

● 法務部調查局「駭客入侵防制系統」簡介

壹、前言

電腦與網路功能不斷增進，提供便利生活，提升政府機關行政效率，加速知識流通；「多用網路，少用馬路」，成為政府重要施政目標，e 化台灣、m 化政府，雲端建設等均為政府重大建設指標。

然而在電腦與網路大量運用之際，不法之徒悄悄地利用病毒程式、電腦系統漏洞、隱碼攻擊、網路釣魚、社交工程等手段，入侵及竊取電腦中重要資料檔案、個人資訊或帳號密碼，藉以獲取不法所得。

調查局為防範網路入侵事件不斷增加，建置「駭客入侵防制系統」，運用系統程式，嘗試協助政府機關、社會大眾，對機關網站、電腦與電子郵件進行初步檢測，並提供檢測報告，期能瞭解機關網站是否遭植入惡意程式或連結？個人電腦是否遭入侵而產生非正常網路連線行為？接獲之電子郵件是否隱含惡意程式等網路不法活動？俾進行清除，確保電腦與網路之使用安全。

貳、目前電腦與網路可能遭受之威脅

一、網頁遭植入惡意程式或連結（即網頁掛馬）：

網站網頁為目前一般民眾獲得機關資訊、交換意見的重要管道，隨著網路使用日益普及，各機關紛紛設置網站，並且隨時更新，方便民眾取得最新訊息。

網路駭客則利用系統漏洞、隱碼攻擊、社交工程等手法，設法滲入機關網站植入惡意程式，或在網頁中埋下惡意連結，伺機對瀏覽網頁者植入惡意程式，達到控制個人電腦之目的。此一攻擊方式，雖不影響機關資訊安全，但對瀏覽網頁之民眾，可能被植入惡意程式，將影響政府機關信譽。下圖即為某機關網頁（如圖 1）於數年前遭掛馬，經調查局赴現場鑑識後，掌握其運作流程（如圖 2）。



