崑山科技大學學報第八期 第47~56頁（民國100年6月）
Journal of Kun Shan University, No.8, pp.47~56(June,2011)

網路僵屍電腦之偵測系統的實作

王 平*，林文暉**，林孝忠***，黃財德****，李奇軒****

*崑山科技大學資訊管理系 副教授
**崑山科技大學資訊管理系 助理教授
***崑山科技大學資訊管理 系講師
****崑山科技大學資訊管理系 研究生

摘要

網路駭客運用僵屍網路(botnet)進行商業資訊的偷竊，造成企業及終端使用者重大威脅。僵屍電腦(zombies)具有隱密、不易偵測的特性，並使用不同的通訊協定進行操控，使得防火牆、防毒軟體難以完整偵測與清除。目前的僵屍病毒(bot)偵測技術主要依賴病毒碼(virus pattern) 與掃毒引擎進行比對。通常病毒碼是由多種特徵所組成，變種病毒(variant)稍加修改單一特徵後，即可能避開病毒碼的偵測；本研究使用沙盒工具SysAnalyzer觀察病毒的行為歷程，依據感染行為的順序及時間，透過頻繁情節(frequent episode)分析，歸納出共同病毒特徵及偵測準則，以建置「病毒特徵資料庫」，並估算病毒偵測之支持度(support)與信心度(confidence)，以利檢測已知及其變種的僵屍病毒。為了證明本研究所提出之方法的可行性，實作完成一個「僵屍電腦偵測系統」及「疑似感染網址地圖」，運用成功大學資通安全測試平台(Testbed@TWISC)於仿真網路環境加以測試與驗證。實驗結果顯示本研究提出之方法可以有效及正確的地偵測出僵屍病毒，透過疑似感染網址地圖的監控，協助管理者快速掌控網路感染之僵屍電腦。

關鍵字：僵屍網路、僵屍電腦、僵屍病毒、情節法則、疑似感染網址地圖

壹、前言

駭客攻擊手法的日新月異，目前透過僵屍病毒(bot)的感染，使防火牆、防毒軟體等防護機制不再可靠，導致全球遭受僵屍病毒感染的電腦數逐漸上升。這些受感染的僵屍電腦(zombies)，成為駭客攻擊的新跳板，透過資訊交換並配合社交工程(social engineering)，發送病毒給其他聯絡人，產生更多的受害主機(victims)並形成僵屍網路(botnet)。僵屍網路的特徵在於僵屍網路主控者(bot master)透過主機的控制與命令(Control and Command; C&C)，就可遙控遠端僵屍電腦進行攻擊；其攻擊手法複雜多變，除傳統分散式阻斷服務攻擊(Distributed Denial of Service; DDoS)攻擊外，新型態攻擊包括跨網站攻擊(Cross-Site Scripting; XSS)、垃圾郵件(Spam Mail)、或透過即時通訊軟體(Instant Message; IM)作媒介的感染，取得使用者隱私的資訊，造成財務的損失及資訊安

全的隱憂。統計 2009 年十大網路威脅的類型，包括系統漏洞之入侵(Injection flaws)、身份認證攻擊及連線管理(broken authentication and session management)、跨網站腳本攻擊(cross-site scripting, XSS)、跨網站請求欺騙等攻擊(cross-site request forgery, CSRF)，其中以系統漏洞之入侵及跨網站腳本攻擊成長率最高 (OWASP, 2010)。現今，病毒及阻斷式服務所造成之攻擊有逐年遞減之趨勢，取而代之的攻擊手法是透過僵屍網路進行商業資訊的偷竊，此一攻擊造成的後果相當嚴重，將影響商業及金融秩序。此外，目前僵屍網路的應用已被駭客進行商業化，透過商業交易模式租用使用權，更有僵屍網路主控者將病毒原始碼出售並附上教學說明，加速僵屍網路變種與改良速度。

