崑山科技大學學報第九期 第37~47頁（民國101年6月）
Journal of Kun Shan University, No.9, pp.37~47（June, 2012）

僵屍病毒解藥與監控系統之研發

王 平* 林文暉** 林孝忠*** 李奇軒**** 呂育華****

資訊管理系 資訊科技學院 崑山科技大學
*副教授 **助理教授 ***講師 ****研究生

摘要

近來駭客的攻擊手段已經從大規模攻擊手法如分散式阻斷服務攻擊，轉變成商業資訊的竊取及販賣。新型的僵屍電腦(zombies)具有隱密、不易偵測的特性、及自我隱藏行為特徵、快速流明等功能，使得防護軟體難以完整偵測與清除。駭客透過其電子郵件、通訊軟體、或利用電腦系統漏洞等方式，將殭屍病毒(Bot)隱藏於應用程式或網頁中，以植入受害主機，造成大量使用者主機交互感染而形成殭屍網路(Botnet)，以執行惡意攻擊。本研究實作完成一套殭屍病毒之「數位解藥 (Digital Antidote, DA)」及以軟體代理人為基礎之「監控管理平台」，能蒐集及記錄受監控遠端主機的感染狀況、網路流量，當受監控主機感染殭屍病毒時，可派送數位解藥，並將解毒後的系統記錄即時回報至監控平台；若發生資安緊急攻擊，可遠端中斷網路連線，並發送警告訊息至管理者，降低網路管理的負擔。

為了證明本研究所提出之方法的可行性，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。實驗結果發現可偵測並解除同類及變種病毒網路感染威脅，於網路內之電腦感染病毒時，可即時自動化修復作業系統，並對可疑電腦進行即時的監控，有效降低病毒對電腦系統造成的破壞，強化校園的網路安全防護。

關鍵字：僵屍網路、僵屍電腦、僵屍病毒、數位解藥、軟體代理人

壹、前言

隨著科技的進步，駭客攻擊手法也日趨成熟與多樣化，從最初的電腦破壞演進到目前的控制或企業資訊竊取。目前透過僵屍病毒(Bot)的感染，駭客改變感染途徑技巧，使得原先的防護機制不再可靠，導致全球遭受僵屍病毒感染的電腦數逐漸上升，依據根據賽門鐵克 2011 年網路安全報告指出，台灣的殭屍電腦數量約佔全球 7%，台北市約有三百萬電腦，其中而目前台北市的殭屍電腦 總數高達三十四萬台，約佔全球總數的 5%，是全球殭屍電腦數量最多的城市。 (Symtech, 2011)。受感染的僵屍電腦(zombies)，也會自動對控制中心進行連線動作，並等待駭客的指令，發起網路上攻擊活動包括受感染主機之帳號密碼及私密資料竊取、散佈垃圾郵件、發動阻斷式服務(Distributed Denial of Service; DDoS)，恐嚇等犯罪行為，造成網際網路上的網路服務運作之安全威脅。

國外研究發現部分僵屍病毒採取使用快速流明(Fast-flux)的技巧設計(Wang, P., Sparks, S., and Zou, C.C. , 2007)，將電腦的完整的網域名稱對應多址，來達到動態改變對外連線網路位址及連接埠，甚至改變查詢的網域伺服器，增加偵測與追蹤上的難度。此外，國內學者積極展開僵屍病毒的研究(Qin, M. and Hwang, K, 2004; 賴溪松、王榮祥, 民 97)，自 2009 年發現之新型的僵屍病毒擁有反偵測虛擬化作業系統能力，並隱藏病毒行為特徵技巧，造成偵測上的困難度增加；基於網路上持續遭受到僵屍病毒的感染，管理者如何清除僵屍病毒與監控疑似的僵屍網路，是一個校園網路管理重要的議題。

本研究透過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)，並完成開發一套僵屍病毒之「數位解藥」及其「監控管理平台」，透過特徵比對分析出變種病毒的共同特徵，製作數位解藥，以增加製作及偵測病毒的速度。

數位解藥已研發完成，經線上使用者測試驗證，證明可有效檢測出已知及變種的病毒，以強化組織內部對僵屍網路之防護。數位解藥之特色，採用集控式管理方式，除自動更新版本、自動防護(疫苗功能)與解毒功能外，解藥會對電腦系統檔案自動進行備份，並回傳主機的系統資訊，達到即時通報與監控目的，可大幅降低對僵屍病毒的威脅。

