行政院國家科學委員會專題研究計畫 成果報告

資安技術真實流量實地評比--子計畫三:資安技術反惡意軟體及反殭屍網路真實流量評比
研究成果報告(精簡版)

計 畫 類 別 ： 整合型
計 畫 編 號 ： NSC 99-2218-E-009-016-
執 行 期 間 ： 99 年 08 月 01 日至 100 年 07 月 31 日
執 行 單 位 ： 國立交通大學資訊技術服務中心

計 畫 主 持 人 ： 陳昌盛

計畫參與人員： 碩士班研究生-兼任助理人員：楊詠仁
碩士班研究生-兼任助理人員：蔡薰儀
碩士班研究生-兼任助理人員：徐苾芬
碩士班研究生-兼任助理人員：丁冠中
大專生-兼任助理人員：徐向賢
博士班研究生-兼任助理人員：施詠宏

中 華 民 國 100 年 10 月 31 日

中文摘要：　近年來惡意軟體急速增加，根據 Panda Labs 的統計，每天需要處理的惡意程式超過 3000 種，而且以 2007 年跟 2006 統計數字相比，增加的比例高達 800%，而其中又以 Botnet 之危害嚴重性最大。以往的惡意程式目的在於表現個人電腦實力或破壞他人電腦為主，但現今則是以竊取機密資料、獲取不法利益為主，甚至是滲透控制他人電腦作為攻擊的跳板以逃避追查。實務上，避免感染惡意程式的常見做法主要有兩大類，首先是保持良好的使用者操作習慣，另一則是使用資安軟體。良好的使用者操作習慣可以避免惡意程式利用社交工程途徑發動感染；而資安軟體常見的則是『防毒軟體(Anti-Virus)』、『防火牆(FireWall)』、『入侵偵測系統(Intrusion Detection System，IDS)』、『入侵預防系統(Intrusion Prevention System，IPS)』等，不同種類軟體系統所採用的偵測防禦技術有別，當然就有不同的處理對象及方法。

本計畫將著重於資安偵測防禦系統測試平台之建置與測試評比反惡意程式(Anti-Malware)及反殭屍網路(Anti-Botnet)兩項資安偵防技術所需要的工具或機制，結合流量錄製、流量萃取、資訊重組、資訊詢問及流量重播技術，重播真實網路流量來找出任何潛在的資安威脅或是已發展的資安偵防技術不足之處。預期在一年內可以發展出 Anti-Botnet 及 Anti-Malware 兩類 Specific 資安技術之實地與重播測試技術，佈建誘捕網路(Honeynet)，將這兩類資安技術成果轉化成為相關之專利申請與論文發表(如 bot recognition、anti-malware product testing、bot collection and analysis: active vs. passive)，研發可萃取此兩類資安技術相關流量內容的萃取工具，同時將執行至少上三件以上的資安產品測試案。

英文摘要：　Recently, the number of malware programs (including virus, Trojan horses, Botnets, phishing mails, etc.) increase rapidly. According to Panda Labs statistics, the number of malware programs to be dealt with every day is more than 3000 types. By comparing the two related statistics in 2007 and 2006, the increasing rate is as high as 800%. Among them, Botnet is one of the most harmful. In the past, the goal of most malware programs aimed at showing off personal computing strength or destroying other computers. However, nowadays more and more malware programs aim at stealing confidential information, intercepting illegal benefit, even intruding and controlling other computers as springboards for attacks in order to avoid tracing. In principle, there are two common practices to prevent malware infection: the first one is that users have good operation habits (including never download unauthorized software arbitrarily)； the other is to use security products to protect computers. There are many well-known security products (including Anti-Virus, Anti-Malware, Firewall, and IDS/IPS). Different

products utilize distinct approaches to protect systems from attacks, and have different dissimilar advantages/disadvantages.
In the project, we will focus on the building of security detection/protection system and the benchmarking of two types of security technologies: Anti-malware and Anti-Botnet. By combining the five profiling/security technologies (including traffic recording, traffic extraction, information reorganization, querying, and traffic replaying with real flows), we can discover and resolve most potential network threats and find out the advantages/disadvantages of the security technologies. This project aims to develop specific security technologies in both field and replaying tests for anti-botnets and anti-malware. After finishing the project, with the research results gained, we would like to apply for the related patents and publish papers in the area of bot recognition with anti-malware product testing, bot collection and active/passive analysis. Besides, more than three testing cases will be executed.

一、 前言

惡意程式(malware)

近年來惡意程式(malware)急速增加，根據 Panda Labs 的統計，每天需要處理的惡意程式超過 3000 種，而且以 2007 年跟 2006 相比，增加的比例高達 800%。惡意程式的定義是指一個會破壞電腦正常運作或是竊取資料的電腦程式，包括有電腦病毒(virus)、蠕蟲(worm)、垃圾郵件(spam mail)、間諜軟體(Spyware)、木馬程式(Trojan Horses)及攻擊程式(attacking tools)等。以往的惡意程式目的在於表現個人電腦實力或破壞他人電腦為主，但現今則是以竊取機密資料、獲取不法利益為主，甚至是滲透控制他人電腦作為攻擊的跳板以逃避追查。惡意程式常被包裝在免費軟體及可植入程式碼的特定圖片格式或是網頁以便引誘使用者下載使用。