98 年至 99 年 3 月份，崑山科大團隊已陸續完成「僵屍病毒特徵分析」及「僵屍病毒資料庫」。為求有效防護網路之 Botnet，本研究重點為研發「僵屍病毒偵測系統」，期望協助管理者找出網路之僵屍電腦(zombies)、清除僵屍病毒及維護網路的安全。目前掃毒引擎大多數是採用病毒碼(Virus Pattern)比對，針對電腦內的記錄逐一對已知行為特徵進行比對或網路行為分析。而變種病毒(variant)利用變形(self-modification)，以多型(polymorphic) 技術改變或隱藏部份的病毒行為特徵，可輕易的躲過部份防毒軟體的偵測，或造成錯誤偵測回報。依據 AV-Test 報告指出，2006 年病毒樣本數大約僅 300 萬，但截至 2008 年 5 月份病毒樣本數已經上升到 1100 萬左右，每月以超過 150 萬隻惡意程式數量成長，掃毒引擎唯有透過持續不間斷的更新病毒碼才能因應快速增長的惡意程式威脅(AV-Test org, 2010；趨勢科技，民 98)。

本研究透過誘捕系統(honeypot) 的部署及國家高速網路中心取得相關惡意程式樣本，運用行為交叉分析表(cross reference table)，透過情節法則(episode rules) 的探勘，整理歸納出病毒的共同特徵，建立「病毒特徵資料庫」及行為決策樹(decision tree)，並完成開發「僵屍電腦偵測系統」，執行病毒特徵比對，改善原有須 100%符合病毒特徵的缺點。「僵屍電腦偵測系統」經線上使用者測試及技轉單位的驗證，證明可有效檢測出已知及變種的病毒，並強化組織對僵屍網路之防護。本病毒偵測系統之特色，面對變種的僵屍病毒偵測亦可執行特徵比對，並提供偵測結果之支持度(support)與信心度(confidence)，改善病毒偵測之分析品質，提高使用者對偵測系統的信心。

第二節文獻探討偵測僵屍網路的相關研究；第三節推導以情節法則為基礎的病毒檢測分析方法，第四節測試及驗證所開發之偵測系統，並與其他偵測方法作比較，第五節作出結論及建議未來研究方向。

貳、文獻探討

1993 年在 IRC 聊天網路中出現了第一個 Bot 程序- Eggdrop，其功能是用以協助用戶方便地使用 IRC 聊天網路，其設計出發點是出於管理及服務的需求，然而此工具卻備駭客所利用，透過 Eggdrop 的改寫，駭客對使用者進行遠端控制。1990 年代末，隨著分散式拒絕服務攻擊概念的成熟，出現了大量分散式拒絕服務攻擊工具如 TFN、TFN2K 和 Trinoo，攻擊者利用這些工具控制大量的控制被感染電腦，發動分散式拒絕服務攻擊。而這些被控電腦從一定意義上來說已經具有了 Botnet 的雛形。

1999 年，在第八屆 DEFCON 年會上發佈的 Su even 2.1 版開始使用 IRC 協定建構的

攻擊者對 Zombie Computer 的控制通道，也成為第一個真正的 bot 程序。隨後基於 IRC 協定的 bot 大量出現，如廣為留傳的 GTBot、Sdbot 等，使得基於 IRC 協定的 Botnet 成為主流。 2003 年之後，隨著蠕蟲技術的不斷成熟，bot 的傳播開始使用蠕蟲的主動傳播技術，從而能夠快速建構大規模的 Botnet。 2004 年爆發的 Agobot / Gaobot 和 rBot / ybot，同年出現的 Phatbot 是在 Agobot 的基礎上，開始獨立使用 P2P 結構建構控制通道，從良性控制程序轉變到惡意 bot 的實現，從被動傳播到利用蠕蟲技術主動傳播，從使用簡單的 IRC 協定構成的控制通道轉變為複雜多變 P2P 結構的控制模式。

僵屍網路依感染之拓樸可分為三種：集中式 (Centralized)、點對點 (Peer-to-Peer; P2P)、隨機連線 (Random)，三種僵屍網路之特性比較表如表 1(Cooke et al., 2005)。