監控管理平台之研發可強化網路安全防護，降低網路管理人員的負擔，主要系統功能包括：1.異常流量監控 2. 數位解藥派送 3.自動化監視病毒感染與緊急斷線 4.標示區網內受感染主機位置 5.描繪僵屍網路之攻擊來源。

第二節文獻探討偵測僵屍網路的相關研究；第三節說明病毒檢測及解藥監控系統的規劃與實做，第四節測試及驗證所開發數位解藥與監控管理平台，最後作出結論及建議未來研究方向。

貳、文獻探討

一、病毒檢驗法

目前常見的病毒檢驗方法可歸納以下六種技巧: (1)病毒碼比對法(Matching Virus Definition Patterns)、(2) 加總檢查法(Check Sum)、(3)即時輸入輸出掃描法(Real Time I/O Scan) 、(4)虛擬機器模擬法(Virtual Machine Simulation)、(5)先知掃描法(Virus Instruction code emulation, VICE)、 (6)人工智慧陷阱(Rule-based)。(劉順德，民 90) 六種病毒檢驗方法的優缺點比較，因限於篇幅，無法在此詳加介紹。

由上述病毒檢驗分析方法得知，行為特徵的觀察是分析未知病毒的重點，觀察重點在於其事件(events)發生的順序及對應發生的時間(Timing)，而順序分析(Sequence analysis)技術是結合了時間上的變數，去分析事件關連，以找出特定的事件組合(病毒特徵)，透過頻繁情節法(Frequent Episodes)(Mannila *et al.*,1997)可透過視窗擷取多個連線間的特定的事件組合，以判定未知及變種病毒感染事件。

二、網路監控平台-Ntop

本系統原本使用網路上開放源碼軟體－Ntop（ntop.org, 2010;楊中皇、丁光立, 民99)作網路監控管理，但發現其將部份截取的封包加密，無法滿足資訊揭示的需求，故參考開放源碼軟體－Ntop 架構與規格，自行開發網路監控管理平台。Ntop 的架構主要可分為三大部份：Packet Capture、Packet Analyzer 、Report Engine 說明如下：
A. Packet Capture:利用 libpcap 函式庫，對通過網路卡介面的封包進行擷取，再交PacketAnalyzer 元件進行後續處理。B. Packet Analyzer:具辨識一般網際網路通訊協定的能力，對於傳送及接收網路封包，可記錄雙方主機的位址與封包數量、通訊協定類別。C. Report Engine: 對於所記錄的數據，經過分類排序後，轉換成網頁型態，並交內建的網頁伺服器作圖形處理，利用 gd 及 libpng 函式庫將數據轉換為圓餅圖或柱狀圖，以利管理者瀏覽與查看。Ntop 系統架構圖如圖 1 所示。

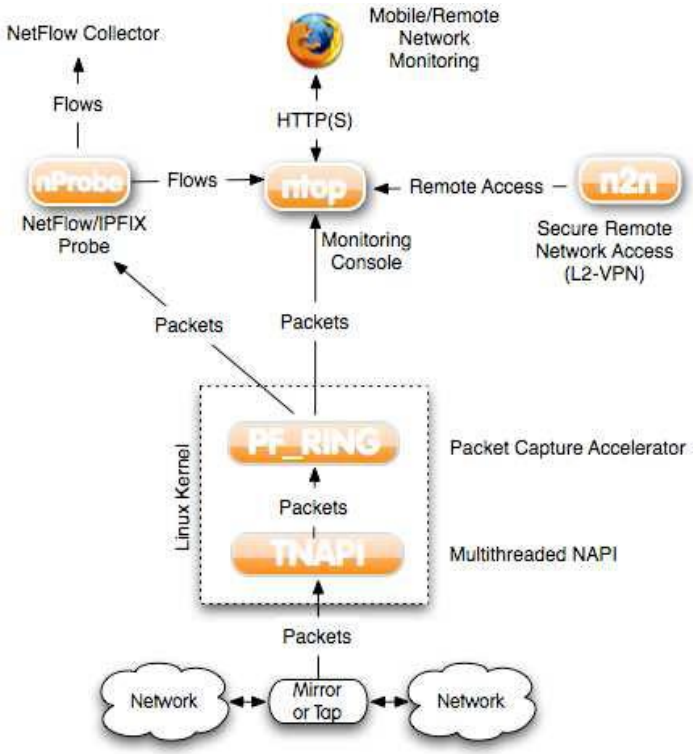

圖 1. 網路監控平台系統架構圖

(source: http://www.ntop.org/news.php)

