# 行政院國家科學委員會專題研究計畫 成果報告

## 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 ：個別型
計 畫 編 號 ：NSC 100-2218-E-009-019-
執 行 期 間 ：100 年 08 月 01 日至 101 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：蘇俊憲
碩士班研究生-兼任助理人員：方智誼
碩士班研究生-兼任助理人員：黃翊綾

公 開 資 訊 ：本計畫可公開查詢

中 華 民 國 101 年 11 月 01 日

中 文 摘 要 ： 傳統的 Honyepot 誘捕機制，主要在於建置一個(或一群)具有許多漏洞的系統，以被動等待入侵的方式 (等待惡意程式或 Bot 前來入侵攻擊)藉此蒐集惡意程式樣本、入侵的方法及可能造成的系統影響等；但這樣的方式也常因為受限於時間過長、網路頻寬、網路架構，以及資安防護系統等因素，成效及搜集到的樣本有沒有代表性而有很大差異。
本計畫的目的在於規劃及設計一個自動化的 Anti-Malware & Anti-Botnet 的資安偵防技術測試平台，整合 Malware & Botnet 之誘補、偵測、行為分析等措施，希望能夠透過此平台促進 Anti-Malware & 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。本計畫延續去年的研究方式，並增加研究的資安設備種類，以期更能涵蓋更完整的技術，經由比較產生一個更實用的平台解決建議方案，並累積相關的測試技術。

中文關鍵詞： 反制惡意程式, 反制殭屍電腦網路, 資安偵防技術測試平台

英 文 摘 要 ：

英文關鍵詞：

## 一、 前言

**惡意程式(malware)**

近年來惡意軟體急速增加，根據 Kaspersky Lab 的 2009 年度安全報告數據顯示，在過去 15 年(1992~2007)間，發現了約 200 萬個新型惡意軟體，其中在 2008 年一年中，就發現超過 1500 萬個，截至 2009 年，Kaspersky Lab 收集到的惡意軟體總量已經達到 3390 萬個之多。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。

**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 或是 Robot Network。Bots 通常是隨著 email、Instant Message Software 或是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。隨著 Bots 結構及本身行為越來越複雜，Bots 躲避資安偵測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、使用 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 Botnet 也被視為現今網際網路上最大的安全威脅。

目前已知偵測 Botnet 的方式大致上有系統與網路兩種方式；系統方式處理的，主要是利用偵測病毒、偵測 Rootkit 的機制[9]或是監看網路的作法；網路方式則是利用 Honeypot project (被動式 Botnet 誘捕系統)[10]、Behavior/Log analysis (多層次網路行為、流量分析)[11~14]、SPAM signature[15]等方式偵測。這兩種方式都是需要長期監控網路，希望利用收集 Bot 的行為模式以便作為偵防時的參考。

**流量來源(Traffic Source)**

此計畫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有同學長期使用各種網路應用程式所產生的網路流量。每台 switch 有 2 個 link 連回交通大學計中的 router (BetaSite 7609)。BetaSite 7609 對外共有 3 條線路，分別連接 TANET、Internet，以及 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自動化的 Anti-Malware & Anti-Botnet 的資安偵防技術測試平台，整合 Malware & Botnet 之誘補、偵測、行為分析等措施，希望能夠透過此平台促進 Anti-Malware & 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。

從一般使用者的使用經驗中得知，常見的感染途徑包括 e-mail 、網頁瀏覽和 P2P 檔案傳送等網

路應用。傳統的 Honyepot 誘捕機制，主要在於建置一個(或一群)具有許多漏洞的系統，以被動等待入侵的方式 (等待惡意程式或 Bot 前來入侵攻擊)藉此蒐集惡意程式樣本、入侵的方法及可能造成的系統影響等；但這樣的方式也常因為受限於時間過長、網路頻寬、網路架構，以及資安防護系統等因素，成效及搜集到的樣本有沒有代表性而有很大差異。因此本計畫中，除了佈建傳統的 Honeypot 方式之外，我們另外也模擬一般使用者的行為，設計一個逆向主動蒐集惡意程式的系統，蒐集下來的惡意軟體經過分析、整理出行為模式後，記錄進資料庫以便後續作更進一步的研究探討。

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

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

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

[12] 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.

[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.

[16] GFI ThreatTrack, http://www.threattrack.com .

[17] virustotal, http://www.virustotal.com .

[18] I. Firdausi, C. Lim, A. Erwin, and A. S. Nugroho, “Analysis of machine learning techniques used in

behavior-based malware detection," in *Proceedings of the 2nd International Conference on Advances in Computing, Control and Telecommunication Technologies (ACT)*, pp. 201-203, December 2010.

## 四、 研究方法

本計劃預期的成果是收集 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)、樣本行為分析(Behavior Analysis)及記錄(Event logging)三部分。在樣本收集方面，除了持續透過交大 Beta Site 平台，取得各式各樣可疑惡意程式樣本外，也開發一『主動式收集 malware 及 botnet 樣本平台』；在樣本行為分析方面，開發一『惡意軟體行為分析系統』，分別在監控的環境中有限制執行範圍的方式執行各個 malware 及 botnet 樣本，並觀察記錄執行期間的主機行為(host behavior)及網路行為(network behavior)等行為訊息；在記錄部分，則將萃取並分析過後的 malware 樣本整合進真實流量資料庫『PCAP Library』中儲存。

### 主動式收集平台

圖 1 是我們開發的系統整體流程圖，包含四個元件：

- *Active Bot Collector*，包含 WWW、P2P、MAIL 三種蒐集 malware/bot 流量的途徑，主要是模擬人類使用 WWW、P2P、Mail 時的操作，利用預先定義的關鍵字在 Beta Site 環境中進行搜尋，並刻意地下載各式各樣的 suspicious binaries 並儲存到 database；
- *Scanning module*，包含 15 種 anti-virus 軟體(即 Avast6-Pro、AVG、BitDefender、Bullguard Anti-Virus、F-Secure、G Data、McAfee Anti-Virus、Panda 2012、SOPHOS 2011 Anti-Virus、PC-cillin 2012 雲端版、Avira、Avast、Kaspersky、NOD32、Symantec)；Scanning module 會從 database 中下載 suspicious binaries 並進行掃瞄比對，判斷是否為 malware/bot 流量；只要有一項防毒軟體認為是，系統就將該流量標示為是，然後進一步交由後續兩元件做處理；
- *Information Collecting VMs*，用來蒐集各項 malware/bot 資訊，包括 host 端資訊(如 registry、disk 及 system call id sequence)、network 端資訊；
- *Analysis module*，利用 sandbox 技術來分析 malware/bot 的網路行為及 screenshot。

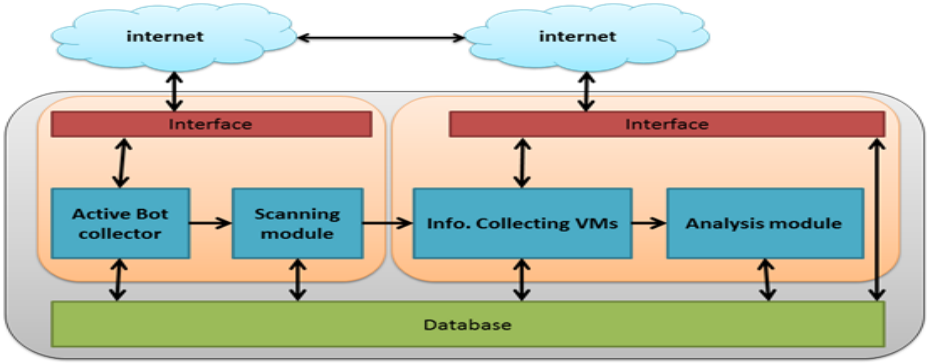



圖 1、主動式收集平台(malware tool chain)架構

圖 2 為 *Active bot collector* 之執行架構，WWW module 經由瀏覽 URL，將 URL 上的 Suspicious Binary 下載下來放至 database；MAIL module 會將收下來的 mail 作分析，把 URL 傳給 WWW，將 mail 中的附件上傳到 database；P2P 則藉由關鍵字作下載搜尋，將下載的檔案存至 database。

