資安訊息：七月份網路安全威脅報告

風險：　資安訊息

摘　　要：資安事件：綜觀本月份資安新聞，與台灣有相關的新聞為趨勢科技發現一個鎖定台灣政府機關的目標式攻擊，攻擊者使用遠端存取木馬 PlugX ，濫用 Dropbox 線上儲存服務下載 C&C 設定資訊。相關新聞可參考 iThome 發佈「趨勢：鎖定台灣政府部門的木馬利用 Dropbox 更新 C&C」。若企業及機構之資安政策允許人員使用 Dropbox 的連線行為，建議請勿隨意瀏覽來源不明的網頁以及開啟郵件附加檔案，以降低受駭風險。

重大弱點：微軟公佈了 6 項重大更新，Adobe 發布旗下產品(Flash Player /Air) 共 1 個弱點通告，Apple 發佈旗下產品(QuickTime /Safari /iOS /OS X /TV) 共 5 個弱點通告，Google 發佈 Chrome 瀏覽器共 2 個弱點通告，Mozilla 發布旗下產品 (Firefox /Thunderbird) 2 個弱點通告，WordPress 發布 11 個弱點通告，Apache 發布 3 個弱點通告，Oracle 發布 56 個弱點通告，Cisco 發佈旗下產品 43 個弱點通告，SUSE 發佈 13 項更新，Red Hat 發布 32 項更新，建議受影響的用戶盡速上網修補。

病毒狀況：防毒軟體廠商近期發現 TSPY_BANKER.WSTA 木馬程式，是一個透過檔案下載或垃圾信件方式感染的間諜木馬。該木馬會將自己注入到正常的程序裡，進而建立登錄項目與檔案，並嘗試竊取銀行或金融機構的敏感資訊。建議您勿瀏覽可疑或惡意網站以及開啟任何可疑的檔案或郵件，並更新防毒軟體病毒碼至最新版本。

網路威脅分析：經由 HiNet SOC 團隊進行網路威脅情報分析後，建議客戶可採取以下防護措施：

(1) 更新 WordPress 最新 3.9.1 版本，並且更新 MailPoet 版本更新至 2.6.9 版本。同時檢查管理者帳號權限及新增使用者帳號清單，刪除 1001001 帳號及阻擋非屬於管理網段之連線。另外，檢查是否有異常 Theme 檔案上傳，如發現異常檔案敬請先刪除。

(2) Symantec EndPoint 目前 0day 防護情況，更新檔已發佈提供(Update to 12.1 RU4 MP1b)，請 SEP 11~12 的使用者進行下載更新。

(3) 群暉 NAS 遭受駭客進行加密資料勒索，目前群暉官方已建議用戶更新至 5.0 版本，並請停用 Synology EZ-Internet / Quick Connect 服務及更改 Port 5000~5001 之對外連線預設通訊埠，以避免被駭客由外部直接進行攻擊。

2014/08/15

本資訊轉自教育部資安服務網