圖 1

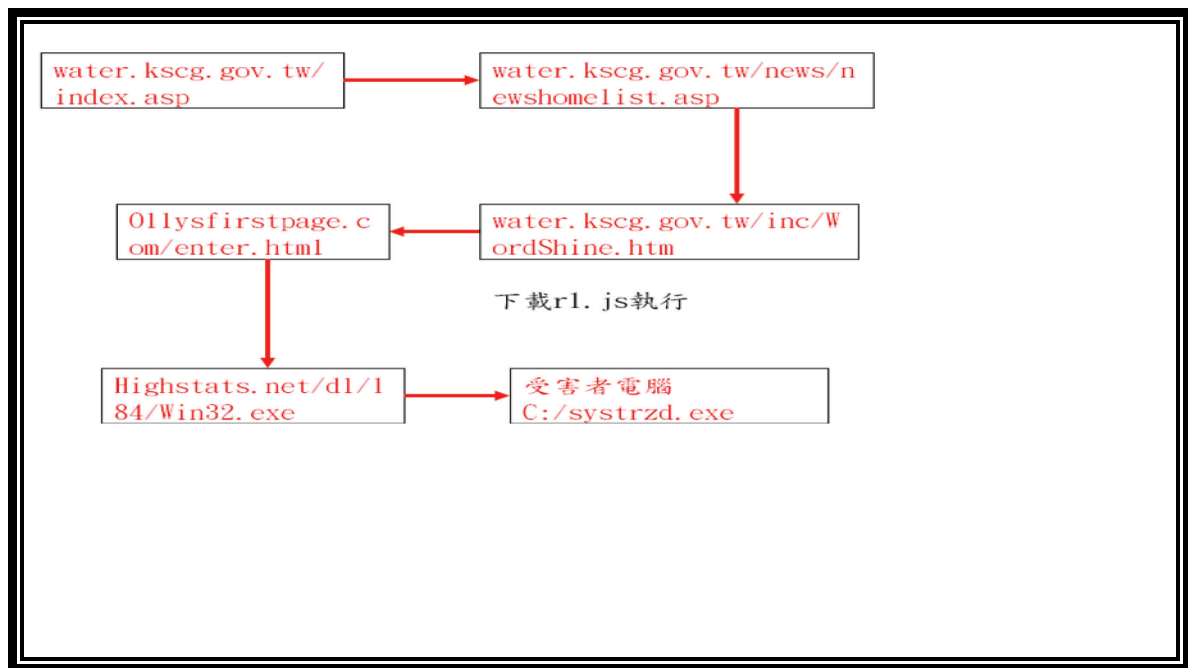


圖 2

二、個人電腦遭入侵產生非正常網路連線行為：

早期電腦感染之病毒，主要企圖是破壞電腦中資料；目前遭植入之惡意程式，目的在於控制電腦，作為攻擊其他網路之跳板，或用於竊取電腦之帳號、密碼及資料，此控制與竊密行為，均藉由網路連線行為達成；惟使用者甚少注意電腦在未啟動網路瀏覽功能時，是否於背景受到控制而自動連上網路傳送資料，而且這些網路連線行為一般防毒軟體無法偵測，因此不會發出警告訊號。

三、APT 電子郵件攻擊

目前讓資訊部門、資安公司大感頭痛之攻擊手法是 APT 攻擊；依據趨勢科技技術通報指出：APT(Advanced Persistent Threat)攻擊，一般稱為進階持續性威脅，是針對特定組織進行複雜且多方位的攻擊。

(一)APT 不似以往的一般惡意程式攻擊：缺乏嚴格掌控；不限定目標地亂槍打鳥。

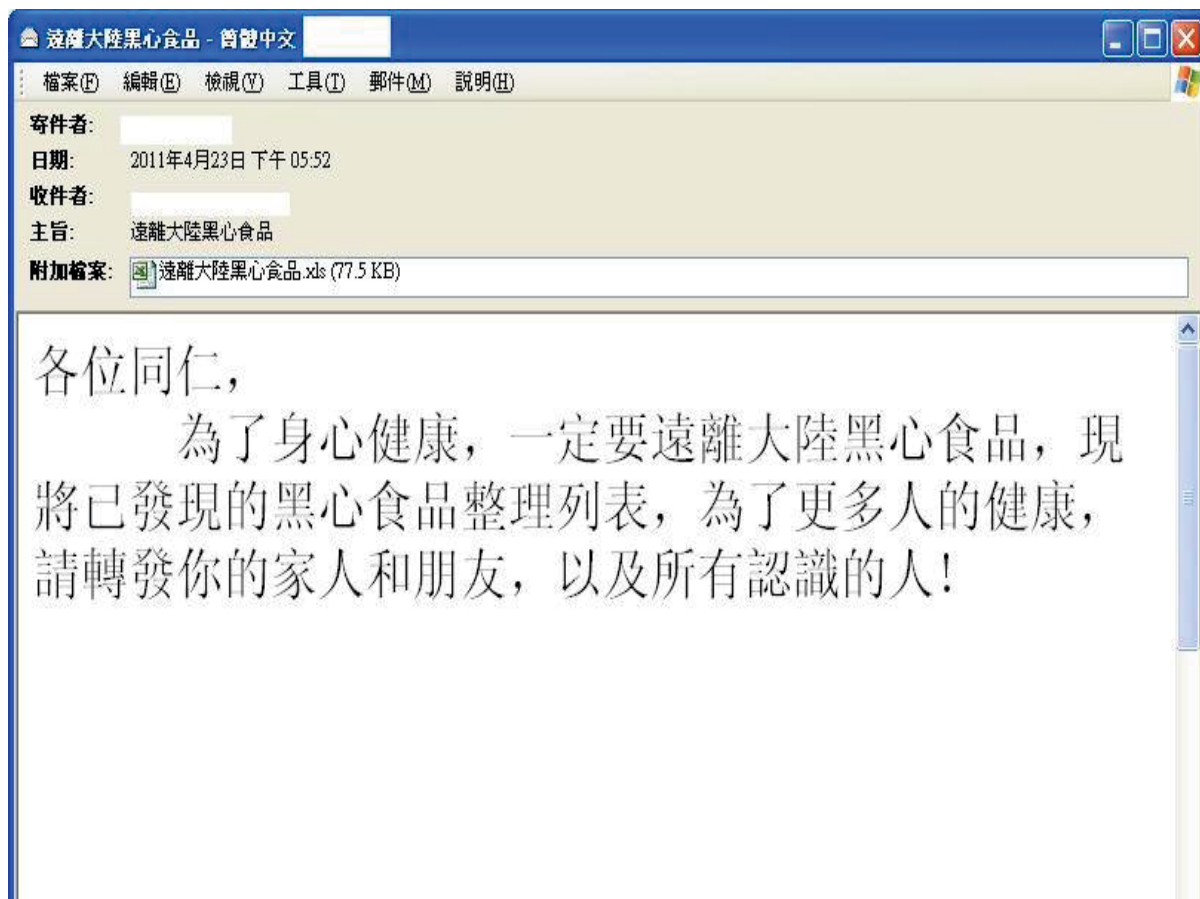
(二)APT 會以較長時間規劃、執行：偵查、蒐集資料；尋找目標的安全漏洞或弱點（2012/04/30 趨勢技術通報）。