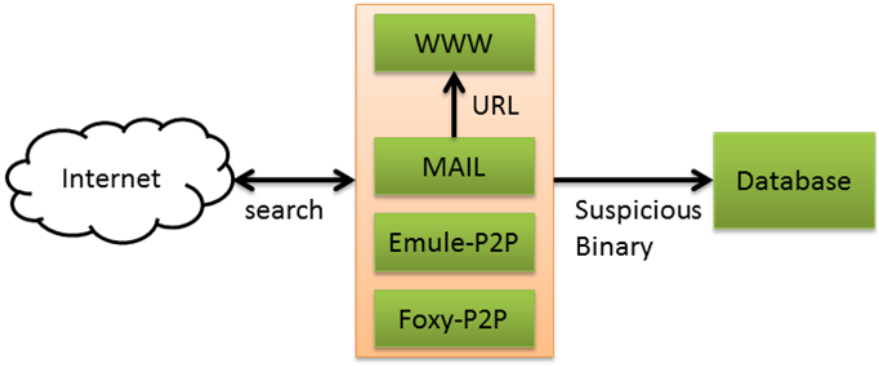



圖 2、Active collector 架構

在圖 3 中，*Scanning module* 會從 database 取得 suspicious binary，然後對檔案進行掃瞄比對。此 Module 是由 database 以及安裝有防毒軟體的 VM 組成，目前選用的防毒軟體為市面上較常見的 anti-virus 軟體(包括 Avast6-Pro、AVG、BitDefender、Bullguard Anti-Virus、F-Secure、G Data、McAfee Anti-Virus、Panda 2012、SOPHOS 2011 Anti-Virus、PC-cillin 2012 雲端版、Avira、Avast、Kaspersky、Nod32、Symantec)。由於各家防毒軟體都有自己的 malware definitions，scan module 若判定是 malware，則會將掃瞄結果寫入總表，若判定不是 malware 則會記錄時間，並根據 rescan 機制的排程結果，進行周期性的 rescan。

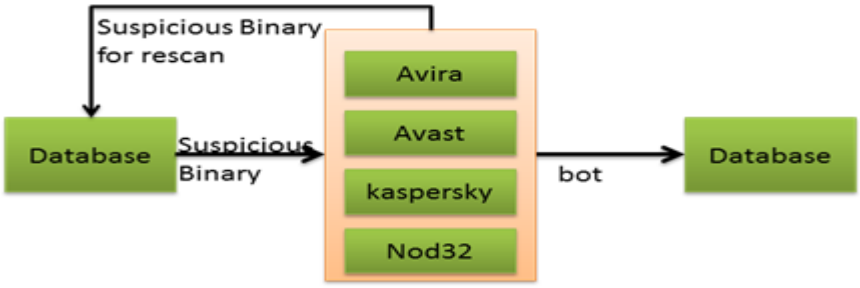



圖 3、scanning module 架構

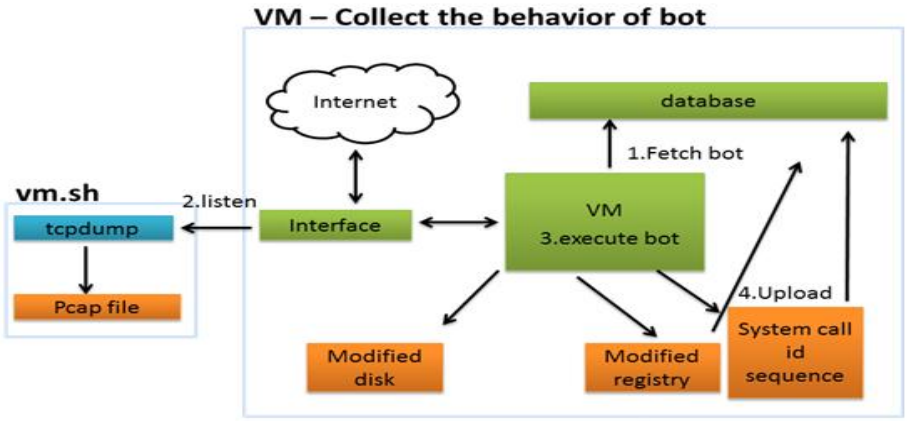



圖 4、information collection module 架構

圖 4 是 information collection 部分，將 VM 做些設定，然後啟動 VM 並同時錄製封包。VM 會主動從 database 中抓取 bot 然後執行，等待錄製時間後，將 registry 上傳並關機。System call id 則是在執行 bot 的過程中，利用 pin tool 偵測 system call 後直接上傳。

在樣本的行為分析部分，為了能夠觀察更多關於 malware/bot 的特性，analysis module 結合了

sandbox 技術來做進一步的行為分析；將 suspicious binary 上傳至 GFI ThreatTrack[16]，透過 sandbox 技術動態地分析該 suspicious binary 所擁有的 malware 特性有哪些，再存入資料庫中。

圖 5 是此收集平台的登入畫面，登入後會提供簡短的統計資訊，包括有目前系統效能及 Module 平均執行時間。圖 6 則是利用系統登入畫面上方的『Collector』功能，可以看到目前存在系統中的 malware/bot 摘要資訊。如果想觀看系統內搜集到的惡意軟體或殭屍網路流量的詳細資訊，可以選擇『Bot Info』功能(如圖 7)。在系統中，每一筆惡意流量記錄是以該流量的 SHA code 作為索引、錄製來源、大小等，並記錄各防毒軟體的偵測結果以方便後續分析利用(如圖 8)。

