Distributed Malware Monitor Systems

孫心蘭　曾典祥　林旻億　蔡志賢

國立中正大學電機所網路組

m9492@cn.ee.ccu.edu.tw

摘要

由於網際網路迅速發展，我們會經由網路發送 e-mail、檔案等資料，在這傳送的過程當中，可能不經意就被植入木馬程式，由於木馬程式猖獗，但是個人用戶及企業或團體用戶常常疏於防範，導致遭植入木馬程式而不自知，因而可能會成為有心人士利用或是公司機密常遭有心人士竊取，而造成不可挽回的損失。在本文中，我們最主要是要解決一般使用者常疏於防護自己的電腦，所以會有一些資安漏洞，因此，我們提出了 DMMS(Distributed Malware Monitor Systems)架構，也就是說，我們可以經由透過監看 Client(一般使用者)所執行中的程式，來達到偵測惡意程式的目的。當 Server 端透過 Heritrix 建立一個惡意程式的資料庫，判斷 Client 端執行中的程式是否為惡意程式，或是企業內部禁止使用的程式，例如 MSN。當 Server 端偵測出惡意程式時會進行移除，並通知 Client 端與管理者，管理者也可經 Web 管理達到最好的防護。

關鍵詞:木馬程式、惡意程式、 DMMS、Web

1. 前言

在傳統的觀念裡，電腦中毒是因電腦病毒藉由某種方式入侵電腦，再伺機感染這部電腦的其他檔案，經一段潛伏期後，會在特定的日子進行破壞，隨著網際網路的發展，開啟另一種新的病毒行為模式，有許多的惡意程式，都夾帶在電子郵件，一般使用者認為只要不開啟夾帶檔案或是不執行就不會感染，殊不知，當閱讀電子郵件的同時，可能正由你的 E-mail 也在散佈病毒給你通訊錄上的聯絡人，在不知覺的情形下，你已經變成散佈病毒的溫床，卻不自知。

藉由電子郵件的轉發及檔案傳送等等的惡意程式，常因使用者不自覺入侵到我們的電腦，以致於個人用戶或是企業團體有時候被植入惡意程式，像是木馬程式、梅沙利病毒之類的惡意程式，常會隱藏在夾帶檔案中，常常使用者被植入木馬程式導致重要的資料被竊取而不自知，而梅沙利病毒是首隻會透過 Outlook 大量並以等比級數的速度散播的巨集病毒，短短一週內毒性席捲全球，許多知名大企業的郵件伺服器(E-MAIL Server)也都因梅沙利病毒所引起的郵件風暴，導致伺服器不堪負荷而紛紛當機，造成無法想像的損失，由此可見，惡意程式總是潛伏在網路環境中，伺機而動。

除了木馬程式，駭客還可經 remote control(VNC)、Spyware 等方式入侵電腦，當使用者執行 VNC 遠端控制電腦，駭客可能同時也正在監看使用者的電腦，利用使用者的電腦發佈攻擊，亦或是竊取重要資料。

監控系統分成 Client 端、Server 端及 Client 端和 Server 端兩者結合等類型，這三種不同的類型，分別可以應用在個人電腦防護、中央控管、檔案伺服器防毒等等應用上面。

在本文，設計一套監控系統是即時監看電腦現在所執行的程式，當一發現有惡意程式入侵，Server 端會立刻拒絕此項服務，並移除此惡意程式。且及時通知管理者及用戶端，以達到及時預警的功能，而假如在公司內部有禁止使用的程式，像是MSN，當管理者看到 Client 端抓到 MSN 執行檔時，會自動移除此程式，並通知 Client 端此為禁止使用的程式，

本系統最主要是在 Windows XP 上運作，此套系統以 Windows XP 作平台，建立一套可以即時監

控的防護機制，再搭配一套完整的惡意程式資料庫，發現 MD5 驗證碼不同時，會主動通知使用者及管理者，並把該程式移除，管理者可以利用本系統達到最即時的處理。

這套系統設計是當電腦只要一執行新的程式或是只要有新的執行緒產生，Client 端便會主動抓取.exe 檔、路徑，接著 Client 端會把.exe 檔利用 MD5 產生一組 MD5 的驗證碼，且 Client 端會把.exe 檔、路徑、MD5 驗證碼收集好傳送到 Server 端的資料庫做比對，判斷它是否為惡意程式，如果是惡意程式，會主動的回傳通知 Client 端及管理者，且會把此惡意程式 deny，進行移除，以提高使用者的安全性，避免成為散佈病毒的溫床。