表 1 僵屍病毒的特性

網路拓樸	設計複雜度	可偵測性	訊息傳播的延遲	存活性
集中式	低	中	低	低
點對點	中	低	中	中
隨機連線	低	高	高	高

集中式是屬目前較廣泛使用的，主要為透過聊天室以 IRC 協定來操控僵屍電腦；點對點模式是目前網路感染主流，其變化型式為透過快速流明技巧改變網路連線的「隨機連線」。感染途徑常透過使用者瀏覽網站，以跨網站指令碼及即時通訊及電子郵件進行散播，僵屍網路逐漸發展成規模龐大、功能多樣、不易檢測的惡意網路，給當前的網路安全帶來了不容忽視的威脅。

參、僵屍病毒偵測決策模式的建立

本章共分為三小節，3.1 節說明僵屍病毒之樣本的蒐集；3.2 節介紹行為特徵記錄及建立病毒特徵資料庫；3.3 節說明僵屍電腦之病毒偵測準則:

一、病毒樣本的蒐集

病毒樣本來源是由「國家網路高速中心」及「國家資通安全會報技術服務中心」之惡意程式交流平台所提供，部份樣本重複並許多無法重新執行的現象，雖提供病毒特徵 XML 檔案，因無法重新執行樣本以確認其正確性，將相關病毒樣本去除。統計至 99.8.10 共蒐集 308 項樣本，本實驗室重新確認病毒的行為歷程分析，去除無法重新執行及部份具反偵測的病毒樣本虛擬作業系統及自我隱藏性，並從樣本庫中挑選具代表性的 90 隻僵屍病毒，包含 IRC 、P2P 、混合型、HTTP 等四類型態病毒進行分析，統計如表 3。透過誘捕系統 KFsensor、系統監控軟體 Process Explorer 、CurrPorts 與沙盒工具 SysAnalyzer 針對病毒進行病毒行為歷程分析。

表 3 病毒樣本數統計表

總樣本數	無法重新執行樣本數	重複樣本數	實驗樣本數
308	150	68	90

另外，利用防毒軟體 Clam AntiVirus、Avira AntiVir 及 Virustotal 分析網站針對所分析之病毒進行病毒命名及判別，完成後即可建立僵屍病毒特徵資料庫。

二、病毒行為特徵分析

本研究透過誘捕系統 KFsensor、系統監控軟體 Process Explorer 與 CurrPorts 工具和沙盒子 SysAnalyzer 記錄病毒行為事件記錄，比較上述工具之事件記錄，以擷取出病毒發作時之共同行為，作為僵屍病毒的行為特徵，再利用防毒軟體 Clam AntiVirus、Avira AntiVir(小紅傘)及分析網站 Virustotal 針對所分析之病毒進行病毒名稱判別。變種病毒之完整行為特徵雖然不易獲得，但部份的行為特徵將與資料庫內的特徵資訊相符，故本研究將運用「行為交叉分析表(如表 4)」記錄某種病毒行為與動作之間的關聯性，將具有共同行為的病毒歸納在同一類，歸納樣本病毒的共同行為歷程並建置僵屍病毒特徵資料庫，協助管理者快速分析出變種病毒與原病毒的差異性，增快分析病毒碼的速度。

表 4 行為交叉分析表

動作/事件 / 行為	開啟檔案	建立檔案	建立程序	刪除檔案	束縛IP	連接IP	開啟埠	感染IP	傳送至IP	傳送至埠
下載惡意程式<路徑><名稱>										
執行程式<名稱>										
刪除程序<名稱>										
重新命名<原名稱><新名稱>										
建立資料夾<名稱>										
修改註冊碼<路徑><名稱>										

資料來源:修改自 Stinson and Mitchell (2007)

三、病毒偵測準則

事件關連分析方法包括資料探勘(data mining)及順序分析(sequence analysis)；前者方法缺乏時間計量，只能分析事件的順序對應的信效度，而病毒行為分析重點在於其事

件(events)發生的順序及對應發生的時間(timing)，故本研究選用順序分析技術之頻繁情節法則(frequent episode rules)，透過情節(episode)進行比對特定事件序列(特徵)，其結合了時間上的變數，去分析事件關連，以找出特定的事件序列 (event sequences)。