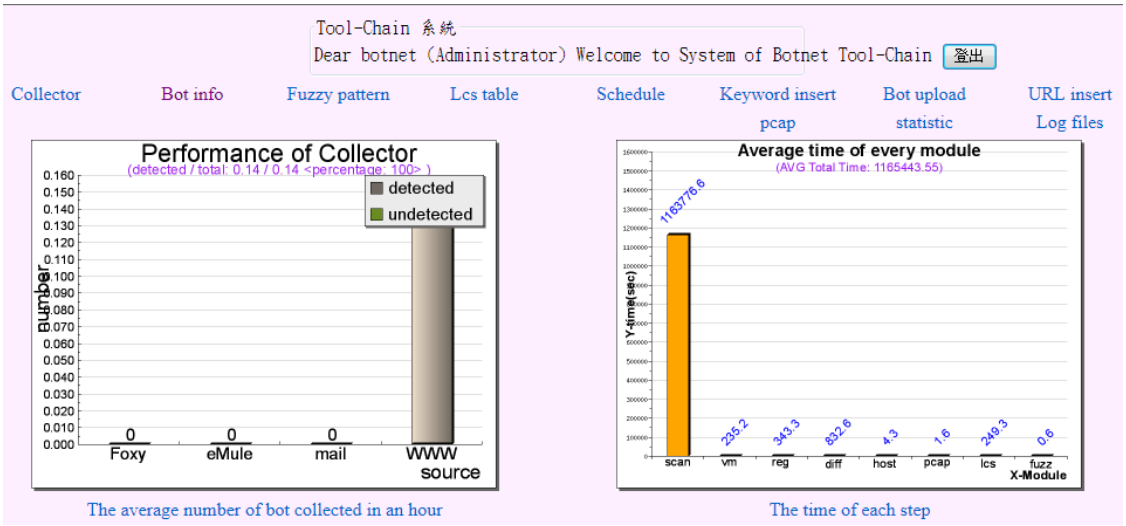
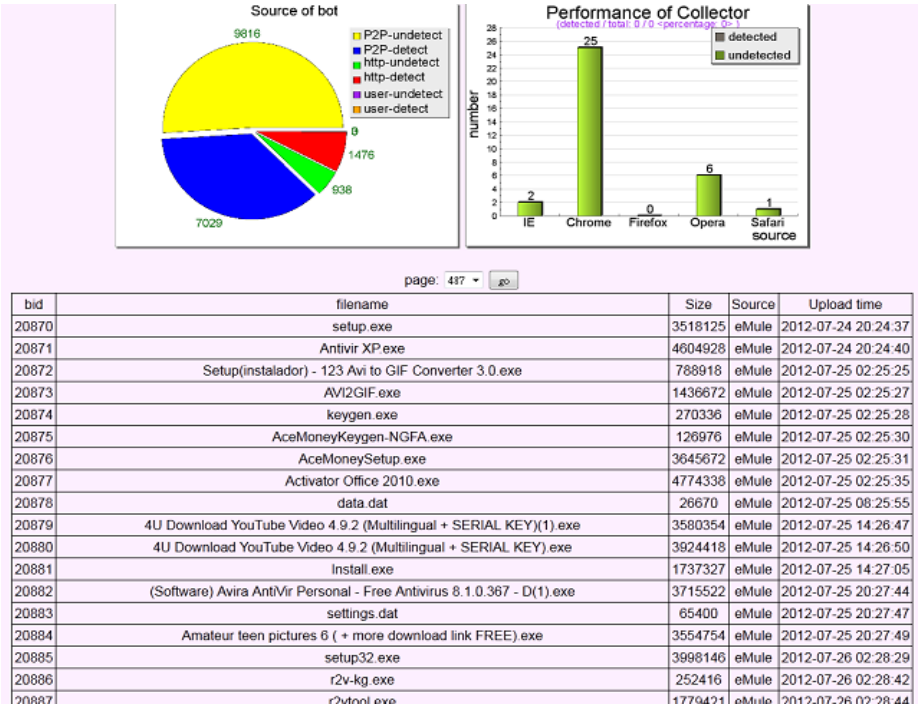


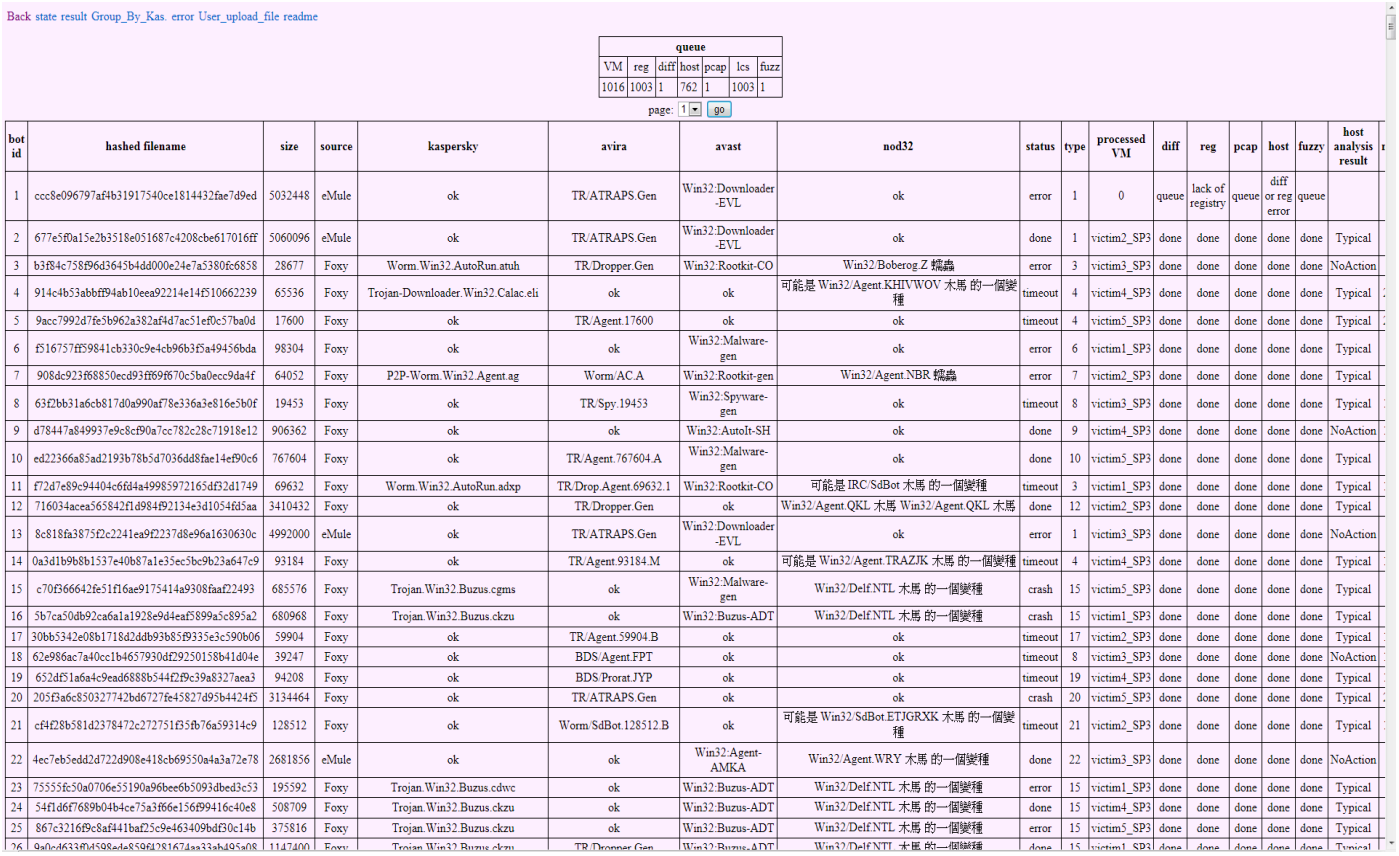

圖 5、主動式收集平台登入畫面




| bid | filename | Size | Source | Upload time |
|---|---|---|---|---|
| 20870 | setup.exe | 3518125 | eMule | 2012-07-24 20:24:37 |
| 20871 | Antivir XP.exe | 4604928 | eMule | 2012-07-24 20:24:40 |
| 20872 | Setup(instalador) - 123 Avi to GIF Converter 3.0.exe | 788918 | eMule | 2012-07-25 02:25:25 |
| 20873 | AVI2GIF.exe | 1436672 | eMule | 2012-07-25 02:25:27 |
| 20874 | keygen.exe | 270336 | eMule | 2012-07-25 02:25:28 |
| 20875 | AceMoneyKeygen-NGFA.exe | 126976 | eMule | 2012-07-25 02:25:30 |
| 20876 | AceMoneySetup.exe | 3645672 | eMule | 2012-07-25 02:25:31 |
| 20877 | Activator Office 2010.exe | 4774338 | eMule | 2012-07-25 02:25:35 |
| 20878 | data.dat | 26670 | eMule | 2012-07-25 08:25:55 |
| 20879 | 4U Download YouTube Video 4.9.2 (Multilingual + SERIAL KEY)(1).exe | 3580354 | eMule | 2012-07-25 14:26:47 |
| 20880 | 4U Download YouTube Video 4.9.2 (Multilingual + SERIAL KEY).exe | 3924418 | eMule | 2012-07-25 14:26:50 |
| 20881 | Install.exe | 1737327 | eMule | 2012-07-25 14:27:05 |
| 20882 | (Software) Avira AntiVir Personal - Free Antivirus 8.1.0.367 - D(1).exe | 3715522 | eMule | 2012-07-25 20:27:44 |
| 20883 | settings.dat | 65400 | eMule | 2012-07-25 20:27:47 |
| 20884 | Amateur teen pictures 6 ( + more download link FREE).exe | 3554754 | eMule | 2012-07-25 20:27:49 |
| 20885 | setup32.exe | 3998146 | eMule | 2012-07-26 02:28:29 |
| 20886 | r2v-kg.exe | 252416 | eMule | 2012-07-26 02:28:42 |
| 20887 | r2vtool.exe | 1779421 | eMule | 2012-07-26 02:28:44 |

