一個新的勒索軟體 DynA-Crypt，不僅會加密受害者電腦的資料，還會竊取並刪除電腦資料。這些竊取資料包括，使用者的行為紀錄、系統聲音、輸入鍵盤的命令、Skype 聯絡人、Chrome 和 Firefox 的瀏覽行為等。DynA-Crypt 鎖定被害者電腦螢幕後，出現要求支付勒索贖金的訊息，警告若沒馬上支付，每 5 分鐘會隨機刪除電腦資料。GData 認為，這類勒索軟體已經有解鎖方式，受害者可不需支付贖金。

Android 銀行木馬 Marcher 感染上萬臺裝置，竊取信用卡資料和銀行資料

荷蘭資安公司 Securify 研究人員發現，Android 銀行木馬 Marcher 在過去 6 個月建置了 9 個殭屍網路，專門感染 Android 6.0.1 和 Android 7.0 裝置。其中，有一個殭屍網路感染了 11,000 臺裝置，分布在德國（5,700 臺）、奧地利（3,100 臺）、法國（2,200 臺）。駭客用寄發釣魚簡訊給受害者，偽裝成是 What’ app 或 Netflix App 的連結，來騙取 Android 管理權限，就能竊取受害者資料和操控該裝置，也會要求受害者輸入銀行帳號，竊取銀行資料。

波蘭 20 家銀行遭惡意軟體感染，攻擊來源竟是國家金融監管局

資安部落格 BadCyber 指出，波蘭至少有 20 家銀行感染惡意軟體，部分資料遭竊。波蘭金融網路監控中心初步調查顯示，攻擊來源 IP 竟然來自波蘭金融監管局網站，金融監管部門成了攻擊金融機構的幫兇，但還不清楚該 IP 是否為真實來源。賽門鐵克檢測發現，該惡意軟體原始碼與惡意軟體 Lazarus 原始碼有共同的字串，懷疑為同一類型的惡意軟體。Lazarus 在 2009 年出現，主要是攻擊美國和韓國的銀行機構，2016 年孟加拉銀行遭竊案，也發現當時使用的惡意軟體也跟 Lazarus 相似。

無檔案惡意軟體橫行，全球 140 個銀行、政府及電信遭滲透

卡巴斯基實驗室於 2 月 8 日提出警告，名為 Meterpreter 的無檔案（fileless）惡意程式滲透了全球 40 個國家的逾 140 個組織，包括銀行、電信業者及政府機構。駭客是利用滲透測試框架 Metasploit framework 產生腳本程式，該程式會分配記憶體、解析 Windows API，並把 Meterpreter 直接下載到 RAM 上，還以 Windows 中的 Netsh 網路配置命令行工具

建立被駭主機及駭客伺服器之間的傳輸通道。卡巴斯基也發現，全球超過 140 個組織網路的 Windows 註冊檔中有不同惡意 PowerShell 腳本的蹤跡，這些蹤跡皆為木馬程式，其中光是在美國就有 21 個組織受到影響，中國也在名單之列。更多新聞

Windows 裝置小心！ Mirai 木馬程式來了

俄國資安業者 Mr. Web 發現，Mirai 已經出現新變種，可感染 Windows 裝置。這支木馬會在 Windows 裝置上面自我複製擴大感染。此外，若是感染 Microsoft SQL 及 MySQL 等資料庫，這隻木馬程式還會建立具有管理員權限的使用者帳號，來執行更多種惡意任務，包括啟動執行檔、刪除檔案、植入自動啟動的圖示或在 Windows registry 建立相應 log 檔，想成為駭客開啟日後攻擊或竊密的大門。過去，駭客只利用 Mirai 惡意軟體感染 Linux 的 IoT 裝置，就可操控 200 多萬臺 IoT 裝置成為殭屍裝置，發動 1.5Tbps 的 DDoS 攻擊，現在還可操控 Windows 裝置，恐怕災情會更嚴重。

IDC：亞太區 8 成 4 的企業資安策略僅達最低標準

根據 IDC 最新的研究結果顯示，亞洲（不含日本在內）800 多家企業，發現高達 84%企業資安策略位於成熟度底線，其中有 43.8%的企業屬於最不成熟的單點型（Ad Hoc），僅部署最基本的資安防護，且缺乏專職的資安人員；此外有 40.2%的企業落在回應型（Opportunistic），配備專責資安人員，但多半仍仰賴外部資源，且資安配置以法規要求的範圍為限，並未具備清楚的防護架構與內部風險評估機制。IDC 表示，綜觀全球，資安管理問題主要都環繞在人員與安全技術兩大挑戰，但在亞太區，缺乏專責的專業資安人力是一

大問題，許多企業仍將資安列為資訊部門的部分責任，甚至讓資訊長主掌資安事務，凸顯出企業對於安全威脅本質的不了解。

Nexusguard：未來駭客會持續鎖定政府和金融機構發動 DDoS 攻擊

資安公司 Nexusguard 發布第四季 DDoS 攻擊威脅報告指出 5 項重點，200Gbps 以上的 DDoS 攻擊較少、12 月 DDoS 攻擊次數跟 11 月相比增加了 52%、金融機構的應用防火牆裝置收到的警告與 11 月相比增加 2.86 倍、美國消費品安全委員會偵測到 17,872,563 次 DNS 攻擊，以及從 10 月到今年 2 月監測到 426,770 臺 IoT 殭屍裝置。Nexusguard 認為 2016 年重大的 DDoS 攻擊事件，經常是 1Tbps 規模以上的 DDoS 攻擊。而且，駭客發動這些大規模 DDoS 攻擊的方式，是利用 IoT 裝置的安全漏洞成為殭屍裝置攻擊，未來會有越來越多殭屍裝置出現。駭客也會持續鎖定政府和金融機構發動 DDoS 攻擊。

資料來源：iThome