感染特定病毒的機率則是統計頻繁情節中之特徵事件之序列及數量來加以估算。一段情節就是表示一個特定事件的序列，例如開啟通訊埠、修改註冊機碼(registry) 及下載檔案等三個有順序的事件，若透過特定的時序性項目集合比對及統計發生頻率，可以找到感染特定病毒的徵兆，並計算出所獲得證據的支持度與信心度。以下為頻繁情節法則相關名詞定義：(曹偉駿等，民 94；蘇民揚等，民 98)

(一) 事件：事件(A, t_1)，表示某個時間點 t_1 發生了類型是 A 的事件；

(二) 事件類型(e-type)：事件序列中的所有事件類型集合 e-type = {$A, B, C, \ldots$}；

(三) 事件序列：對於一個滿足事件類型 e-type 範圍的事件序列 s，記為$(s, T_s, T_e) = \{(A_1, t_1), (A_2, t_2), \ldots, (A_n, t_n)\}$，其中 A_i　e-type, $1 \le i \le n$；$t_j \leqq t_{j+1}$, $1 \le j \le n-1$，T_s 表示事件序列開始時間，T_e 表示事件序列結束時間，T_s 與 T_e 都是整數，且 $T_s \leqq t_i < T_e$。

(四) 情節：情節即為若干事件類型的組合。

(五) 時間視窗(time window)：

病毒感染行為是一時間序列的資料流程，在考察事件關聯性時，需考慮事件之間的觀察時間間隔，因此必須定義一滑動視窗，於事件的搜索的過程中，這個視窗從第一條記錄滑向最後一條記錄，只有視窗中的事件才被觀察與比對。對於事件序列 s=(s, Ts, Te)，假設有一個視窗 w 記為(w, Ts, Te) ，其中 Ts 表示啟始時間，Te 表示為結束時間，其視窗寬度 width(w)= Te –Ts。

(六) 情節 α 在事件序列 s 中出現的信心度與支持度：

支持度 sup 是透過寬度為 win 的時間視窗 w 觀察，並以特定時序性的項目集合進行比對，故 *sup* 定義為事件序列 s 中特定情節(α)發生的相對機率：

$$\sup(\alpha) = p(\alpha, s, win) = \frac{|\{w \in W(s, win) \mid \alpha \quad occurs \quad in \quad w\}|}{|\{W(s, win)\}|}, \qquad (1)$$

其中分子表示情節α在全部時間視窗w中出現的次數且$w \in W(s, win)$；$W(s,\ win)$表示在事件序列s 中，視窗寬度為win 的視窗事件序列所構成的集合。分母$|\ W(s,\ win)|$表示上述的總視窗數。(Mannila *et al.*, 1997; Qin and Hwang, 2004)

以$w(s,\ 5)$為例如圖2，情節α 為{C,D,E}，事件序列透過w觀察發現共三次出現{C,D,E} ，$sup(\alpha) = \ p(\alpha,s,win) = 3/25 = 0.12$。「頻繁情節」主要為過濾關連性較低的事件序列，意即大於或等於最小支持度(minimum support)縮寫為min_p，支持度介於0與1之間。假設A_i 及B_j 均代表示為一有序性序列(ordered list)集合，以視窗做為比對的基礎，當比對中之事件E，之前已發生的事件序列記為A_i，於事件E之後發生的事件序列為B_j。接下來，推估感染病毒之信心度$conf(A_i\ ,B_j)$應與累積頻繁情節的出現事件的相對次數成正比，故信心度計算公式為

$$conf(A_i, B_j) = \frac{\sup(A_1, A_2, ..., A_m, B_1, B_2, ..., B_n \geq \min\_P)}{\sum \sup(A_1, A_2, ..., A_m, B_1, B_2, ..., B_n \geq \min\_P)}, \quad (2)$$