圖 6、Malware/Bot 摘要資訊

『Bot Info』提供的欄位資訊依序包括了：hashed filename、檔案大小、收集的軟體來源、多個防毒軟體、狀態、差異、執行的 VM、對 registry 行為，及有無經 fuzzy 測試等。



Back state result Group_By_Kas. error User_upload_file readme

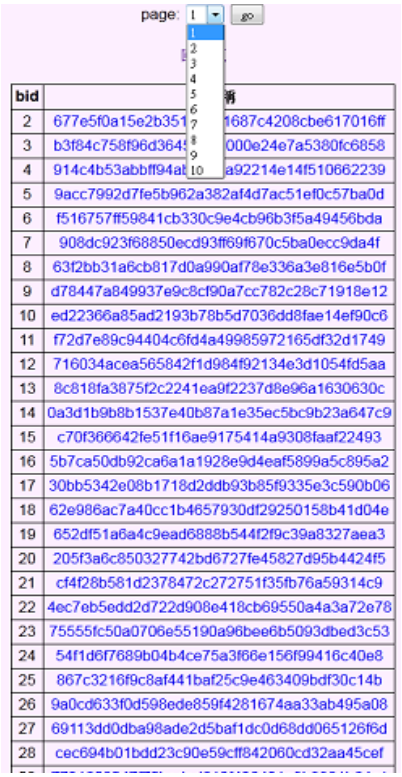
queue

| VM | reg | diff | host | pcap | lcs | fuzz |
|---|---|---|---|---|---|---|
| 1016 | 1003 | 1 | 762 | 1 | 1003 | 1 |

page: 1 go

| bot id | hashed filename | size | source | kaspersky | avira | avast | nod32 | status | type | processed VM | diff | reg | pcap | host | fuzzy | host analysis result |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ccc8e096797af4b31917540ce1814432fae7d9ed | 5032448 | eMule | ok | TR/ATRAPS.Gen | Win32:Downloader-EVL | ok | error | 1 | 0 | queue | lack of registry | queue | diff or reg error | queue | |
| 2 | 677e5f0a15e2b3518e051687c4208cbe617016ff | 5060096 | eMule | ok | TR/ATRAPS.Gen | Win32:Downloader-EVL | ok | done | 1 | victim2_SP3 | done | done | done | done | done | Typical |
| 3 | b3f84c758f96d3645b4dd000e24e7a5380fc6858 | 28677 | Foxy | Worm.Win32.AutoRun.atuh | TR/Dropper.Gen | Win32:Rootkit-CO | Win32/Boberog.Z 蠕蟲 | error | 3 | victim3_SP3 | done | done | done | done | done | NoAction |
| 4 | 914c4b53abbff94ab10eea92214e14f510662239 | 65536 | Foxy | Trojan-Downloader.Win32.Calac.eli | ok | ok | 可能是 Win32/Agent.KHIVWOV 木馬 的一個變種 | timeout | 4 | victim4_SP3 | done | done | done | done | done | Typical |
| 5 | 9acc7992d7fe5b962a382af4d7ac51ef0c57ba0d | 17600 | Foxy | ok | TR/Agent.17600 | ok | ok | timeout | 4 | victim5_SP3 | done | done | done | done | done | Typical |
| 6 | f516757ff59841cb330c9e4cb96b3f5a49456bda | 98304 | Foxy | ok | ok | Win32:Malware-gen | ok | error | 6 | victim1_SP3 | done | done | done | done | done | Typical |
| 7 | 908dc923f68850ecd93ff69f670c5ba0ecc9da4f | 64052 | Foxy | P2P-Worm.Win32.Agent.ag | Worm/AC.A | Win32:Rootkit-gen | Win32/Agent.NBR 蠕蟲 | error | 7 | victim2_SP3 | done | done | done | done | done | Typical |
| 8 | 63f2bb31a6cb817d0a990af78e336a3e816e5b0f | 19453 | Foxy | ok | TR/Spy.19453 | Win32:Spyware-gen | ok | timeout | 8 | victim3_SP3 | done | done | done | done | done | Typical |
| 9 | d78447a849937e9c8cf90a7cc782c28c71918e12 | 906362 | Foxy | ok | ok | Win32:AutoIt-SH | ok | done | 9 | victim4_SP3 | done | done | done | done | done | NoAction |
| 10 | ed22366a85ad2193b78b5d7036dd8fae14ef90c6 | 767604 | Foxy | ok | TR/Agent.767604.A | Win32:Malware-gen | ok | done | 10 | victim5_SP3 | done | done | done | done | done | Typical |
| 11 | f72d7e89c94404c6fd4a49985972165df32d1749 | 69632 | Foxy | Worm.Win32.AutoRun.adxp | TR/Drop.Agent.69632.1 | Win32:Rootkit-CO | 可能是 IRC/SdBot 木馬 的一個變種 | timeout | 3 | victim1_SP3 | done | done | done | done | done | Typical |
| 12 | 716034acea565842f1d984f92134e3d1054fd5aa | 3410432 | Foxy | ok | TR/Dropper.Gen | ok | Win32/Agent.QKL 木馬 Win32/Agent.QKL 木馬 | done | 12 | victim2_SP3 | done | done | done | done | done | Typical |
| 13 | 8c818fa3875f2c2241ea9f2237d8e96a1630630c | 4992000 | eMule | ok | TR/ATRAPS.Gen | Win32:Downloader-EVL | ok | error | 1 | victim3_SP3 | done | done | done | done | done | NoAction |
| 14 | 0a3d1b9b8b1537e40b87a1e35ec5bc9b23a647c9 | 93184 | Foxy | ok | TR/Agent.93184.M | ok | 可能是 Win32/Agent.TRAZJK 木馬 的一個變種 | timeout | 4 | victim4_SP3 | done | done | done | done | done | Typical |
| 15 | c70f366642fe51f16ae9175414a9308faaf22493 | 685576 | Foxy | Trojan.Win32.Buzus.cgms | ok | Win32:Malware-gen | Win32/Delf.NTL 木馬 的一個變種 | crash | 15 | victim5_SP3 | done | done | done | done | done | Typical |
| 16 | 5b7ca50db92ca6a1a1928e9d4eaf5899a5c895a2 | 680968 | Foxy | Trojan.Win32.Buzus.ckzu | ok | Win32:Buzus-ADT | Win32/Delf.NTL 木馬 的一個變種 | crash | 15 | victim1_SP3 | done | done | done | done | done | Typical |
| 17 | 30bb5342e08b1718d2ddb93b85f9335e3c590b06 | 59904 | Foxy | ok | TR/Agent.59904.B | ok | ok | timeout | 17 | victim2_SP3 | done | done | done | done | done | Typical |
| 18 | 62e986ac7a40cc1b4657930df29250158b41d04e | 39247 | Foxy | ok | BDS/Agent.FPT | ok | ok | timeout | 8 | victim3_SP3 | done | done | done | done | done | NoAction |
| 19 | 652df51a6a4c9ead6888b544f2f9c39a8327aea3 | 94208 | Foxy | ok | BDS/Prorat.JYP | ok | ok | timeout | 19 | victim4_SP3 | done | done | done | done | done | Typical |
| 20 | 205f3a6c850327742bd6727fe45827d95b4424f5 | 3134464 | Foxy | ok | TR/ATRAPS.Gen | ok | ok | crash | 20 | victim5_SP3 | done | done | done | done | done | Typical |
| 21 | cf4f28b581d2378472c272751f35fb76a59314c9 | 128512 | Foxy | ok | Worm/SdBot.128512.B | ok | 可能是 Win32/SdBot.ETJGRXK 木馬 的一個變種 | timeout | 21 | victim2_SP3 | done | done | done | done | done | Typical |
| 22 | 4ec7eb5edd2d722d908e418cb69550a4a3a72e78 | 2681856 | eMule | ok | ok | Win32:Agent-AMKA | Win32/Agent.WRY 木馬 的一個變種 | done | 22 | victim3_SP3 | done | done | done | done | done | NoAction |
| 23 | 75555fc50a0706e55190a96bee6b5093dbed3c53 | 195592 | Foxy | Trojan.Win32.Buzus.cdwc | ok | Win32:Buzus-ADT | Win32/Delf.NTL 木馬 的一個變種 | error | 15 | victim1_SP3 | done | done | done | done | done | Typical |
| 24 | 54f1d6f7689b04b4ce75a3f66e156f99416c40e8 | 508709 | Foxy | Trojan.Win32.Buzus.ckzu | ok | Win32:Buzus-ADT | Win32/Delf.NTL 木馬 的一個變種 | done | 15 | victim4_SP3 | done | done | done | done | done | Typical |
| 25 | 867c3216f9c8af441baf25c9e463409bdf30c14b | 375816 | Foxy | Trojan.Win32.Buzus.ckzu | ok | Win32:Buzus-ADT | Win32/Delf.NTL 木馬 的一個變種 | error | 15 | victim5_SP3 | done | done | done | done | done | Typical |
| 26 | 9a0cd633f0d598ede859f4281674aa33ab495a08 | 1147400 | Foxy | Trojan.Win32.Buzus.ckzu | TR/Dropper.Gen | Win32:Buzus-ADT | Win32/Delf.NTL 木馬 的一個變種 | done | 15 | victim1_SP3 | done | done | done | done | done | Typical |