參、數位解藥之監控管理平台系統

一、 先前研究

本實驗室從 2008 年陸續完成 Honeynet Gen II 架設，搭配 KFsensor 及 Honey D 網路

誘捕器，模擬網站、檔案傳輸及郵件處理等服務來誘捕惡意程式攻擊，蒐集與分析網路惡意軟體等研究工作。研究重點工作為 a.分析僵屍病毒的行為歷程，藉由分析病毒發作時之共同行為，找出病毒行為特徵，b.建立病毒特徵資料庫，c.發展病毒偵測系統。2008 年~2010 年研發的成果包括(1) 完成溯源定位僵屍網路之控制中心之數學模式及模擬 (2) 完成僵屍病毒第一代數位解藥 (3)研發具信度與效度之僵屍病毒受感染路徑的網址地圖(Dark IP Map)顯示系統。

二、研究規劃

本研究整合資安實驗室發展之現有研究成果，開發數位解藥之「監控管理平台」如圖 2，其提供校園內主機對僵屍病毒監控、解毒、網路控管及風險分析之平台。其主要優點為校園區網內之正常電腦下載 JADE(Java Agent DEvelopment Framework)軟體代理人(agent)（AgentLand, 2001)，由監控平台發送後，agent 會主動針提醒使用者定期進行重要資料備份，並對該電腦之系統與網路狀態進行監控；搭配先前研發之僵屍電腦偵測系統，若作業系統感染病毒時，agent 即會對作業系統進行自我修復，直到回復至中毒前狀態。但如遭遇「新型病毒」無法進行解毒，導致病毒進行攻擊網路時，則 agent 會配合收集病毒行為特徵，並產生 log 自動回傳至監控平台。判斷區網內主機產生攻擊行為，例如大量產攻擊封包，連線至特定的網址（如 DNS dynamic query 的連線 IP），或是由特定 Port 進行連線等行為，符合監控平台設定之資安準則，即可自動切斷該電腦之網路連線。

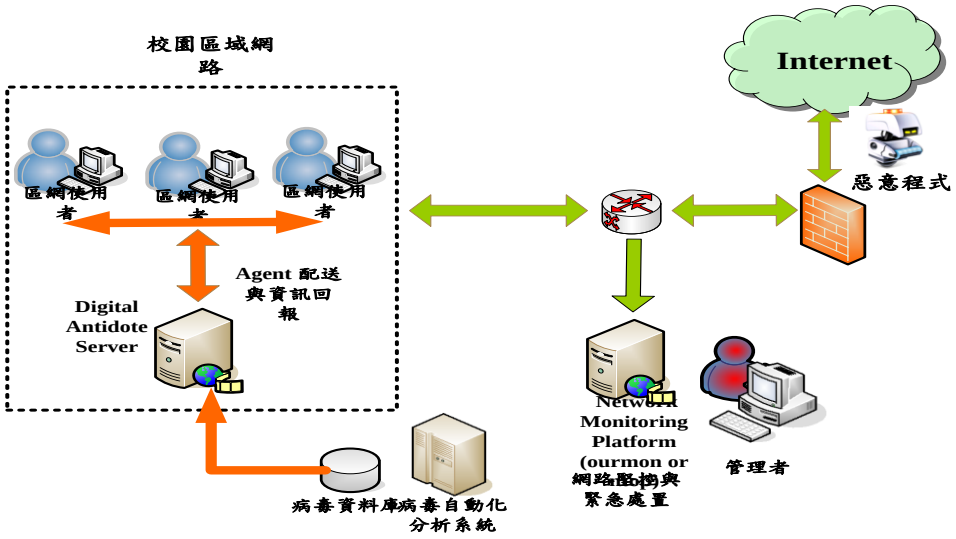

圖 2 校園僵屍電腦監控平台概念圖

三、系統實做

分析僵屍電腦病毒，需先瞭解病毒發作後的「行為歷程(behavior)」與「行為特徵(signature)」；行為歷程是指病毒發作後的行為，行為特徵為病毒感染行為的特點，可作為病毒碼偵測樣態及解毒的依據。本研究數位解藥製作參考先前研究產出之病毒特徵，製作病毒行為/動作關連表，如表 1，透過惡意行為之查表，以逆向工程方式產生事件/