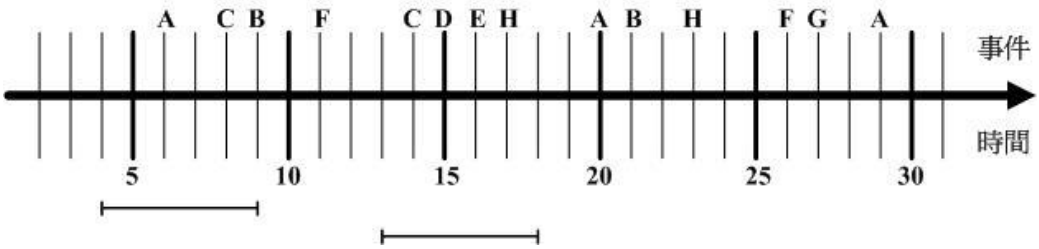

圖 2 事件序列及二個時間視窗(寬度為 5)

其中分子 sup(A_1,A_2,...,A_m,B_1,B_2,...,B_n) 代表同時出現 A_i 及 B_j 事件序列{A_i, B_j}支持度，其須滿足大於或等於最小支持度，去除低支持度的事件；分母為所有出現 A_i 及 B_j 事件序列{A_i, B_j}的支持度總合。

肆、模式的模擬與驗證

本研究實證將模擬真實網路環境的電腦感染僵屍病毒後，利用僵屍電腦偵測系統進行系統掃描，來鑑別其病毒型態與病毒名稱。測試與驗證於崑山科技大學資訊系統應用與服務實驗室以虛擬機器模擬工具 VMware 測試案例的可行性，記錄僵屍病毒的行為歷程；然後運用成功大學資通安全測試平台(TestBed@TWISC) Emulab 以真實作業系統，進行仿真測試與分析(如圖 3)。透過測試案例，驗證本研究之可行性。

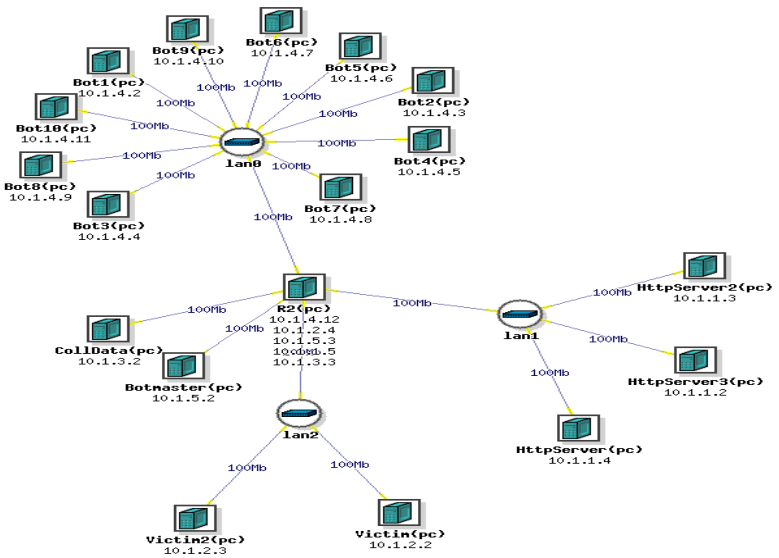

圖 3 僵屍病毒測試之網路拓樸

(一) 病毒編號：Sample 8 IRC 型態僵屍病毒 (2) 病毒名稱：TR/Downloader.Gen，由防毒軟體 Clam AV 定義 (3)病毒來源：國家網路高速中心(TWAREN) (4)取得日期：2009 年 10 月 20 日。

實驗程流主要有以下四個步驟：

步驟 1. 本工具安裝檔為 Scan.exe 自解安裝檔，點擊安裝檔後，按下「安裝」按鈕，即可由預設目錄 C:\下執行 BotScan.exe 掃描工具。

步驟 2. 執行病毒編號為 Sample 8 的 IRC Bot 病毒，當病毒執行後，執行檔將自動隱藏。

步驟 3. 開啟偵測系統(BotScan.exe) 後，點擊「系統掃描」，將開始偵測比對並記錄本機行為特徵與網路行為特徵。

步驟 4.掃描結果如圖 4，顯示系統已感染僵屍病毒，病毒名稱為 TR/ Downloader.Gen ，由 Clam AV 掃描引擎定義，並顯示信心度與支持度及相關異常特徵。由圖 5 得知偵測系統的掃描結果為 IRC 型態的僵屍病毒，依據公式(1)、(2)計算，偵測之信心度為 71%、支持度為 53%。