圖 7、Malware/Bot 經過防毒軟體辨識的結果



page: 1 go

| bid | |
|---|---|
| 2 | 677e5f0a15e2b351 1687c4208cbe617016ff |
| 3 | b3f84c758f96d364 000e24e7a5380fc6858 |
| 4 | 914c4b53abbff94ab a92214e14f510662239 |
| 5 | 9acc7992d7fe5b962a382af4d7ac51ef0c57ba0d |
| 6 | f516757ff59841cb330c9e4cb96b3f5a49456bda |
| 7 | 908dc923f68850ecd93ff69f670c5ba0ecc9da4f |
| 8 | 63f2bb31a6cb817d0a990af78e336a3e816e5b0f |
| 9 | d78447a849937e9c8cf90a7cc782c28c71918e12 |
| 10 | ed22366a85ad2193b78b5d7036dd8fae14ef90c6 |
| 11 | f72d7e89c94404c6fd4a49985972165df32d1749 |
| 12 | 716034acea565842f1d984f92134e3d1054fd5aa |
| 13 | 8c818fa3875f2c2241ea9f2237d8e96a1630630c |
| 14 | 0a3d1b9b8b1537e40b87a1e35ec5bc9b23a647c9 |
| 15 | c70f366642fe51f16ae9175414a9308faaf22493 |
| 16 | 5b7ca50db92ca6a1a1928e9d4eaf5899a5c895a2 |
| 17 | 30bb5342e08b1718d2ddb93b85f9335e3c590b06 |
| 18 | 62e986ac7a40cc1b4657930df29250158b41d04e |
| 19 | 652df51a6a4c9ead6888b544f2f9c39a8327aea3 |
| 20 | 205f3a6c850327742bd6727fe45827d95b4424f5 |
| 21 | cf4f28b581d2378472c272751f35fb76a59314c9 |
| 22 | 4ec7eb5edd2d722d908e418cb69550a4a3a72e78 |
| 23 | 75555fc50a0706e55190a96bee6b5093dbed3c53 |
| 24 | 54f1d6f7689b04b4ce75a3f66e156f99416c40e8 |
| 25 | 867c3216f9c8af441baf25c9e463409bdf30c14b |
| 26 | 9a0cd633f0d598ede859f4281674aa33ab495a08 |
| 27 | 69113dd0dba98ade2d5baf1dc0d68dd065126f6d |
| 28 | cec694b01bdd23c90e59cff842060cd32aa45cef |

圖 8、可下載之 PCAP 檔列表

『statistics』功能則是列出了一天 24 小時內系統收集到的 malware/bot 檔案數量(圖 9)。

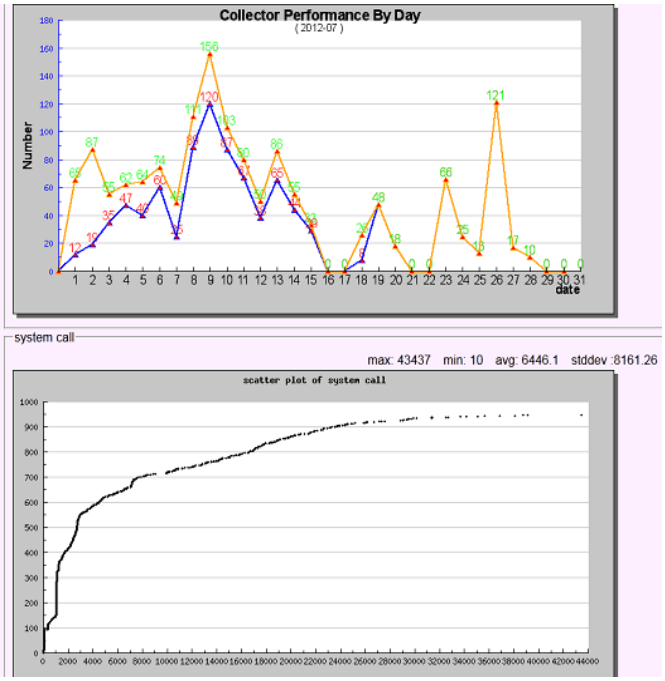



圖 9、statistic 功能

如果想要增減搜尋的關鍵字，可以透過圖 10 的介面，修改系統用來搜尋惡意軟體或是殭屍網路的關鍵字。

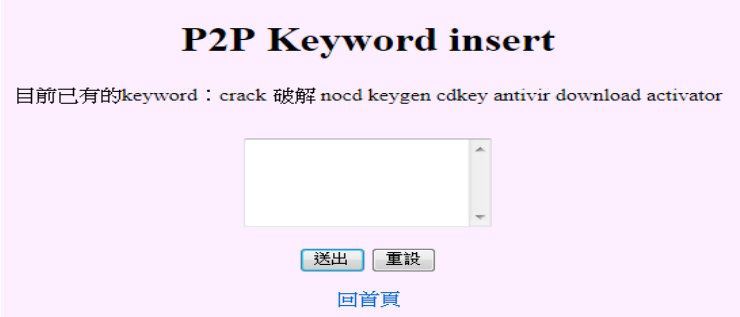
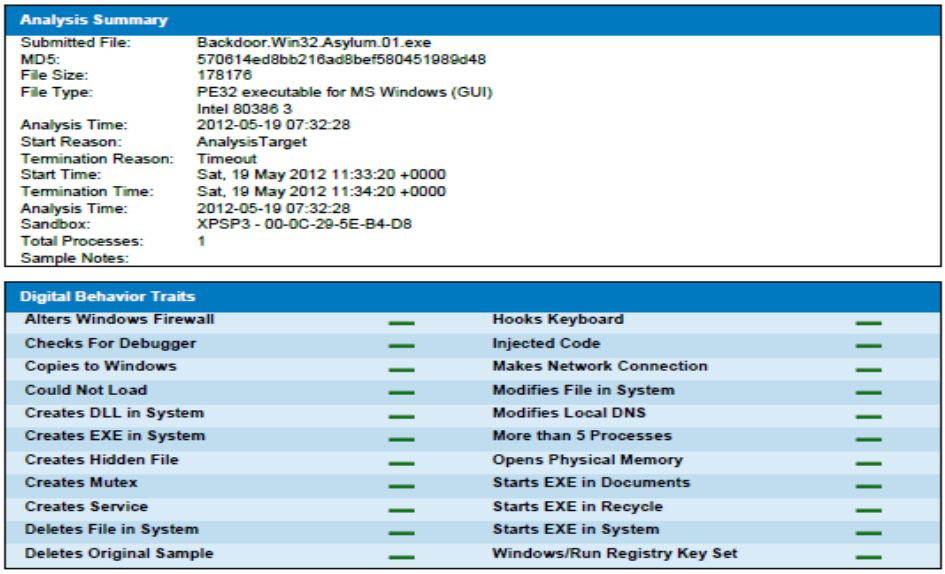