動作之指令(script command)，透過 XML 呈現數位解藥，製作流程如圖 3。

表 1 病毒行為/動作關連表

動作/事件 / 惡意行為	開啟檔案	建立檔案	建立程序	修改檔案	束縛IP	連接IP	開啟埠	感染IP	傳送至IP	傳送至埠
對外連線至主機<IP><port>					V	V	V			
下載惡意程式<路徑><名稱>		V			V	V	V	V		
上傳資訊<路徑><名稱><IP> <port>			V		V	V	V		V	V
修改註冊碼<路徑><名稱>	V			V						

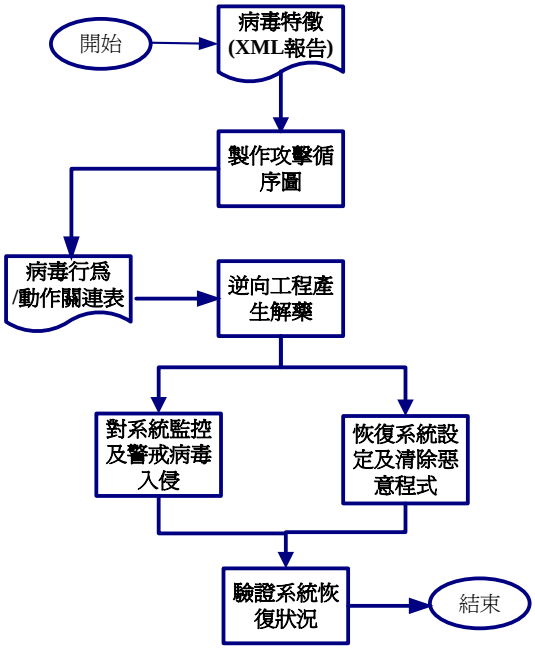

圖 3 數位解藥製作流程

2010 年首先研發第一代數位解藥，其運作流程是透過病毒分析過程所建立的病毒資料庫，比對取出僵屍病毒行為特徵，以病毒特徵建立相對應的解藥，圖 4 程序主要可分為三個主要部份－「系統資料備份」、「系統資料監控」及「系統修復」三大程序。「系統資料備份」程序是依僵屍病毒行為特徵裡，病毒會異動修改的註冊碼與系統檔案，有目地的進行備份動作。「系統資料監控」程序則為監控感染該病毒時，其所會異動的註冊碼與系統檔案，當感染病毒後，註冊碼異動時，則系統會立即進行系統修復程序，反之則定期進行系統備份程序。「系統修復」程序 1 與 2 為僵屍數位解藥系統的核心，其修復的原理是以該病毒的行為特徵所建立之解藥規則，依其順序與病毒行為，逐一對系統進行修復。

針對 2010 年研發之第一代解藥系統，無法與監控管理平台整合，本年度搭配 agent 導入並改良資料庫之資料結構，增加「回報訊息機制」及「病毒碼自動更新」，並能接