感染惡意程式後，常見的症狀可能有電腦資料被刪除、電腦效能變慢、不斷出現特定視窗、無法上網、上網後只能連上某些特定網頁，或是 CPU 負載持續滿載，透過網路有莫名大量資料在傳送等。以 2003 年 Slammer 蠕蟲病毒為例，就是利用 MS SQL Server 的漏洞，在短短幾分鐘內感染數十萬台散佈在世界各地的電腦，甚至造成某些國家網路通訊中斷。之前喧騰一時的巨集病毒，則是利用軟體或是作業系統的巨集功能散播，例如像 Microsoft Word 巨集病毒 Taiwan No. 1，只要系統日期不是十三號，病毒只是寄生在 word 內，將正常文件檔感染成含有巨集病毒的文件檔案並流出；到了每月十三號，只要使用者隨便打開一份文件，病毒就會發作，如果沒有處理好，病毒甚至會佔滿記憶體，造成硬碟損害。

要避免感染惡意程式通常可以分成兩個方面來看，首先是良好的使用者操作習慣，另一則是使用資安軟體。良好的使用者操作習慣可以避免惡意程式利用社交工程途徑發動感染；而資安軟體常見的則是『防毒軟體(Anti-Virus)』、『防火牆(Firewall)』、『入侵偵測系統(Intrusion Detection System，IDS)』、『入侵預防系統(Intrusion Prevention System，IPS)』等，軟體系統不同，偵測防禦技術也不同，就有不同的處理對象及方法[1, 2, 3, 4, 5, 6, 7]。

殭屍網路(Botnet)[8]

目前企業存在最大的網路安全威脅則是 Botnet (殭屍網路)，也有人稱為 Zombie Network。Bots 通常是隨著 E-mail、Instant Message Software 或是其他系統漏洞入侵電腦後，再潛伏起來伺機而動。Botnet 由 Master (Command)及已經被 Bots 感染成為 Botnet 一員的主機組成，惡意攻擊者可透過 Master 遠端控管受感染主機，發動網路攻擊，包含 DDoS 攻擊、網路釣魚攻擊、發送廣告信及竊取資料等。

Botnet 就像是網路的隱形地雷，平常潛伏時很難被偵測出來，受感染的主機往往並不知情，必須等到攻擊發生了才會發現；況且，隨著 Bots 越來越複雜，Bots 躲避資安偵防技術與系統的能力也越

來越強，例如使用可執行的封裝程式、Rootkit 和多種通訊協定、加密技術，以及可以隱藏通訊痕跡等的新機制，都加深偵測 Bots 的難度，因此被視為現今網際網路上最大的安全威脅。根據 Gartner 統計，大概全世界會有 75%以上的企業感染上 Bots；刑事局偵九隊的統計指出，全台有三分之一的電腦被植入 Bots；Marshal 的報告則宣稱，有六個 Botnet 必須為現今 85%的垃圾郵件與網路釣魚電子郵件負責。

目前已知偵測 Botnet 的方式主要是利用偵測病毒或是 Rootkit 機制[12]、或是架設 Honeypot project[9] (Botnet 誘捕系統)、結合 Behavior/Log analysis[10, 13, 14, 15] (多層次網路行為、流量分析)、SPAM signature[11]等方式，都是需要長期監控網路，希望可以藉由收集分析 Bot 的行為模式以作為偵防時的參考。

流量來源(Traffic Source)

此整體計畫預計使用由交大網路測試中心(NBL)結合交大資訊技術服務中心(ITSC)，在總計畫與各子計畫中，共同以交通大學宿舍網路所建置之 Beta Site 做為真實網路流量來源。目前 Beta Site 在交通大學學生宿舍共擺放 48 台 48 port switch 銜接學生個人電腦，有來自 1200~1500 位同學長期使用各種網路應用程式所產生的網路流量。BetaSite 7609 對外共有 3 條線路，分別連接 TANet、Internet (交大自行申請出國專線)，以及國內其他 ISP。對外雙向總流量最高可達 4Gbps，平均也有 2Gbps 流量。這個環境提供本計畫一個絕佳的平台，除了提供真實流量以發展及評估網路鑑識各個元件的技術，更可用以部署所發展的鑑識系統，協助產品問題重製(Bug Reproduction)及校園流量分析(Traffic Profiling)與問題鑑識(Forensics)。

二、 研究目的

本計畫的目的在於規劃及設計一個 Anti-Malware & Anti-Botnet 的資安偵防技術測試平台，其中包含 Malware & Botnet 之誘補、偵測、追踪、清除、防堵等措施，希望能夠透過此平台促進 Anti-Malwae & Anti-Botnet 資安偵防技術的進步，以期減少 Malware & Botnet 感染、攻擊事件，以提升網路安全與減少因資安威脅而產生之傷害及成本。同時，藉此培育資安專業人才，並與國際資安組織交流及交換 Anti-Malware & Anti-Botnet 相關資訊。

三、 參考文獻

[1] E. Carrera and G. Erdelyi, "Digital genome mapping–advanced binary malware analysis," in *Virus Bulletin Conference*, Sep. 2004.

[2] A. Moser, C. Kruegel, and E. Kirda, "Exploring multiple execution paths for malware analysis," in *IEEE Symposium on Security and Privacy* 2007.