偵測系統發現異常行為特徵共有以下五項：(1)下載 myreceve.com 並新增至 C:\WINDOW \System32\ 目錄下 (2)修改系統登錄檔 HKEY_LOCAL_MACHINE\ Software\ Microsoft\Windows\ CurrentVersion\Run，並新增 Myreceve file 變數，預設值為 myreceve.com 、(3)開啟特定埠號 6668，服務程式為 myreceve.com、(4)對外連線為 188.136.143.10、(5)查詢 DNS IP：202.43.215.28、210.242.175.120、203.84.204.69、207.46.197.32、203.84.204.124、89.221.18.86、218.93.205.24、207.166.122.72。將掃描結果與僵屍病毒行為特徵比對，發現此系統可正確偵測出病毒。另外，根據掃描結果所顯示之信心度、支持度與病毒偵測準則比較後，確認兩者為一致。

圖 4 系統掃描結果

步驟 5. 接下來將攔截的對外連線的網址，運用 Google Map 及網址查詢技術顯示其國籍資料及詳細地置。將符合疑似感染網址名單之資訊，運用網址查詢技術追溯位置，並利用 Google Map 顯示。根據偵測系統所取得之惡意連線 IP 為 188.136.143.10，經查詢後發現此網址位於伊朗的 Shahreza 省 Esfahan 地區，詳細位置為經度 51.8668、緯度 32.0089，如圖 5。從上述測試案例發現當病毒行為特徵完整分析後，建置病毒特徵資料

庫，並開發僵屍電腦偵測系統可以無誤地檢測出病毒，並列出主機及網路異常的相關資訊。另外，透過疑似感染網址地圖，即時提供主機的連線情況給管理者參考，透過攻擊路徑的重建，可進一步反追蹤至僵屍網路的控制中心。(王平等，民 98)

圖 5 疑似感染網址名單地圖

伍、結論與未來研究方向

本研究基於先前研究的基礎－「僵屍病毒特徵分析」及「僵屍病毒資料庫」，針對僵屍病毒偵測，提出變種僵屍病毒分析的概念，實作出一套「僵屍電腦偵測系統」，包括「僵屍病毒偵測」及「疑似感染網址地圖」兩個次系統，透過技轉單位進行 8 個月的驗證，已證明其有效性，並可用於疑似感染網址的通報與顯示其對外惡意連線。本系統的限制為須以人工方式進行病毒行為特徵分析，透過數項工具交叉驗證行為特徵，以確保偵測準則的正確性，須耗用大量人力；未來研究方向可朝向「病毒特徵分析自動化環境之建立」與「僵屍病毒之數位解藥」之研發二方向進行研究。前者搭配自動化病毒特徵分析平台的建立，能提昇病毒分析及偵測效能。僵屍病毒之數位解藥可針對系統檔案進行自動備份，當系統檢測出感染病毒時，數位解藥將對系統進行自動修復，並回復至中毒前狀態，結合上述二者將能強化電腦主機的防護。

參考文獻

[1] AV-Test.org (2010), “Trend Micro Endpoint Comparative Report Performed,” . Retrieved July 22, 2010, from http://us.trendmicro.com/imperia/md/content/us/trendwatch/coretechnologies/av-test_may_2010_endpoint_comparative_report_final.pdf.

[2] Cooke, E., Jahanian, F., and McPherson, D.(2005), “The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets,” In Proceedings of the Steps to Reducing Unwanted Traffic on the Internet (SRUTI), June, Cambridge, Massachusetts, USA, 39-44.

[3] Mannila, H., Toivonen, H. and Verkamo, I. A. (1997), "Discovery of Frequent Episodes in Event Sequences," Data Mining and Knowledge Discovery, 1(3):259-289.