圖 10、增減關鍵字

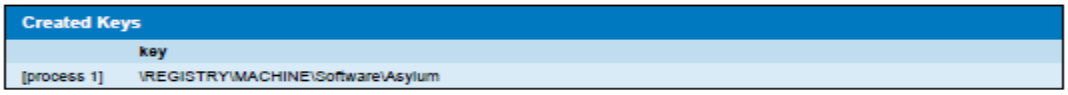
圖 11~14 是利用將 suspicious binary 上傳至 ThreatTrack[16]後，利用 sandbox 技術觀察該 suspicious binary 的行為分析結果，包括特性、對 registry 影響、造成的網路事件及 VirusTotal[17]分析等，再根據這些結果將所有 suspicious binary 分門別類儲存下來，作為後續研究分析。



| Analysis Summary | |
|---|---|
| Submitted File: | Backdoor.Win32.Asylum.01.exe |
| MD5: | 570614ed8bb216ad8bef580451989d48 |
| File Size: | 178176 |
| File Type: | PE32 executable for MS Windows (GUI) Intel 80386 3 |
| Analysis Time: | 2012-05-19 07:32:28 |
| Start Reason: | AnalysisTarget |
| Termination Reason: | Timeout |
| Start Time: | Sat, 19 May 2012 11:33:20 +0000 |
| Termination Time: | Sat, 19 May 2012 11:34:20 +0000 |
| Analysis Time: | 2012-05-19 07:32:28 |
| Sandbox: | XPSP3 - 00-0C-29-5E-B4-D8 |
| Total Processes: | 1 |
| Sample Notes: | |

| Digital Behavior Traits | | | |
|---|---|---|---|
| Alters Windows Firewall | — | Hooks Keyboard | — |
| Checks For Debugger | — | Injected Code | — |
| Copies to Windows | — | Makes Network Connection | — |
| Could Not Load | — | Modifies File in System | — |
| Creates DLL in System | — | Modifies Local DNS | — |
| Creates EXE in System | — | More than 5 Processes | — |
| Creates Hidden File | — | Opens Physical Memory | — |
| Creates Mutex | — | Starts EXE in Documents | — |
| Creates Service | — | Starts EXE in Recycle | — |
| Deletes File in System | — | Starts EXE in System | — |
| Deletes Original Sample | — | Windows/Run Registry Key Set | — |

圖 11、經 Sandbox 分析後的摘要資訊

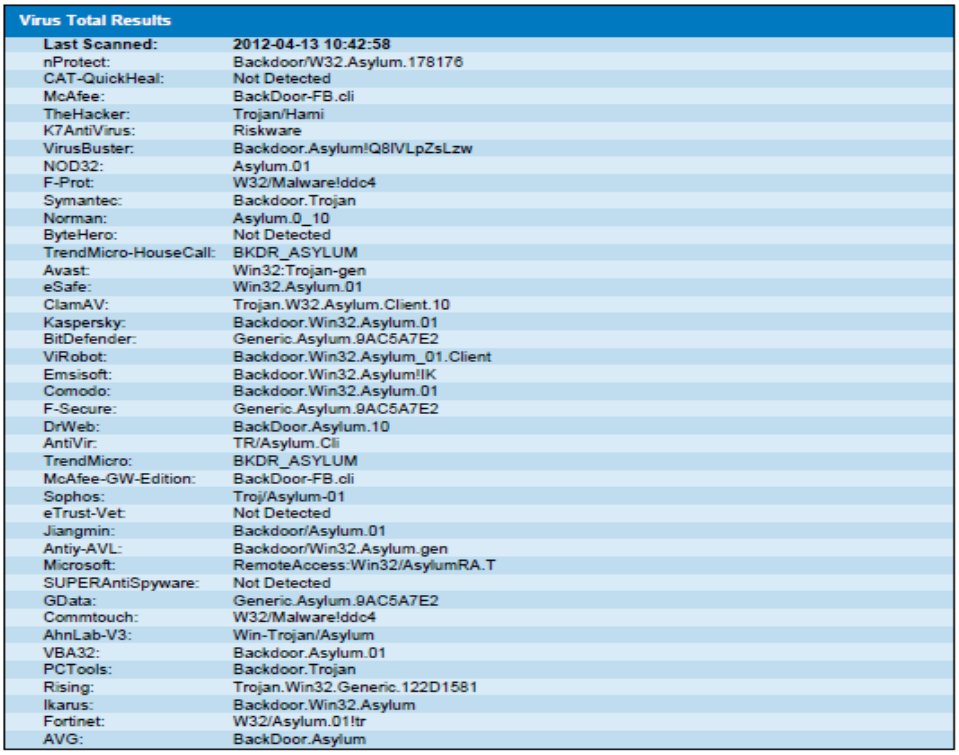


| Created Keys | |
|---|---|
| | key |
| [process 1] | \REGISTRY\MACHINE\Software\Asylum |

圖 12、該 suspicious binary 產生的 registry 行為

| Network Events | | | |
|---|---|---|---|
| | Remote IP | Local IP | HTTP Command |
| [process ] | | | none |

圖 13、該 suspicious binary 產生的 network 事件



| Virus Total Results | |
|---|---|
| Last Scanned: | 2012-04-13 10:42:58 |
| nProtect: | Backdoor/W32.Asylum.178176 |
| CAT-QuickHeal: | Not Detected |
| McAfee: | BackDoor-FB.cli |
| TheHacker: | Trojan/Hami |
| K7AntiVirus: | Riskware |
| VirusBuster: | Backdoor.Asylum!Q8lVLpZsLzw |
| NOD32: | Asylum.01 |
| F-Prot: | W32/Malware!ddc4 |
| Symantec: | Backdoor.Trojan |
| Norman: | Asylum.0_10 |
| ByteHero: | Not Detected |
| TrendMicro-HouseCall: | BKDR_ASYLUM |
| Avast: | Win32:Trojan-gen |
| eSafe: | Win32.Asylum.01 |
| ClamAV: | Trojan.W32.Asylum.Client.10 |
| Kaspersky: | Backdoor.Win32.Asylum.01 |
| BitDefender: | Generic.Asylum.9AC5A7E2 |
| ViRobot: | Backdoor.Win32.Asylum_01.Client |
| Emsisoft: | Backdoor.Win32.Asylum!IK |
| Comodo: | Backdoor.Win32.Asylum.01 |
| F-Secure: | Generic.Asylum.9AC5A7E2 |
| DrWeb: | BackDoor.Asylum.10 |
| AntiVir: | TR/Asylum.Cli |
| TrendMicro: | BKDR_ASYLUM |
| McAfee-GW-Edition: | BackDoor-FB.cli |
| Sophos: | Troj/Asylum-01 |
| eTrust-Vet: | Not Detected |
| Jiangmin: | Backdoor/Asylum.01 |
| Antiy-AVL: | Backdoor/Win32.Asylum.gen |
| Microsoft: | RemoteAccess:Win32/AsylumRA.T |
| SUPERAntiSpyware: | Not Detected |
| GData: | Generic.Asylum.9AC5A7E2 |
| Commtouch: | W32/Malware!ddc4 |
| AhnLab-V3: | Win-Trojan/Asylum |
| VBA32: | Backdoor.Asylum.01 |
| PCTools: | Backdoor.Trojan |
| Rising: | Trojan.Win32.Generic.122D1581 |
| Ikarus: | Backdoor.Win32.Asylum |
| Fortinet: | W32/Asylum.01!tr |
| AVG: | BackDoor.Asylum |