[3] C. Willems, T. Holz, and F. Freiling, “Toward automated dynamic malware analysis using cwsandbox,” in *IEEE Security and Privacy*, Volume 5, Issue 2, March 2007.

[4] U. Bayer, C. Kruegel, and E. Kirda, "TTAnalyze: A tool for analyzing malware," in *International Secure Systems Lab*.

[5] Zhiyin Liang, Tao Wei, Yu Chen, Xinhui Han and Jianwei Zhuge, “Component Similarity Based Methods for Automatic Analysis of Malicious Executables,” in *Virus Bulletin Conference* 2007.

[6] Qinghua Zhang, Douglas S. Reeves “MetaAware: Identifying Metamorphic Malware,*”* in *ACSAC* 2007.

[7] M Bailey, J Oberheide, J Andersen and ZM Mao, “Automated Classification and Analysis of Internet Malware,” in *RAID 2007*.

[8] B.McCarty, “Botnets: big and bigger”, in *IEEE Security & Privacy*, 2003.

[9] T. Yen, and M. Reiter, “Traffic aggregation for malware detection,” in *Lecture Notes in Computer Science, vol. 5137, pp. 207-227*, 2008.

[10] Q. Zhang, and D. Reeves, “Metaaware: Identifying metamorphic malware,” in *Twenty-Third Annual Computer Security Applications Conference*, 2007.

[11] M. Bailey, J. Oberheide, J. Andersen et al., “Automated classification and analysis of internet malware,” in *Lecture Notes in Computer Science, vol. 4637, pp. 178-197*, 2007.

[12] C. Willems, T. Holz, and F. Freiling, “Toward automated dynamic malware analysis using cwsandbox,” in *IEEE Security & Privacy*, pp. 32-39, 2007.

[13] S. Gianvecchio, M. Xie, Z. Wu, and H. Wang, “Measurement and classification of humans and bots in internet chat” in *Proceedings of USENIX 17th conference on Security symposium*, 2008.

[14] C. Livadas, B. Walsh, D. Lapsley and W. Timothy Strayer, “Usilng Machine Learning Technliques to Identify Botnet Traffic” in *Proceedings of 31st IEEE Conference Local Computer Networks*, 2006.

[15] G. Gu, J. Zhang, and W. Lee, “BotSniffer: Detecting botnet command and control channels in network traffic” in *the 15th Annual Network and Distributed System Security Symposium*, 2008.

四、 研究方法

本計劃的成果是收集 malware 及 botnet 樣本，並且能萃取及重播相關流量，因此進行的階段分為樣本收集(Sample Collection)、樣本分析(Sample Analysis)及記錄(Event logging)三部分。在樣本收集方面，除了透過合作，取得國家高速網路與計算中心之『被動式 honeypot 的樣本』外，本計畫也開發『主動式 HoneyMonkey 惡意程式蒐集系統』以收集 malware 及 botnet 樣本；在樣本分析方面，分別針對 malware 及 botnet 的主機行為(host behavior)及網路行為(network behavior)等特性作進一步觀察分析。在記錄部分，則將萃取出並經過防毒軟體確認後的 malware 樣本，整合進子計畫一所開發之資料庫 – PCAP Library 儲存。

樣本收集(Sample Collection)

在樣本收集方面，除了利用取得自國高的被動式 honeypot(包含約六十個 TANet IP addresses、三千多台主機)捕捉的 malware 或 botnet 樣本外，我們也設計了一主動式 honeypot – HoneyMonkey，模擬一般人最常使用網路的習慣，透過 Mail、Web 以及 P2P 等常見網路應用程式來收集更多樣本，如圖 1 所示。在這個方法中，我們利用幾種常見的傳染途徑：透過 spam 內容中的惡意連結或是 email 附件夾檔、WWW 中的惡意連結(URL)及 P2P 檔案分享中常見的關鍵字(Keyword)等項目，輸入至系統自動尋找、下載檔案後，再輸入給防毒軟體確認；如果確認真的是 malware 或 botnet，則將完整流量檔案存進資料庫並記錄相關結果，以作為後續分析研究。以下，則分別介紹 HoneyMonkey 處理 Mail、Web 及 P2P 傳播方式的機制：

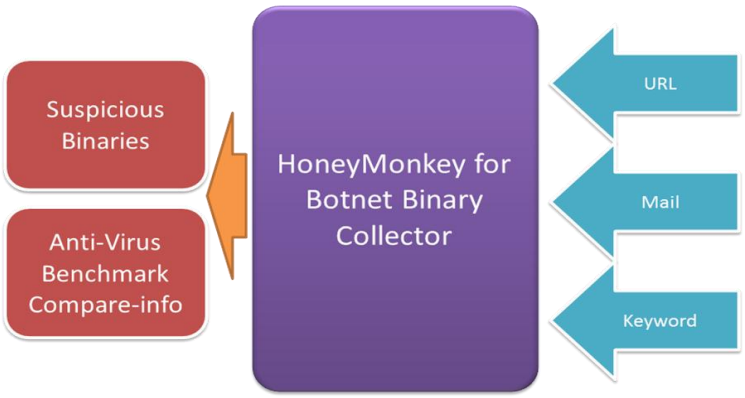

圖 1：malware & botnet 樣本收集示意圖

圖 2 為 HoneyMonkey 利用 mail 收集 malware 的機制示意圖。此 Mail module 利用 mailbox 中的信件作為輸入，先解析信件內容以嘗試取得：(1)信件附件檔、(2)郵件標題，及(3)URL 等資訊。如果取得附件檔，則上傳至 FTP 待後續防毒軟體確認；如果取得郵件標題及 URL，先上傳至 database (MySQL)記錄後，再輸入給 Web module 作瀏覽及關鍵字搜尋以確認是否為 malware 可疑樣本。

