自動化殭屍電腦通報機制

◎葉羅堯

殭屍網路（Botnet）已成為近年來非常熱門的資通安全議題之一，根據調查臺灣已成為世界前三名的殭屍電腦地區，其中最容易被駭客看上的一個族群就是「校園電腦」。依國家實驗研究院國家高速網路與計算中心（以下簡稱國網中心）調查，全國的校園電腦中，包含公用電腦（如：計算機中心電腦、系計中電腦）及個人電腦，至少有六成曾經被植入惡意程式（malware），而淪為「殭屍電腦（bot）」。

國網中心自民國 99 年起於八大校園中建置誘捕網路（Honeynet），用以捕捉殭屍電腦（bot）、中繼站（Command & Control Server），甚至是最末端的殭屍網路主宰者（Bot master），並且在接續的兩年間不斷擴建「誘捕網路」，至今已有超過三千個 IP 位址的偵測系統，包含 Windows、Linux、Android 系統，用以蒐集各項資訊提供學、研、業界進一步運用，例如：惡意程式分析報告、惡意程式樣本、攻擊來源分布圖等等。

而在誘捕的後端，我們也研發「互動式探測通報系統」，用以改善學術研究網路上殭屍電腦的通報效率，並抑制殭屍網路的擴張規模。

我們可先由圖一了解現行校園電腦中毒通知流程。由圖可知，當各種偵測單位檢測到攻擊事件時，其中必須先經由 A-ISAC（教育機構資安通報平台）依「攻擊端所在位置」區別後，再分別通知相關校園管理單位（通常是計算機中心），由相關人員再對中毒電腦的使用者個別進行通知。這一來一往所耗費的時間往往超過 12 小時，尤其在例假日期間，經常要到上班日學校相關人員才會收信，其所需要的時間更可能達到 48 至 60 小時以上；因此我們也經常在分析時看到專門在例假日、連續假日前才進行攻擊的殭屍網路。

相反地，藉由本中心開發之互動式探測通報系統，可充分縮短通報流程，直接藉由使用者端工具列進行定時輪詢（Polling）確認，目前設定為每 15 分鐘（可進行調整）之內即可讓使用者察覺其使用中的電腦是否已淪為「殭屍電腦」。故本系統可有效地改進現有通報流程，讓殭屍電腦的運作時間縮短，降低交互感染的機率，進而侷限住殭屍網路的成長規模。

另外，為了進一步了解惡意程式並進行分析，此通報系統的另一功能即為：加速蒐集電腦受感染之特徵。圖二為此「互動式探測通報系統」的整體架構圖，其中 A-SOC DB 即為國網中心前期所建置之誘捕系統資料庫，只要受感染的電腦對誘捕系統進行攻擊時，此資料庫便可即時取得此攻擊事件相關資料，如：攻擊來源位址、攻擊目標位址、攻擊網路埠號等等。為了減少 A-SOC DB 的負擔，此通報系統獨立建置另一主伺服器（Main Server），定時（約 15 分鐘）至 A-SOC DB 更新最新攻擊事件資料，並且維護互通式探測通報系統網頁，以供管理者及特定使用者查詢攻擊資訊。

此外，考量未來可能有眾多的使用者，此通報系統亦能利用「雲端虛擬機器技術」與「使用者端工具列」進行即時通訊。當誘捕系統受攻擊時，藉由 A-SOC DB，本通報系統會在短時間內取得此攻擊者的位址，並且新增進入相對應之雲端虛擬機器的資料庫中；而使用者端工具列則會定時（約 15 分鐘）輪詢確認是否「此使用者電腦的網路位址在攻擊者位址名單中」，若無出現，代表此使用者電腦並未進行攻擊行為，則繼續進行原本之網頁瀏覽；若有出現，代表此使用者電腦很可能已遭受感染，本系統將進行特徵問卷調查，請使用者提供其電腦相關資訊，如作業系統版本、電腦異狀特徵等等。根據使用者的回報，本系統將提供初步排除問題之可能解決方案，最後再將使用者導回原本之網頁瀏覽。而使用者所提供之特徵問卷則會回饋至主伺服器，可供未來進行惡意程式分析之參考數據。

「使用者端工具列」安裝後圖示，如圖三。目前版本適用於 Windows 作業系統下之 Internet Explorer 瀏覽器，未來可依需求再進行其他瀏覽器之開發。使用者安裝此工具列後，將會自動定時（目前設定為 15 分鐘）確認是否遭受感染，使用者並可利用工具列之功能鍵進行即時檢測及瀏覽通報系統網頁。

未來互動式探測通報系統會再不斷地新增各種功能，目前正著手進行自動化惡意網址比對之功能，期望降低使用者進入帶有惡意程式之網頁的頻率。此外，國網中心將會持續依使用者的需求加入新功能，提供使用者更安全、方便的上網環境。