2. 系統運作原理

此機制的基本運作原理為當 Client 端抓到.exe 檔、路徑後，把.exe 檔轉成 MD5 驗證碼，送到 Server 端的資料庫去做比對，一旦發現 Client 端的 MD5 驗證碼跟 Server 端資料庫的驗證碼不同時，此程式很有可能是惡意程式，Server 端會拒絕該程式的存取，假如該程式例外情形，像是資料庫裡沒有更新到，則會由防毒軟體進行偵測，掃出來為惡意程式則把它 delete 掉，並存成 log 檔，以供管理者查看，系統同時會通知 Client 端及管理者，告知系統最新狀況，以徹底達到及時的防護功能，對系統維護達到最好的效果。

2.1 系統架構

本機制的運作包含了下列幾個部份，分別為 Client 端跟 Server 端、資料庫、Gateway、管理者，由 Client 端負責抓取相關資料，傳送給 Server 端，經資料庫比對分析，判別是否為惡意程式，資料庫則設定每天定時自動上網更新一次，管理者可經由網路登錄，隨時查看最新訊息，也可經此管理系統，對判別惡意程式的 rule 作設定，整個系統架構圖如下；

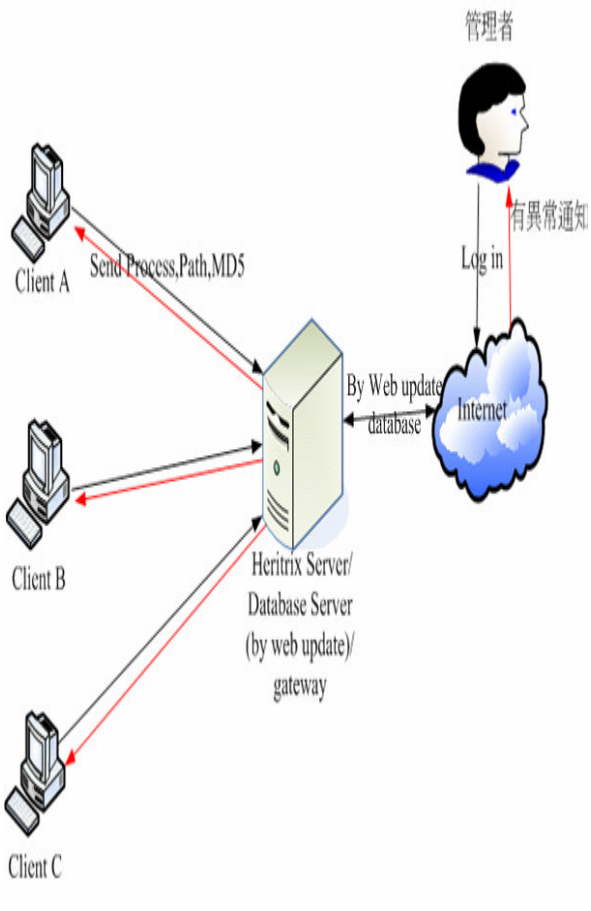

圖 1 系統架構

在圖 1. 中可以清楚看到整個系統的架構，只要安裝了這個系統，當使用者一開機或是開啟新的程式，Client 端便會去抓取所有.exe 檔及它所在的路徑，經由 MD5 的運算，求得.exe 檔的 MD5 驗證碼，在送到 Server 端的資料庫去做比對，而 Server 端的資料庫是經由 Heritrix 抓取的惡意程式資料庫，經判斷可得知 Client 端是否為惡意程式，如為例外情況，像資料庫沒有把該程式列為比對資料，則會由防毒軟體對該程式進行掃描，當有發現異常狀況會立刻進行通知並移除該程式，而資料庫定時會自動上網更新且下載相關 process 及病毒相關資料，利用防毒軟體掃描相關的資料，以設定相關的 rule 並且更新資料庫，管理者經通知可由 Web Browser 登入控制介面並進行監看以及更改相關 rule，已達到即時性的管理。