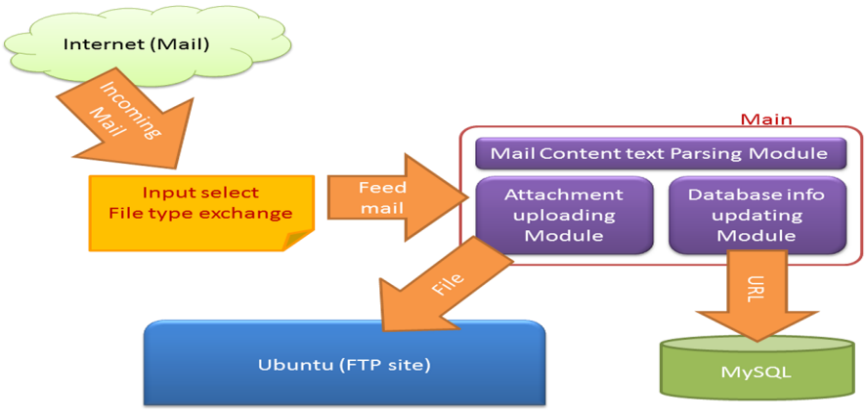

圖 2：HoneyMonkey 之 Mail module 機制示意圖

圖 3 為 HoneyMonkey 利用 web 途徑收集 malware 的機制示意圖。此 Web module 分為兩個部分：Human browsing simulating sub-module 及 Mail sub-module。Human browsing simulating sub-module 主要是模擬上網瀏覽網頁的行為，利用自剪貼簿(Clipboard)取得的 URL 或是關鍵字、透過 AutoIT 語言、針對每個網站設定四十秒鐘的瀏覽時間並回應相對應的對話方塊，如果過程中出現網頁驅動下載的要求，則會自動下載檔案並存至 FTP 待後續確認；而 Mail sub-module 則是負責監控整個模組及資料庫輸出入的資料、觸發 Human browsing sub-module、使用剪貼簿傳遞 URL 及關鍵字，如果有意外的檔案下載，會上傳至 FTP 待後續確認。

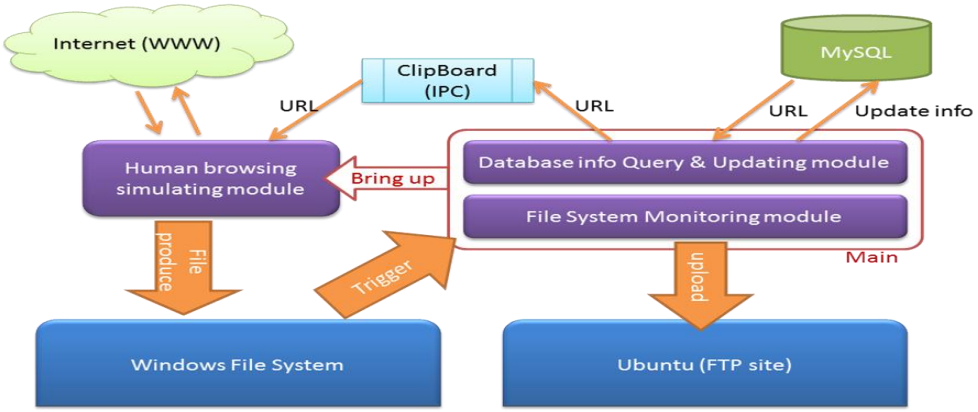

圖 3：HoneyMonkey 之 Web module 機制示意圖

圖 4 則是 HoneyMonkey 嘗試透過 P2P 檔案分享功能，搜尋常見之 malware 關鍵字以收集 malware 之機制示意圖。此 P2P module 分為兩個部分：File System Monitoring sub-module 及 Main sub-module。Main sub-module 負責控制 P2P 程式自動下載的部份，利用 AutoIT 語言實作自動化控制 P2P 程式之 GUI 介面，自系統取得關鍵字後呼叫 P2P 程式進行檔案搜尋後進行下載。File System Monitoring sub-module 負責過濾處理下載後的檔案；如果是包含 malware 機會很小的檔案(如.txt、.jpg 及.bmp 等)或是下載不完整的檔案會先被移除、壓縮檔會先解壓縮等，之後剩下的檔案則會算出其 SHA1 碼後上傳至 database (MySQL)記錄後待後續確認。