圖 14、suspicious binary 經 virustotal[17]分析結果

**惡意軟體行為分析系統**

圖 15 則是重播 suspicious binary 流量時所使用的重播測試方法與環境，左半邊是 Internet，右半邊則是 malware 分析環境，將 malware 在 sandbox 中執行起來，動態地觀察 malware 在執行前後及過程中產生的行為及影響，中間則是用來攔截及重導 malware 執行時所產生的惡意流量。傳統的動態分析會搭配封閉網路環境以避免 malware 在分析過程中攻擊到網際網路中的主機；可是現今的 malware 卻又大多需要網路連線運作，如果網路連線受到限制，malware 無法正常運作，容易造成分析結果不完整或是不具代表性。所以我們利用下列的 malware 重播方法，允許動態 malware 分析環境擁有看似無限制的網路存取權，並且利用流量分流器(dispatcher)透明地將惡意流量導入系統內的誘捕器(decoy)中，同時允許無害的控制流量存取網際網路，確保 malware 可以正常運作以進行分析。

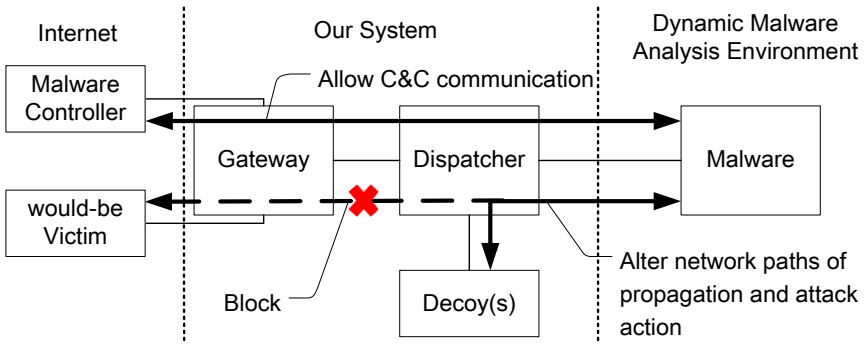



圖 15、惡意軟體行為分析系統

Dispatcher 有三個網路界面，NIC#1 與 malware 行為分析環境相接，NIC#2 與 Internet 相接，NIC#3 則與誘捕器相接(如圖 16)。當有流量從 NIC#1 進來時，此流量會同時 forward 到中間的 Coordinator 及內部 IDS；如果該流量來源端已經在黑名單(Blacklist)上或是觸發 IDS 發出 alert 的話，Coordinator 會判定該流量為惡意流量，並將該流量重導至誘捕器去；否則，該流量會被視為正常流量，直接從 NIC#2 流出；如果有流量從 NIC#2 進來時，該流量也會同時 forward 到 IDS 及 NIC#1 去。

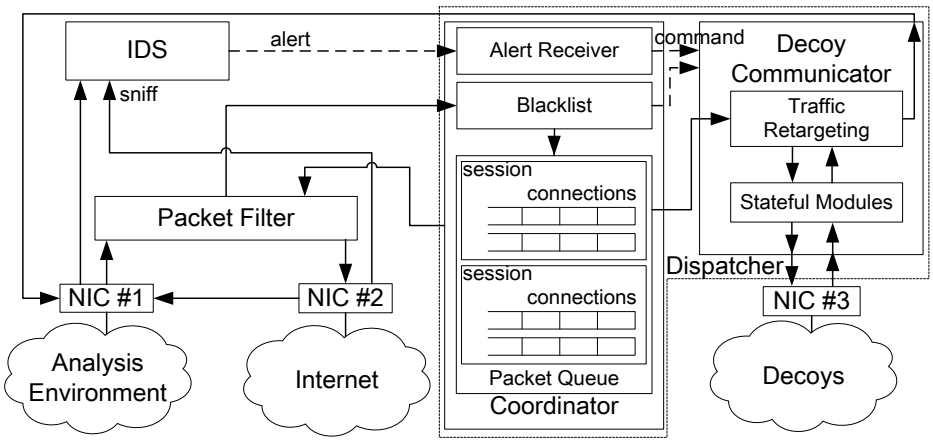



圖 16、Dispatch 架構

只有當兩種情況發生時，流量才會被重導進入誘捕器：(1)流量的來源端或是目的端在 Coordinator

的黑名單上，及(2)流量通過 IDS 時觸發 IDS alert。流量重導的時機可能發生在 session 剛起始時或是 session 結束前任一時段，因此，為了保持兩方交談狀態的一致性，所以在誘捕器中必須佈建多個 Stateful modules 來負責維持目前對話交談狀態。

## 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 25,669 個可疑檔案，移去重複或類似的檔案後，經確認為惡意軟體的(四家防毒軟體均有定義)有 1,276 個。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。

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 | ★★★☆☆ | ★★★★★ | ★☆☆☆☆ | ★★★★☆ |

在樣本行為分析方面，透過 sandbox 比對惡意樣本與正常樣本，我們發現兩種樣本間有 13 種行為是明顯不同出現機率的(如表 2)。

(1) Creates Mutex – Obtain the exclusive access to system resources[18]
(2) Creates Hidden File – Create file without the notification of the user
(3) Starts EXE in System – Execute EXE without the permission of the user
(4) Checks for Debugger – Check whether there is any anti-virus systems under the environment
(5) Starts EXE in Documents – Documents execute EXE automatically without the permission of the user
(6) Windows/Run Registry Key Set – Creation, modification, or deletion of Windows registry key
(7) Hooks Keyboard – Check keyboard values
(8) Modifies File in System – Modify files in the system permanently
(9) Deletes Original Sample – Delete the original sample
(10) More than 5 Processes – Create more than 5 processes
(11) Opens Physical Memory – Access physical memory
(12) Delete File in System – Delete a file in the system without the permission of the user
(13) Auto Start – Start automatically when the system reboots

表 2、惡意樣本與正常樣本行為比較

| No. | Behavior | Appearance frequency of a malicious sample | Appearance frequency of a benign sample |
|---|---|---|---|
| 1 | Creates Mutex | 53.8% | 2.4% |
| 2 | Creates Hidden File | 65.4% | 8.0% |

| | | | |
|---|---|---|---|
| 3 | Starts EXE in System | 54.4% | 11.0% |
| 4 | Checks for Debugger | 37.1% | 9.0% |
| 5 | Starts EXE in Documents | 34.0% | 1.4% |
| 6 | Windows/Run Registry Key Set | 72.0% | 3.2% |
| 7 | Hooks Keyboard | 25.4% | 2.0% |
| 8 | Modifies File in System | 28.6% | 3.4% |
| 9 | Deletes Original Sample | 16.0% | 0.6% |
| 10 | More than 5 Processes | 16.7% | 2.4% |
| 11 | Opens Physical Memory | 34.8% | 6.0% |
| 12 | Delete File in System | 15.4% | 3.0% |
| 13 | Auto Start | 35.6% | 0.0% |

此外，為了檢視『惡意軟體行為分析系統』，我們從惡意樣本中(前述四家防毒軟體判定)挑選出 124 個 malware 進行測試，經先期測試後移除沒有嘗試產生網路流量的，最後留下 12 個 malware(如表 3)。這 12 個可以再進一步分成兩群：Malware with C&C 及 Malware without C&C。