[7] OWASP, "OWASP Top Ten for 2010: The ten most critical web application risks," 2010. Retrieved February 09, 2010, from http://www.owasp.org/images/0/0f/ OWASP_T10 _-_2010_rc1.pdf.

[8] Passerini, E., Paleari R., Martignoni, L., and Bruschi, D. (2008), "FLuXOR: Detecting and Monitoring Fast-Flux Service Networks", In *Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (DIMV), Springer-Verlag, 186-206.

[9] Stinson E. and Mitchell C. J. (2007), Towards Systematic Evaluation of the Evadability of Bot/Botnet Detection Methods, *Lecture Notes in Computer Science*, 4579:89-108.

[10] Trend Micro (2008), "Trend Micro 2008 Annual Threat Roundup and 2009 Forecast," 2010, Retrieved December 24, 2009 from: http://us.trendmicro.com/imperia/ md/content/us/pdf/threats/securitylibrary/trend_micro2009_annual_threat_roundup.pdf.

[11] Qin, M. and Hwang, K. (2004), "Frequent Episode Rules for Internet Anomaly Detection," In *Proceedings of Third IEEE International Symposium on the Network Computing and Applications*, August 30, Los Angeles, CA, USA, 161-168.

[13] 蘇民揚、葉生正、林呈俞、張瑞德 (民96), "植基於模糊關聯規則的網路入侵偵測系統," Journal of Internet Technology, 第八卷二期, 221-228頁。

[15] 賴溪松、王榮祥(民97),「僵屍網路偵測方法之研究與實作」, 電腦與通信工程研究所未出版碩士論文。

[16] 陳嘉玫、鄭炳強、蔡育洲(民97),「使用 Flow 資訊偵測以網頁為基礎之殭屍網路」, 國立中山大學資訊管理研究所未出版碩士論文，。

[17] 鄭憲宗、曾瑞瑜(民98),「以活動關連為基礎的IRC殭屍網路偵測」, 國立成功大學資訊工程研究所未出版碩士論文。

[18] 曾黎明、陳天豪(民 98),「透過封包分析偵測並瓦解僵屍網路」, 國立中央大學資訊工程研究所未出版碩士論文。

[19] 曹偉駿、柯文元、林明孝(民 94),「模糊關聯與情境法則探勘於入侵偵測」, 2005 年全國計算機會議，台南: 中華民國電腦學會。

[20] 王 平、王榮祥、蘇浩儀、郭溥村(民 97),「殭屍網路的感染途徑重建與分析」, TANET 2008 臺灣網際網路研討會，高雄: 教育部電子計算機中心。

[21] 王平、郭溥村、王子夏、王清平(民 98),「殭屍網路的攻擊路徑分析模式」, 第二十屆資訊安全會議研討會(CISC2010)，新竹: 教育部電子計算機中心。

Implementation of Zombie Detection System

Ping Wang*, Wen-Hui Lin **,
Hsiao-Chung Lin*, Cai-De Huang****, Ji-Xuan Lee******

Department of Information Management, Kun Shan University of Technology
***Associate Professor, **Assistant Professor, ***Lectuer, ****Graduate Student**

Abstract

Hackers used botnet to steal business information and led to serious threats for enterprises and end-users. Zombies can be manipulated by distinct protocols having features of stealthy, and difficult to be detected and cleaned, even using firewalls and anti-virus tools. The detection techniques of existing bots primarily used virus scan engine to scan via pattern matching matter. The variants can be formed by modifying virus signatures then they can be hardly detected. This work investigates virus behaviors via sandbox analysis and examines the common signatures of bots using frequent episodes for constructing a virus signature database with detection rules enhancement of estimation of support and confidence degree. Furthermore, a Zombie Detection System (ZDS) and a Dark IP Map have successfully been built to detect bots and variants. To validate the effectiveness of system, test cases in Testbed@TWISC are conducted to emulate network attacks scenario. Experimental results show that the proposed approach can effectively detect zombies and help managers rapidly monitor network zombies in a precise way.

Keywords: Botnet, zombie, bot, episode rule, Zombie Detection