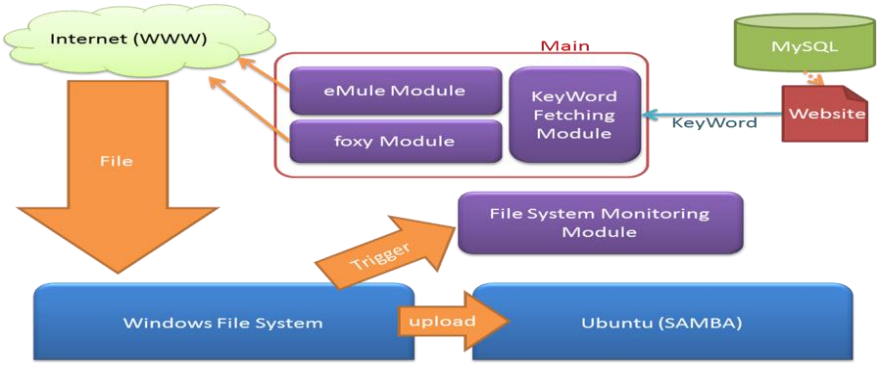

圖 4：HoneyMonkey 之 P2P module 機制示意圖

圖 5 則是利用防毒軟體驗證下載檔案是否為 malware 之機制示意圖。此 Scan module 除了用

來對下載取得的檔案進行掃描、確認是否真為 malware，同時還可以藉著同時使用多種防毒軟體的 scan engine 進行判讀的結果來評估各防毒軟體的 scan engine 的效能。為了配合防毒軟體的種類，所以目前計畫中所使用的 scan engine 是以 windows 為開發平台，並有 Kaspersky、Avira、avast 以及 ESET NOD32 共四種。此掃描機制分成三個部分：AV module、Database info inserting module 及 Rescan triggering module。執行時，先到儲存可疑檔案的 SAMBA server 上抓取檔案後，再選擇呼叫單一或是多個 scan engine – AV module 進行掃描，掃描時會一併記錄其掃描時間等資訊，掃描完成後再透過 Database info inserting module 上傳結果至 database (MySQL)。除此之外，針對某些先前已下載卻未能被 scan engine 判讀出結果的檔案，會透過 Rescan triggering module 定期從 database 中找出來，先利用網路查詢是否已有相關資訊被揭露；如果有，就更新 AV module 後再重新掃描，掃描後再更新 database 的相關記錄。最後，再根據人為檢查結果，搭配各 AV module 的判讀結果，亦可以作為評估各 AV module 效能表現的一種評估方法。

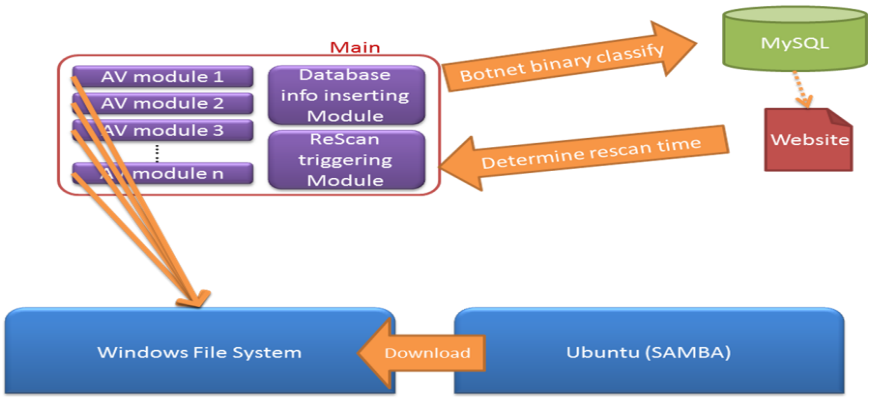

圖 5：HoneyMonkey 之 Scan module 機制示意圖

<u>樣本分析(Sample Analysis)</u>

為了能夠記錄 malware 在執行過程中的各種表現行為，所以把 malware 執行期間發生的行為分成主機行為(host behavior)及網路行為(network behavior)各自記錄分析。傳統的防毒軟體多是以掃描整個系統，嘗試尋找是否系統內存在某特定 malware 的 signature 為主，但這樣的方法容易因為 malware 的變種或是 signature 沒有更新而失去效力；此外，malware 之所以能夠在每次開機後自動被執行運作，背後一定有修改了系統檔案系統上某些重要資訊；因此，我們設計開發了一種新的掃描方式來分析 malware 的主機行為—利用監控 malware 在主機檔案系統內的行為，包含檔案的新增、修改、刪除以及 system registry 的修改等操作，來偵測及清除 malware。圖 6 及圖 7 分別為此主機行為分析系統之軟硬體架構示意圖。

這套 malware 主機行為分析系統有幾項重點：(1)被 malware 入侵感染過後的系統是不可信的—因為如果是用被感染後的檔案系統來分析的話，有可能會被 malware 刻意製造的假資訊所欺

騙，所以在比對過程中，我們是以執行過 malware 的系統硬碟及原先乾淨的系統硬碟作檔案系統的比較，在執行 malware 前後各拍下一張 system snapshot，再比較前後 snapshot 的不同處；(2)額外分析 system registry 是必須的—因為 registry 在 windows family operating systems 是以自己定義的 binary format 存在的，如果僅是單純分析檔案系統是無法確切知道被修改的資訊位置的，而且，malware 能夠一再地每次開機後自動執行運作，大多數也是因為修改了 registry 的關係；(3)使用 virtual machine 環境—為了方便大量重製相同環境、減少 overhead 及監控管理，所以將系統架設在 virtual machine 上；(4)為了清除 malware 造成的影響，有時候需要復原被 malware 修改過後的 shared library；可是因為 windows family 作業系統版本眾多，可能會遇到無法決定該用哪種版本復原的情況，目前預設是回復當初安裝系統時所安裝的版本，暫不考慮可能經過 windows update 機制更新過後的新版本。