表 3、selected samples

| Type | Malware | Scan Result | Discovered | Activities |
|---|---|---|---|---|
| **Malware Without C&C** | m7.exe | Email-Worm.Win32.NetSky.q | Mar 24 2004 09:02 GMT | "Worm/NetSky.P" attachment |
| | m10.exe | Worm.Win32.Fujack.aa | Jul 02 2007 14:18 GMT | SMB password guessing |
| | m11.exe | Worm.Win32.Fujack.aa | Jul 02 2007 14:18 GMT | |
| | m12.exe | Worm.Win32.Viking.n | Aug 03 2006 22:09 GMT | |
| **Malware With C&C** | m1.exe | Trojan.Win32.Scar.bqfv | Feb 25 2010 16:09 GMT | SMB password guessing NETBIOS buffer overflow attempts |
| | m2.exe | Packed.Win32.Black.d Backdoor.Win32.Rbot.gen | Aug 06 2004 12:02 GMT | |
| | m3.exe | Trojan-PSW.Win32.Dybalom.bu | Aug 15 2009 09:06 GMT | |
| | m4.exe | P2P-Worm.Win32.Palevo.vyc | Mar 05 2010 12:11 GMT | |
| | m5.exe | Trojan-PSW.Win32.Dybalom.bu | Aug 15 2009 09:06 GMT | |
| | m6.exe | Trojan-PSW.Win32.Dybalom.bu | Aug 15 2009 09:06 GMT | |
| | m8.exe | Virus.Win32.Tenga.a | Jul 22 2005 17:11 GMT | Get e-mail content and recipient lists from the C&C |
| | m9.exe | Trojan-PSW.Win32.LdPinch.gqo | Feb 13 2009 15:42 GMT | |

表 4 比較了使用 closed network 與本系統觀察 malware without C&C 後得到的結果，其中的 closed network 是指沒有網路連線。m7.exe 會嘗試建立 SMTP 連線以便發送 spam e-mails、m10.exe 會透過

port 139 及 port 445 產生 369,199 個封包、m10.exe/m11.exe/m12.exe 都嘗試要透過 HTTP protocol 建立網路連線。

表 4、Malware without C&C 的網路事件

| Malware | Closed Network | Our system |
|---|---|---|
| **m7.exe** | No response for DNS MX record | 9 spam e-mail attempts |
| **m10.exe** | 362 TCP port 139 SYN packets<br>345 TCP port 445 SYN packets | 369199 packets for TCP port 139 and 445<br>HTTP GET advertising HTML files |
| **m11.exe** | 407 TCP port 139 SYN packets<br>388 TCP port 445 SYN packets | 23161 packets for TCP port 139 and 445<br>HTTP GET advertising HTML files |
| **m12.exe** | Probe machines by ICMP echo request | Probe machines by ICMP echo request<br>60285 packets for TCP port 139 and 445<br>HTTP GET advertising HTML files |

表 5 比較了使用 closed network 與本系統觀察 malware with C&C 後得到的結果。在 closed network 只能看到失敗的建立連線要求封包；但利用本系統，我們可以觀察到更多的 malware 行為，m4.exe 透過 port 47221 與某 IRC server 建立連線並嘗試下載 "TR/Kzay.15451.21"及透過 port 445 傳播；m8.exe 及 m9.exe 都是針對 Yahoo e-mail 服務的 spammers，他們會透過 port 80 與 C&C server 溝通，下載 e-mail subjects 及 e-mail recipients，然後開始發送 spam mails。

表 5、Malware with C&C 的網路事件

| Malware | Closed Network | Our system |
|---|---|---|
| **m1.exe** | No response for DNS A query<br>No response for TCP SYN | TCP C&C connection (60.165.98.198:8680) |
| **m2.exe** | No response for DNS A query | TCP C&C connection (70.107.249.167:6668)<br>TCP SYN flooding at port 139 after receiving "xvvv asn1smbnt 100 0 0 -b -r -s" command |
| **m3.exe**<br>**m5.exe**<br>**m6.exe** | No response for DNS A query | TCP C&C connection (74.117.174.122:16667)<br>TCP SYN flooding at port 445 after receiving ".advscan asn445 100 5 0 -b -r -s" command<br>FTP connection with non-standard port |
| **m4.exe** | No response for DNS A query | TCP C&C connection (46.161.29.202:47221)<br>HTTP GET "TR/Kazy.15451.21" after receiving ".asc -S -s\|.http http://black-cash.com/rep.exe\|.asc exp_all 10 0 0 -b -s\|.asc exp_all 20 0 0 -b -r -e –s" command<br>HTTP GET status report from other bots in the C&C channel<br>TCP SYN flooding at port 445 after receiving command |
| **m8.exe** | No response for DNS MX query<br>TCP SYN flooding at port 139 | TCP C&C connection (208.77.45.146:80)<br>TCP SYN flooding at port 139<br>34 spam e-mails |
| **m9.exe** | No response for DNS MX query | TCP C&C connection (208.77.45.146:80)<br>179 spam e-mails |

有些 malware/bot 在執行過程中會嘗試去偵測是否處在監控環境下，如果是，就會潛伏不建立連線，透過上述實驗可以發現，我們的系統在面對這些 malware/bot 時尤其有效。

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，並進行多項資安產品測試案；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:2012/10/31

| | |
|---|---|
| 國科會補助計畫 | 計畫名稱: 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: 100-2218-E-009-019- 學門領域: 推動計畫-資安 |

無研發成果推廣資料

# 100 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：**100-2218-E-009-019- |
| **計畫名稱：**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 | 1 | 1 | 100% | | |
| | | 研討會論文 | 1 | 1 | 100% | | |
| | | 專書 | 0 | 0 | 100% | | |
| | 專利 | 申請中件數 | 0 | 0 | 100% | 件 | |
| | | 已獲得件數 | 0 | 0 | 100% | | |
| | 技術移轉 | 件數 | 0 | 0 | 100% | 件 | |
| | | 權利金 | 0 | 0 | 100% | 千元 | |
| | 參與計畫人力（本國籍） | 碩士生 | 3 | 2 | 100% | 人次 | |
| | | 博士生 | 0 | 0 | 100% | | |
| | | 博士後研究員 | 0 | 0 | 100% | | |
| | | 專任助理 | 0 | 0 | 100% | | |
| 國外 | 論文著作 | 期刊論文 | 0 | 1 | 100% | 篇 | 投稿論文（’’’’How different are malware collected actively and passively’’’’, IEEE Computer), 目前正 revise 當中 |
| | | 研究報告/技術報告 | 0 | 0 | 100% | | |
| | | 研討會論文 | 0 | 0 | 100% | | |
| | | 專書 | 0 | 0 | 100% | 章/本 | |
| | 專利 | 申請中件數 | 0 | 0 | 100% | 件 | |
| | | 已獲得件數 | 0 | 0 | 100% | | |
| | 技術移轉 | 件數 | 0 | 0 | 100% | 件 | |
| | | 權利金 | 0 | 0 | 100% | 千元 | |
| | 參與計畫人力（外國籍） | 碩士生 | 0 | 0 | 100% | 人次 | |
| | | 博士生 | 0 | 0 | 100% | | |
| | | 博士後研究員 | 0 | 0 | 100% | | |
| | | 專任助理 | 0 | 0 | 100% | | |

| | |
|---|---|
| 其他成果<br>(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。) | 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。<br>本計劃建置一適用 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。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。 |

| | 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)

本研究團隊, 已撰寫一篇論文’’’’’’’’’ How Different are Malware collected actively and passively’’’’’’’’’, 投搞至 IEEE Computer(目前 under revision 中). 另外, 也已經在 TANET2012 發表一篇 DNSSEC 在資安防護上面的相關論文.

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，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。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。