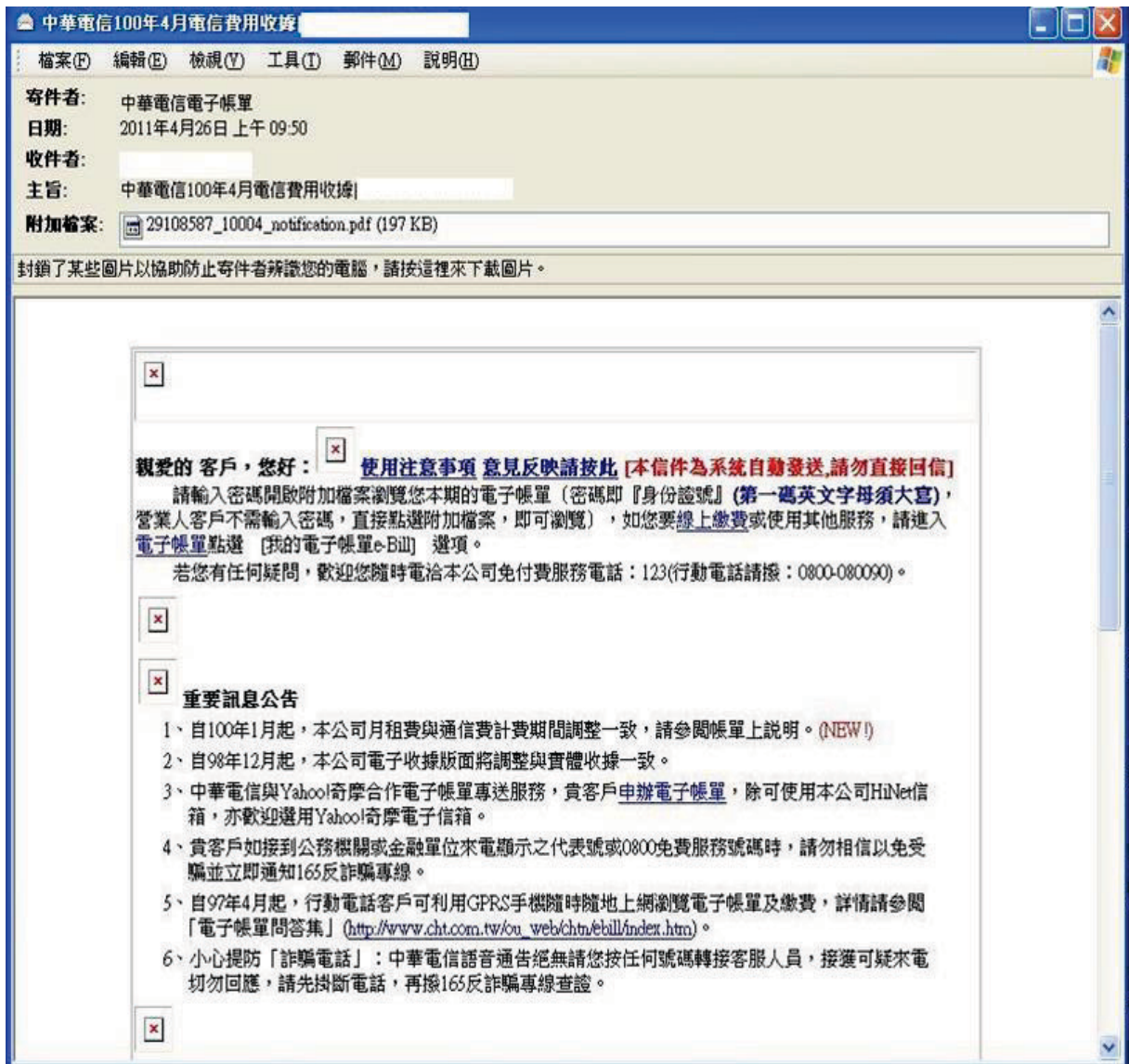
(三)APT 攻擊特色：

1. **【鎖定特定目標】**：針對特定政府或企業，長期間進行計畫性、組織性地竊取情資行為，可能持續數天，數週，數個月，甚至更長的時間。
2. **【假冒信件】**：針對被鎖定對象寄送幾可亂真的社交工程惡意郵件，例如冒充長官來信，取得在電腦植入惡意程式的第一個機會。
3. **【低調且緩慢】**：為進行長期潛伏，惡意程式入侵後，具有自我隱藏能力，避免被偵測，伺機竊取管理者帳號及密碼。
4. **【客製化惡意元件】**：攻擊者除使用現成的惡意程式外，亦使用客製化的惡意元件。