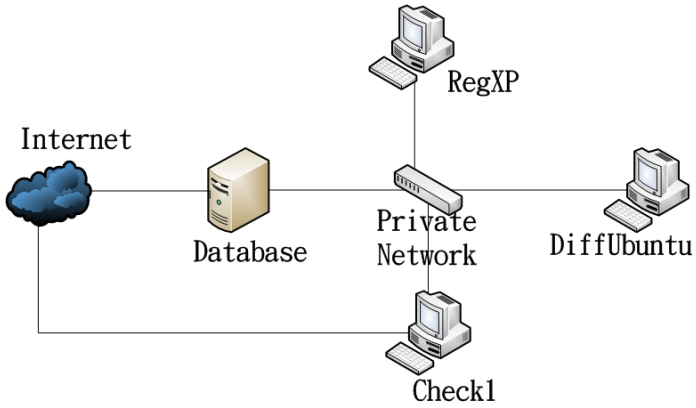

圖 6：malware 主機行為分析硬體架構示意圖

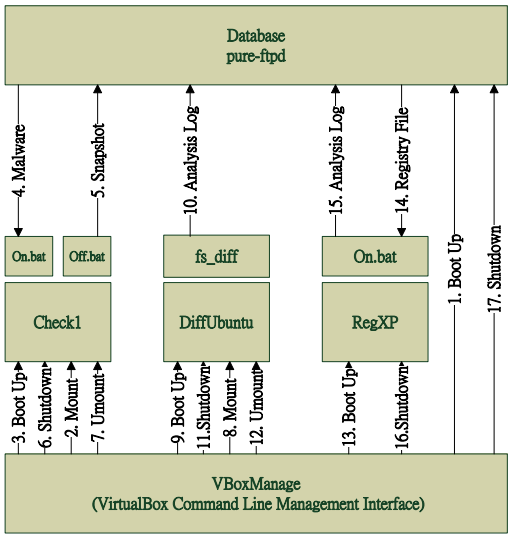

圖 7：malware 主機行為分析軟體架構示意圖

系統中共有四台虛擬機器(virtual machine, VM)，其中的 database 是作為 ftp server 用途，擔任系統內部各個元件溝通的橋樑及系統外部查詢的行為資料庫；Check1 是執行 malware 的 VM，是負責從 database 中下載 malware 後執行、在執行 malware 前後照下 snapshot 後並上傳回

database；DiffUbuntu 會比較掛上的兩顆硬碟中的檔案系統：一是系統安裝後，乾淨的硬碟，另一則是執行 malware 後受感染的硬碟；RegXP 則會從 dabase 中下載受感染過的 registry file，與一乾淨無感染的 registry 比較後，才上傳回 database。圖 7 是系統軟體架構圖，其中的 on.bat 及 off.bat 各是用來在開機後及關機前照下系統 snapshot 的批次檔；而 fs_diff 則是一用來比對兩 snapshot 的演算法。

Malware 的網路行為(network behavior)是指在 malware 執行過程中透過網路進行指令收發或是攻擊等的行為模式。我們希望透過錄製在 malware 執行過程中所出現的網路封包，嘗試發掘 malware 完整的傳染途徑、攻擊手法以及可能影響的範圍或是系統資源等網路行為，這些資料不但可以用來分析 malware 行為特性，日後還可以用作測試入侵防禦系統(Intrusion Prevention System)的測試流量。圖 8 為此 malware 網路行為分析系統示意圖，其中的 HoneyTrap1~N 代表著 N 台虛擬機器(使用 Windows XP SP3 作為客端作業系統)、recorder 負責錄製通過 network interface 的網路流量、DBInserter 負責利用封包的 5-tuple 資訊(source IP, source port, destination IP, destination port, protocol)把擁有相同資訊的封包集合成一條條的連線(connection)後，再將這些連線的資訊及流量新增至 Database 中儲存、Share Folder 則是用來儲存待錄製的 malware。

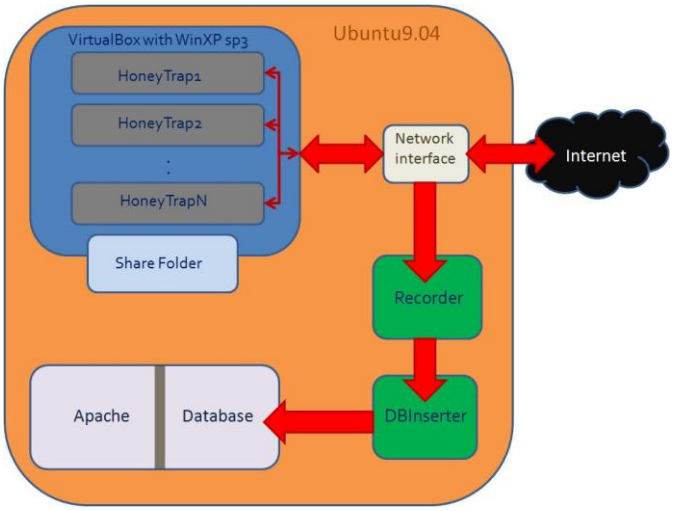

圖 8：malware 網路行為分析系統示意圖

當各虛擬機器自 Share Folder 處抓取 malware 回來執行後，在 malware 透過預設的 network interface 端與外界溝通的同時，所產生的網路流量會被 recorder 錄製儲存下來交給 DBInserter 來檢查分析所產生的 PCAP 流量檔，分析的結果再被上傳至後端的 Database 存放，之後使用者可以透過系統提供的網頁介面來檢視結果或下載 malware 相關流量檔。