收監控平台發送之「中斷網路連線」的指令，並且會「自動彈出警告視窗」提醒使用者要備份重要資訊，精進為第二代數位解藥，如圖 4(修改部份如紅字部份)。

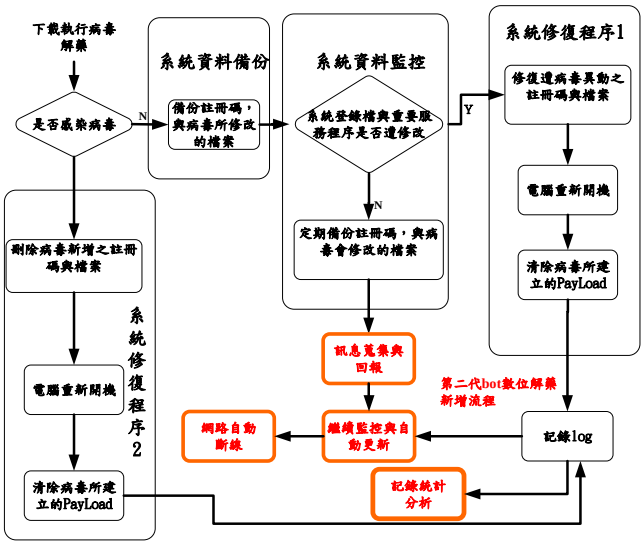

圖 4 第二代數位解藥之佈署及運作流程

監控管理平台實做是參考 Ntop 開放源程式碼，使用 C#.Net 並搭配 JADE 軟體代理人，將病毒行為/動作關連表(如表 1)轉換為網路監控準則(detection rules)，監控準則例如開啟特定 Port 與查詢特定網址，或短時間內產生大量攻擊封包，並將這些規則納入至監控平台之偵測準則，當區網內電腦出現異常行為並觸發準則，則可對該電腦之 IP 進行連線封鎖，並發信通知管理員，直到該電腦之網路行為獲得改善方解除封鎖，監控管理平台監控示意圖，如圖 5。

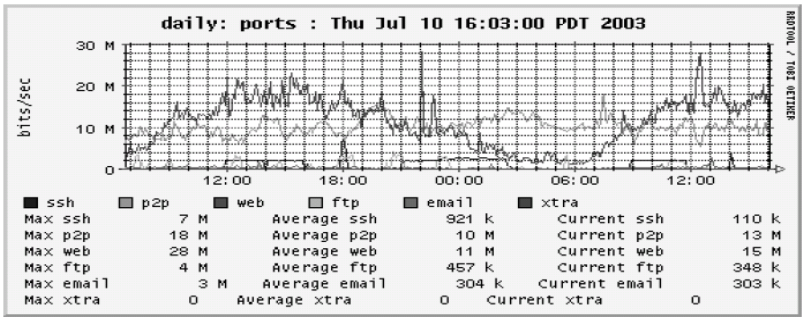

圖 5 網路事件之監控系統 (Source: Binkley and Massey, 2005)

肆、模式的模擬與驗證

本研究實證將透過案例，模擬真實網路環境的電腦感染僵屍病毒後，利用數位解藥系統之監控管理平台進行系統監控防護。第一階段測試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，確認僵屍病毒解毒與了解網路監控的情況；第二階段測試將運用成功大學資通安全測試平台(TestBed@TWISC)

進行 Bot 數位解藥測試驗證如圖 6。

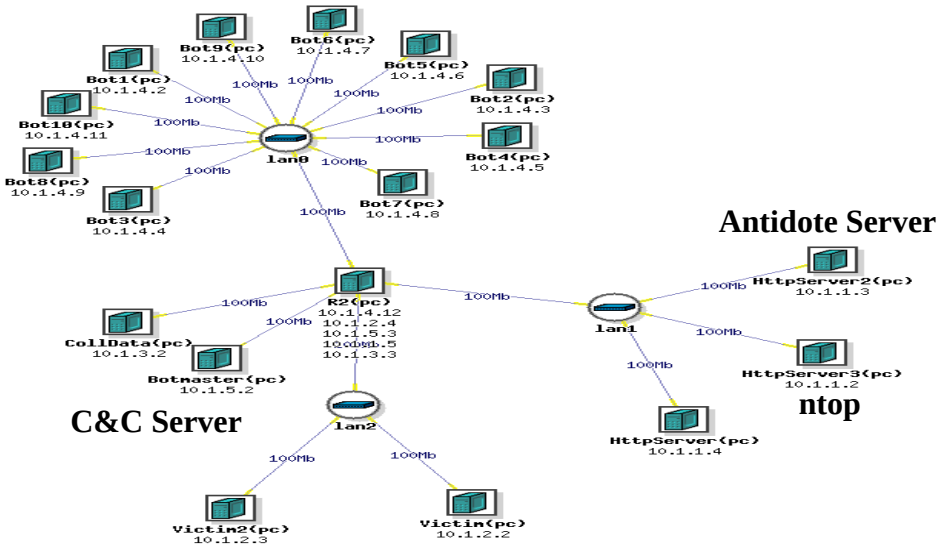

圖 6. 數位解藥測試驗證

病毒樣本來源: (1) 病毒編號：Sample 1 IRC 型態僵屍病毒 (2) 病毒名稱：Worm/SdBot.JUIIRC，由防毒軟體 AntiVir 定義 (3)病毒來源：國家網路高速中心 (TWAREN) (4)取得日期：2009 年 11 月 20 日。
實驗程流主要有以下五個步驟：