5. **【安裝遠端控制工具】**：攻擊者建立類似殭屍網路/傀儡網路 Botnet 遠端控制架構，定期傳送有潛在價值的文件副本給「命令和控制伺服器」(C&C Server)審查。

6. **【傳送情資】**：將過濾後的敏感機密資料，以加密方式外傳。(2011/07/13 趨勢技術通報)

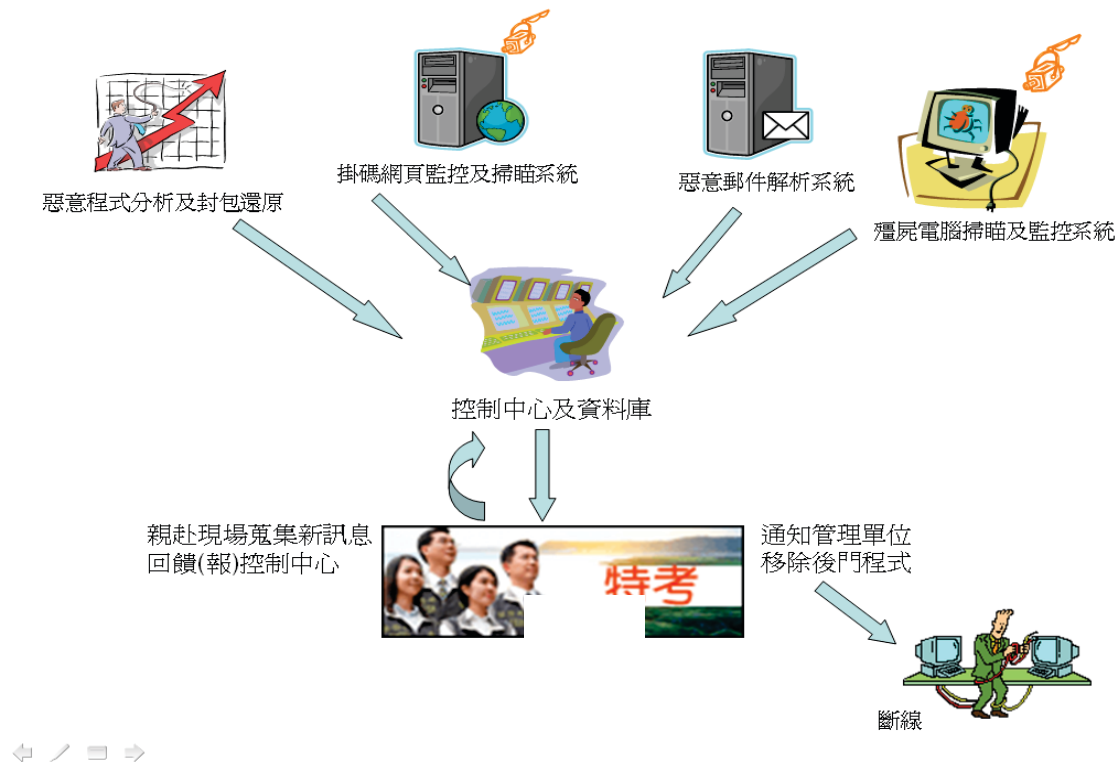
由於 APT 主要活動係藉目標郵件進行滲透式攻擊，成功率相當高，亦成為駭客入侵途徑之首選。以下二封看似普通之郵件，卻是 APT 郵件的樣本(2011/08/30 趨勢技術通報)。