五、 結果與討論

在樣本收集的成果部分—從系統上線後已經收集了兩萬多個可疑檔案，其中確認為惡意軟體的(四

家防毒軟體均有定義)有 1183 個；但若以 Kaspersky、Avira 及 ESET NOD32 三家防毒軟體定義來算的話，總數有 5884 個。圖 9 是系統透過網頁查詢統計資料的介面。此外，表 1 則是關於在收集 malware 過程中各家防毒軟體的反應速度結果。

在錄製分析 malware 主機行為的成果部分—根據分析結果，我們將 malware 的主機行為分為三種：(1)Typical：不正常地改變 registry 及檔案系統、(2)Strange：不正常地改變檔案系統，及(3)No Action：沒有不正常地改變。所謂『不正常地改變』是指不在單純開關機以內的操作行為，例如檔案系統在開關機前後會有一些記錄檔的變動，像是記錄時間、記錄某些程式關機前的狀態等；只要排除掉這些對照資料對檔案系統做的改變後，就可以找出因為執行 malware 而對 registry 及檔案系統所做的改變。圖 10 是利用執行 475 個 malware samples 所得到的行為比例示意圖。在這項測試中發現，最多有 23.78%(= 16% No Action + 7.78% Excluded from No Action)的 malware 是無法用這四種防毒軟體偵測出來的—不僅包含系統的漏判外，還包含了因為 malware 無法被執行的情況。

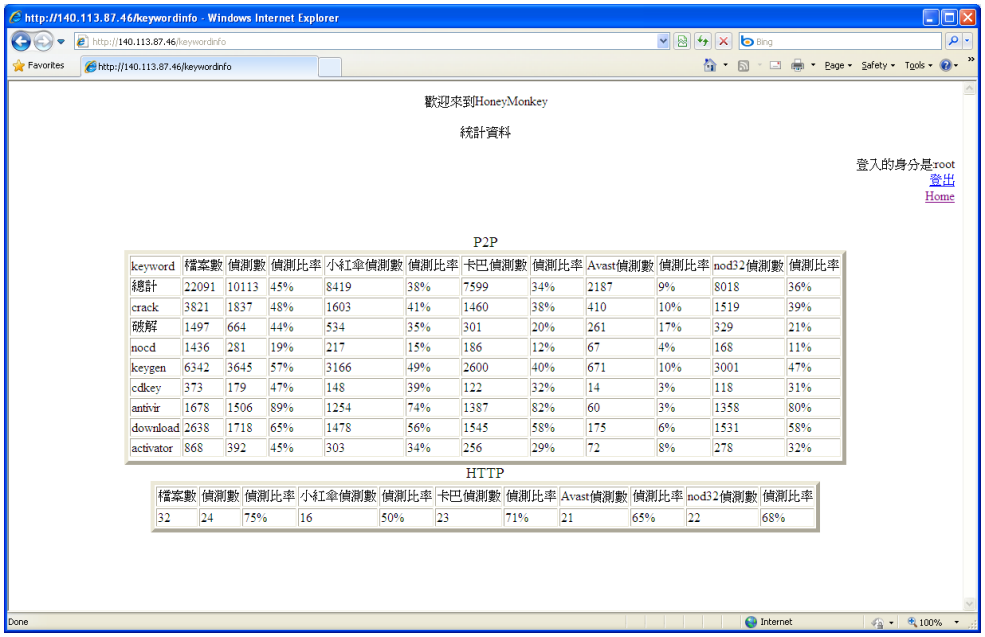

圖 9：HoneyMokey 提供的統計資料查詢介面

表 1：四家防毒軟體反應速度比較結果

	Kaspersky	Avira	Avast	Nod32
1st time scan	★★★★★	★★★★☆	★☆☆☆☆	★★★☆☆
Rescan	★★★★☆	★★★☆☆	★☆☆☆☆	★★★★★
Total	★★★☆☆	★★★★★	★☆☆☆☆	★★★★☆