步驟 1. 本工具安裝檔為 DAScan.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:\DA\下執行 DA.exe 掃描工具，如圖 7。

圖 7. 數位解藥(疫苗)啟動主機自動監控

步驟 2. 執行病毒編號為 Sample 1 的 IRC Bot 病毒，當病毒執行後，執行檔將自動隱藏。

步驟 3. 開啟數位解藥系統(BotScan.exe) 後，點擊「啟動監控」，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. 解藥修復的結果如圖 8 顯示，系統在背景作業進行對殭屍病毒還原(解毒) 動作。

2010/9/14 07:44:22	c:\windows\system32\dirtile.com	Set registry value	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Dir Tile	Permitted
2010/9/14 07:44:23	c:\windows\system32\dirtile.com	Access network	TCP [Local host : 1123] -> [63.173.172.98 : 6668]	Permitted
2010/9/14 07:44:35	c:\windows\explorer.exe	Create new process	c:\da\da.exe	Permitted
2010/9/14 07:44:42	c:\da\da.exe	Create new process	c:\windows\system32\netstat.exe	Permitted
2010/9/14 07:44:43	c:\da\da.exe	Delete registry value	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Dir Tile	Permitted
2010/9/14 07:44:44	c:\da\da.exe	Set registry value	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Start	Permitted
2010/9/14 07:44:44	c:\da\da.exe	Set registry value	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv\Start	Permitted
2010/9/14 07:44:44	c:\da\da.exe	Set registry value	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc\Start	Permitted
2010/9/14 07:44:46	c:\da\da.exe	Terminate another pr...	c:\windows\system32\dirtile.com	Permitted
2010/9/14 07:44:46	c:\da\da.exe	Delete file	C:\WINDOWS\system32\dirtile.com	Permitted
2010/9/14 07:44:48	c:\da\da.exe	Access network	TCP [Local host : 1126] -> [72.14.213.109 : 587]	Permitted

圖 8 系統修復結果

步驟 5. 系統重開驗證，病毒已完全清除。

數位解藥系統依據行為特徵，進行逆向工程執行以下四項還原動作：

1. dirtile.com 並新增至 C:\WINDOW\System32\目錄下 2.建立 a.bat 批次檔進行修改系統登錄檔 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run，並新增 Dir Tile 變數，預設值為 dirtile.com 及關閉系統服務等等 3.開啟特定埠號 6668，服務程式為 dirtile.com 4.對外連線為 63.173.172.98。

管理平台可統計客戶端感染的現況如圖 9，運用 Mail server 保存病毒的數位證據如圖 10。

圖 9 客戶端電腦感染情況

圖 10 數位證據之存檔

此外，管理者發現新病毒或變種病毒，可編輯病毒特徵以更新數位解藥之病毒特徵，並透過 Agent 派送新版本的數位解藥，解藥版本更新如圖 11；監控管理中心持續監控網路流量是否異常，如圖 12，點擊圖 12 之 IP 欄位，可顯示個別主機之網路流量，如圖 13。從監控管理平台上可完整分析，Agent 目前該管理區域內的主機資訊(IP、網卡位址及使用者) ，作為病毒感染情況的緊急處理的判定，受感染主機詳細資訊如圖 14。