參、防範對策

針對前述幾種電腦與網路威脅，調查局結合產、官、學、研各方面的能量，共同研究發展「駭客入侵防制系統」，示意圖如下：



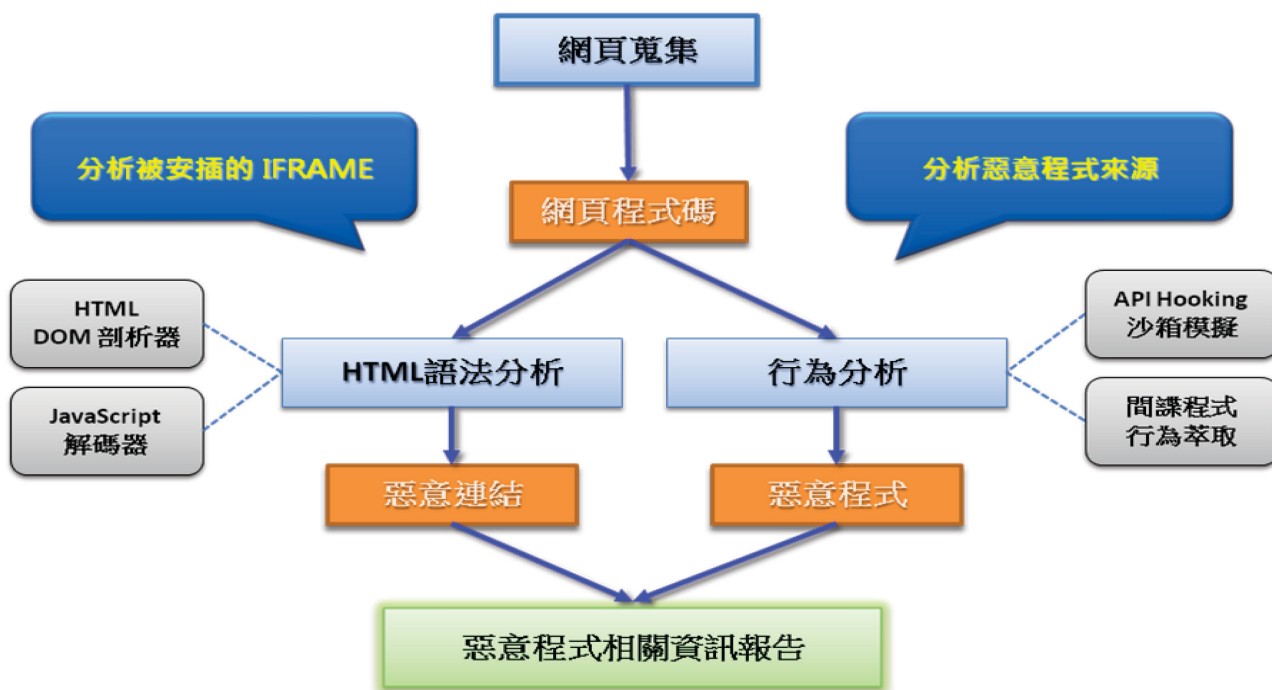
圖中之三套子系統可協助檢測網路惡意行為，茲分別說明如下：

一、網頁惡意程式掃描系統：

(一)系統功能：

- 以非入侵方式開啓網際網路之網頁（www），以維持網站網頁正常運作。
- 檢測網站網頁是否遭植入惡意連結，並記錄其連結位置。
- 檢測瀏覽網頁，若發現下載惡意程式，蒐集該惡意程式，以瞭解其行為模式。