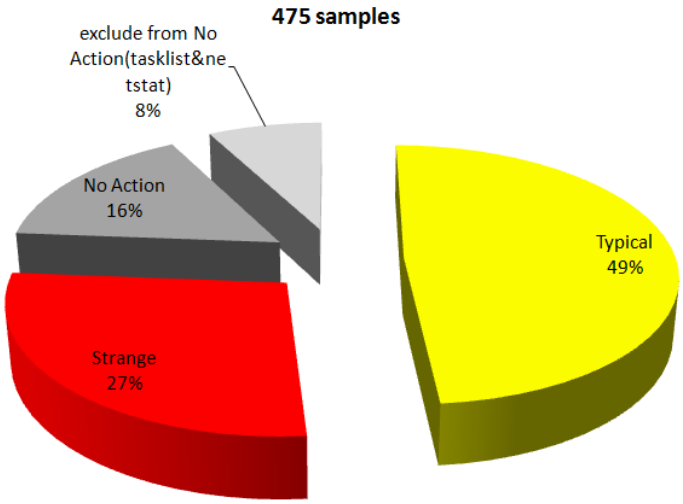

圖 10：475 個 malware samples 的行為比例示意圖

所以我們可以發現，透過主動式 honeypot—HoneyMonkey 的輔助，確實可以提高收集 malware 的效率、增加收集的 malware 數量，甚至可以收集到比防毒軟體廠商提供定義還更早的 malware；而且透過監控 malware 的主機行為，我們也發現，malware 在入侵主機後為了確保自身可以持續地運作，至少會在 registry 或檔案系統中擇一修改，也因為這樣的修改動作提高了後續清除動作的難度，因為很不容易找出所有被修改過的欄位或資料並予以徹底清楚乾淨，使得感染率或是復發比率居高不下；此外，透過所設計開發的網路行為分析架構，目前已經可以完整地錄製下 malware 執行時所產生的網路行為流量，降低行為分析的困難度。

本計劃執行迄今已獲得多項成果：建置一適用Anti-Malware與Anti-Botnet的實地與重播測試環境與機制、設計開發蒐集惡意軟體及殭屍網路相關流量的誘捕機制、實際蒐集各種真實惡意軟體及殭屍網路相關流量、萃取重組出真正相關的各session真實惡意軟體與殭屍網路流量、產出研究報告、培育碩博士學生持續進行相關研究與訓練，並與網通資安設備(如合勤科技、威播科技、利基網路等)進行合作執行資安產品測試案；在追求相關測試技術研究發展外，也協助國內相關廠商進行各種資安產品測試與除錯。

網路持續發展，各種擁有複雜網路行為的網路應用程式層出不窮、使用者使用網通產品的情境與各種惡意軟體與殭屍網路流量行為途徑也日趨複雜及難以預料，光靠實驗室測試及人造流量來進行測試是不夠的，此特性在高階資安產品的測試上尤為顯著。期望透過此項計畫的執行成果，能對國內相關產業界提供另一產品測試機制，並正視真實流量在未來高階資安產品測試的重要性。

國科會補助計畫衍生研發成果推廣資料表

日期:2011/10/31

國科會補助計畫	計畫名稱: 子計畫三:資安技術反惡意軟體及反殭屍網路真實流量評比
	計畫主持人: 陳昌盛
	計畫編號: 99-2218-E-009-016- 學門領域: 資訊

無研發成果推廣資料

99 年度專題研究計畫研究成果彙整表

計畫主持人：陳昌盛	計畫編號：99-2218-E-009-016-
計畫名稱：資安技術真實流量實地評比--子計畫三:資安技術反惡意軟體及反殭屍網路真實流量評比	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	2	2	100%		
		研討會論文	1	1	100%		
		專書	0	0	0%		
	專利	申請中件數	1	1	100%	件	
		已獲得件數	0	0	0%		
	技術移轉	件數	0	0	0%	件	
		權利金	0	0	0%	千元	
	參與計畫人力（本國籍）	碩士生	3	2	150%	人次	
		博士生	1	2	50%		
		博士後研究員	0	0	0%		
		專任助理	0	0	0%		
國外	論文著作	期刊論文	1	1	100%	篇	
		研究報告/技術報告	0	0	0%		
		研討會論文	0	0	0%		
		專書	0	0	0%	章/本	
	專利	申請中件數	0	0	0%	件	
		已獲得件數	0	0	0%		
	技術移轉	件數	0	0	0%	件	
		權利金	0	0	0%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	0%	人次	
		博士生	0	0	0%		
		博士後研究員	0	0	0%		
		專任助理	0	0	0%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	本計劃執行迄今已獲得多項成果:建置一適用 Anti-Malware 與 Anti-Botnet 的實地與重播測試環境與機制、設計開發蒐集惡意軟體及殭屍網路相關流量的誘捕機制、實際蒐集各種真實惡意軟體及殭屍網路相關流量、萃取重組出真正相關的各 session 真實惡意軟體與殭屍網路流量、產出研究報告、培育碩博士學生持續進行相關研究與訓練，並與網通資安設備(如合勤科技、威播科技、利基網路等)進行合作執行資安產品測試案；在追求相關測試技術研究發展外，也協助國內相關廠商進行各種資安產品測試與除錯。

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 ■申請中 □無

技轉：□已技轉 □洽談中 ■無

其他：(以 100 字為限)

子計畫三,

1. 發表國外期刊論文一篇, 國內會議論文一篇. 另外正撰寫一篇論文, 擬投搞國際期刊.

2. 目前有一項, Botnet 相關的自動化分類專利, 正在申請中.

3. 產學合作方面, 本計畫與國內資安廠商<威播科技>, 共同研發(合作金額 560,000) 資安偵測技術及資安防禦技術

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以 500 字為限）

本計劃執行迄今已獲得多項成果：建置一適用 Anti-Malware 與 Anti-Botnet 的實地與重播測試環境與機制、設計開發蒐集惡意軟體及殭屍網路相關流量的誘捕機制、實際蒐集各種真實惡意軟體及殭屍網路相關流量、萃取重組出真正相關的各 session 真實惡意軟體與殭屍網路流量、產出研究報告、培育碩博士學生持續進行相關研究與訓練，並與網通資安設備(如合勤科技、威播科技、利基網路等)進行合作執行資安產品測試案；在追求相關測試技術研究發展外，也協助國內相關廠商進行各種資安產品測試與除錯。