圖 11 病毒碼更新

圖 12 異常流量查詢

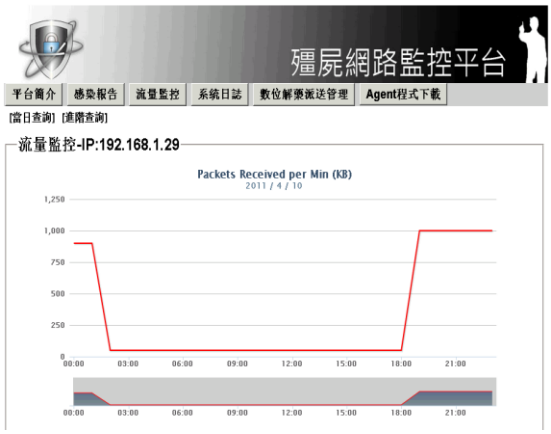

圖 13 異常流量之監控

圖 14 感染報告-單一電腦詳細感染記錄

管理者點擊圖 14 右下角之 Botnet 攻擊來源按鈕，可查看 Botnet 攻擊來源如圖 15。

圖 15 感染報告-描繪 Botnet 攻擊來源

伍、結論與未來發展方向

本研究基於先前研究的基礎－「僵屍病毒偵測系統」及「第一代數位解藥」，針對僵屍病毒長期監控需求，結合軟體代理人實作出一套僵屍病毒「第二代數位解藥」與結合感染路徑的網址地圖之「監控管理中心」兩個系統，建構校園資安監控平台的雛型，可有效監控 Bot 攻擊來源及標示區網內受感染電腦主機位置，即時掌控疑似感染網址與對外惡意連線。數位解藥其主要限制為，需掌握僵屍病毒行為特徵完整的分析事件及正確序列，否則研發出來的數位解藥將無法發揮功效。

未來研究方向將朝著建立一個「僵屍病毒自動化分析系統」，當國家網路高速中心及行政院資通安全會報技術服務中心將僵屍病毒送至本平台，則啟動自動化分析流程，分析完成後即產生病毒解藥的指令，並開始解毒程序，最後將分析的結果歸納成網路監控準則，傳送至監控平台作偵測判斷的依據。

參考文獻

[1] AgentLand, “What's an agent.”, 2001, from:http://www.agentland.com/

[2] Binkley J., Massey B., "Ourmon and Network Monitoring Performance", Freenix/ USENIX ’05, April 13, 2005.

[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.

[4] Ntop.org, “ NetFlow-lite and sFLOW based Open Source Network Traffic Monitoring.”2011, from: http://www.ntop.org/news.php

[5] 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.

[6] Wang, P., Sparks, S., and Zou, C.C. (2007), “An Advanced Hybrid Peer-to-Peer Botnet,” In *Proceedings of the USENIX Workshop on Hot Topics in Understanding Botnets* (*HotBots’07*), April 10, Berkeley, CA, 2-2.

[7] 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。

[8] 劉順德(民90)，「以樹狀關聯式架構偵測電子郵件病毒之探討」，國立中央 大學資訊管理學系未出版碩士論文。

[9] 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。

[10] 楊中皇、丁光立(民 99)，「殭屍網路活動偵測工具研發」，國立高雄師範大學資訊教育研究所未出版碩士論文。

[11] 賽門鐵克，“北市殭屍電腦 全球最「駭」城市”2011, from: http://tw.myblog.yahoo.com/major_technology/article?mid=843&next=841&l=d&fid=9

Implementation of Antidote and Monitoring System for Bots

Wang Ping *　Lin Wen-Hui**
Lin Hsiao-Chung ***　Lee Ji-Xuan ****　Lu Yu-Hua ****

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

Abstract

Recently hackers used the botnet to steal and sell the privacy information such as business information, instead of the previous network attacks, i.e., distributed denial of service attack (DDOS). New bots include the following features - stealthy, detected and fast-flux such that they are constantly difficult to be detected even using anti-virus tools as well as completly cleaned after infected. Generally, botnet are formed by injecting bots into victims thru the use of Web pages, spam mails, social networks and host vulnerabilities in order to perform the malicious attacks for hacker. This project has developed an antidote for bots and constructed an agent-based monitoring/management platform that can accumulate and record the infection flow of remote hosts. Once hosts were infected by bots, the monitoring platform will send the antidote to victims, receive the reply reports and send the alert messages to managers for decreasing their management loading; especially shutdown the network connections, if required. To validate the effectiveness of system, test cases in Testbed@TWISC are conducted to emulate network attack scenarios. Experimental results show that the proposed approach can effectively protect the attacks from both virus and its variant thru recovering the infected operation system and help managers monitor network zombies. Consequently, decrease the contagious damages of bots and remarkably increase the securities of campus networks.

Keywords: Botnet, zombie, bot, antidote, agent