(二)系統架構：

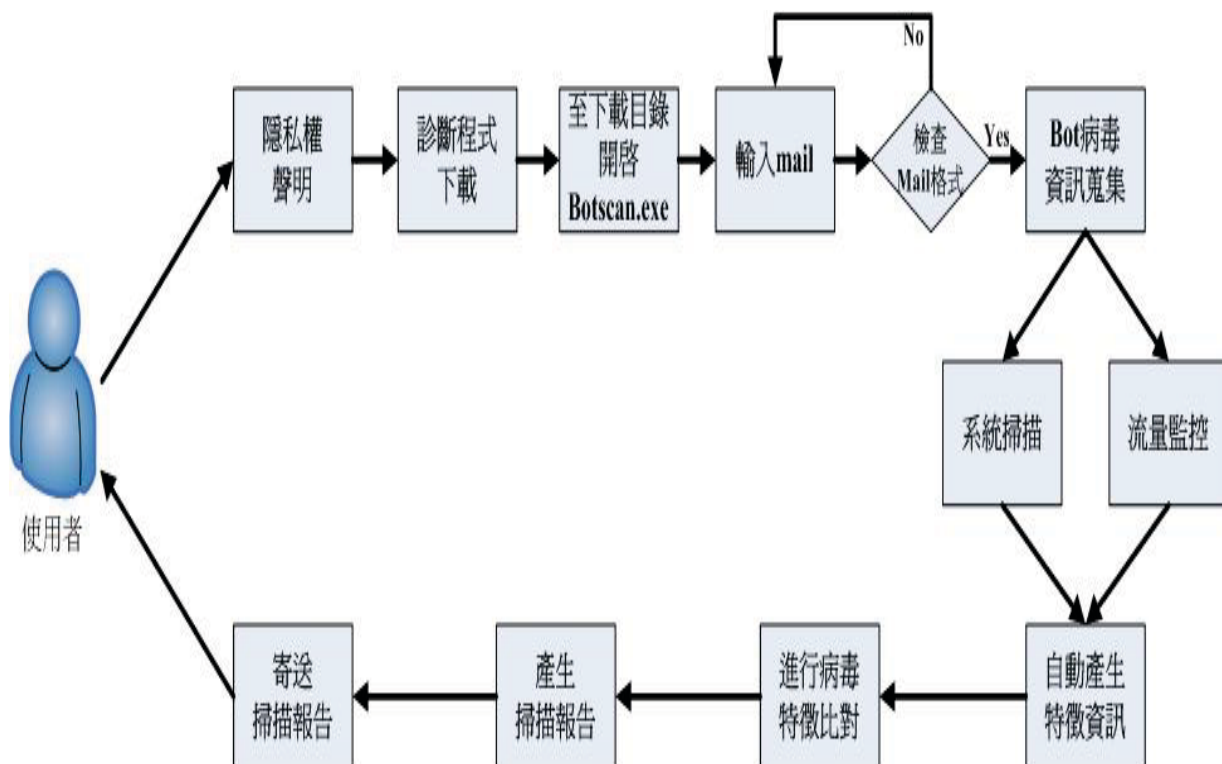


二、Botnet 搜捕、分析及診斷比對系統：

(一)系統功能：

- 蒐集殭屍電腦及惡意程式樣本，分析其行為模式，擷取惡意程式特徵，建置行為、態樣資料庫。
- 比對受測者個人電腦註冊機碼（Registry）及前項行為、態樣資料庫中惡意程式特徵，研判其電腦是否隱藏惡意程式。
- 運用防毒軟體、沙盒子及分析軟體技術，針對各式惡意程式，使用本診斷比對系統進行殭屍病毒研析與檢測，以發掘受測者個人電腦是否遭植入惡意程式，有無違常對外連線之 IP 位址及開放埠。
- 使用者可自行連接至本系統網站，下載檢測程式，進行診斷。

(二)系統架構：



(三)系統網址：

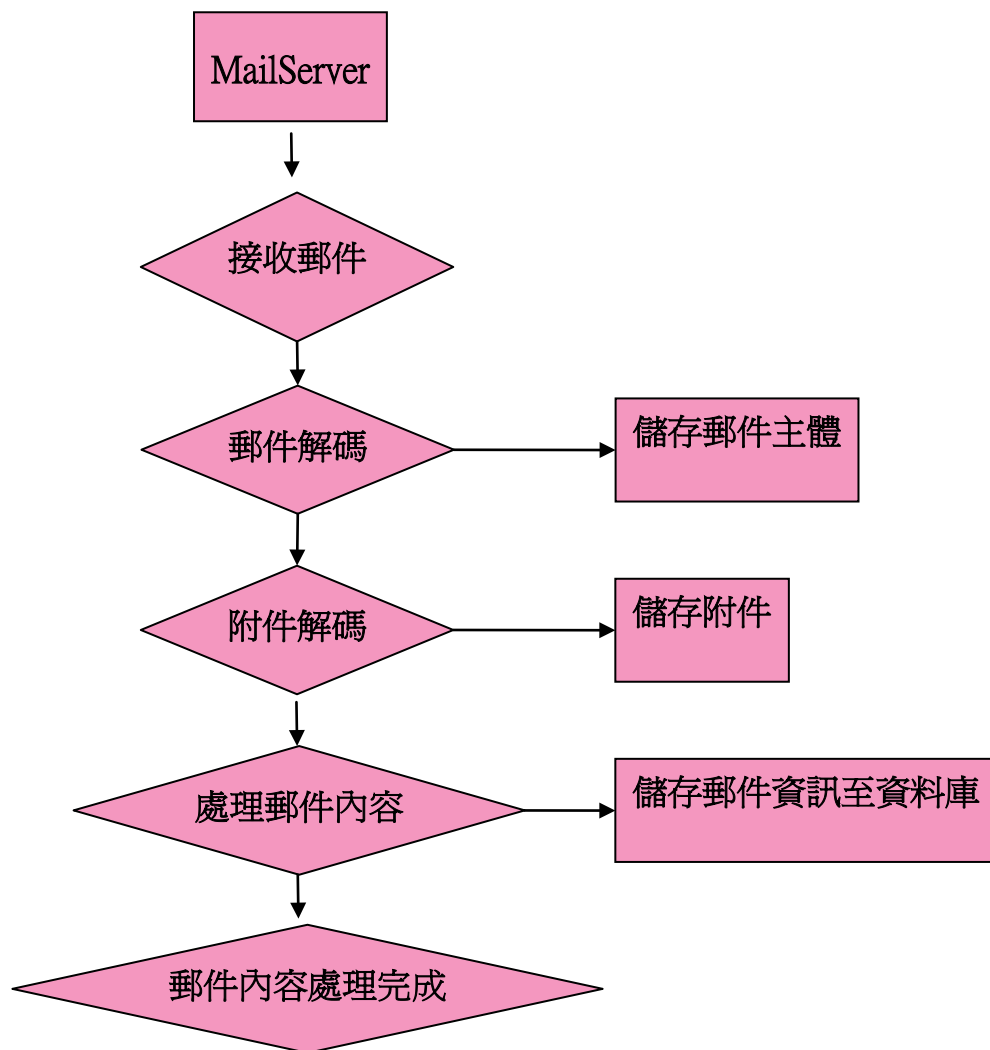
網址：<https://antibot.mjib.tw>

三、惡意郵件檢測系統：

(一)系統功能：

- 使用者將疑似含有惡意程式的郵件，藉由電子郵件轉寄方式，將該郵件轉寄到本系統設定之專屬信箱。
- 本系統專屬信箱收到檢測信件後，首先將郵件檔頭及內文儲存。
- 透過虛擬機器作業，開啓郵件附檔，記錄其是否發生感染，並解析其行爲。
- 將檢測、分析結果，以報表方式自動寄送給使用者。

(二)系統架構：



(三)轉寄電子郵件信箱：bot1@ms.mjib.tw

肆、結語

對於層出不窮的網路資安事件，以有限人力實在難以應付；就有形損失而言，據國外學術機構研究，全世界不法之徒由網路犯罪得到的利益超過販毒所得，無形的損失更是千百倍於有形。運用系統化檢測，初步過濾可疑的網路活動，據以深入調查，方能產生防制效果。

各機關網頁如需本系統協助檢測，請以電子郵件連繫：pdoc1403@mjib.gov.tw。

(本文由法務調查局資通安全處 提供)