整個系統最主要分成 Server 端及 Client 端，兩者主要功能分述如下：

2.2 Server 端設計

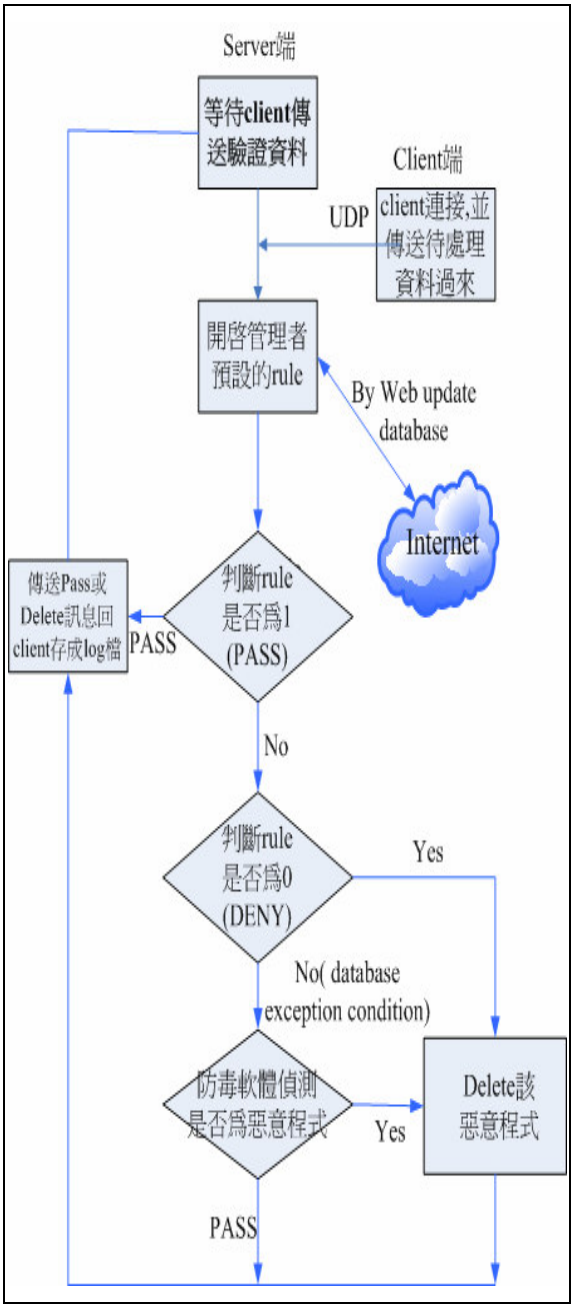

圖 2 Server端

現在先來探討Server端，在圖2. 一開始當Server端收集到Client端所傳過來的process name、 path和MD5驗證碼、Server端會把所收集到的資訊送到資料庫裡作分析，根據我們所訂的正面表列和負面表列，判別何者為惡意程式，何者是我們所要杜絕不准通過的程式，當資料庫沒有相關程式資訊表列，則用防毒軟體進行掃描，如果為惡意程式，則直接刪除該程式，並回傳delete的訊息回傳給Client端，如果為正常程式，則繼續執行，並把分析結果以網頁的方式存成log檔，以供管理者參考，像是有些業界禁止使用MSN等等，都可以利用它來把它杜絕掉，讓用戶端還是能上網但卻不能使用MSN。

資料庫是利用Heritrix建立，經由上網抓取惡意程式的資料把它建立成資料庫，透過網頁的方式，可以設定成定時上網抓取更新資料庫一次，以提高資料庫的更新頻率，達到更好的防護措施。

在這個系統裡，Server端會把它所收集到的資訊和資料庫裡的資料去做比對，當比對出來的驗證碼結果和資料庫裡的不同時，系統會認定它為惡意程式，並會去通知使用者和管理者，且會把所分析到的資料以網頁的方式把它呈現出來，管理者隨時可以經由網頁查看，了解整個系統的狀態，進行最佳的控管，如果是公司禁止使用的程式，如MSN，管理者可以經由修改資料庫，拒絕MSN執行檔的存取，讓使用者還是可以上網，但是不能使用MSN，在程式的設計上，Server端具有分析比對的功能，它會根據所規定的rule去比較，根據制定的資料庫，管理者根據實際需要可達到所要的功能。

2.3 Client 端的設計

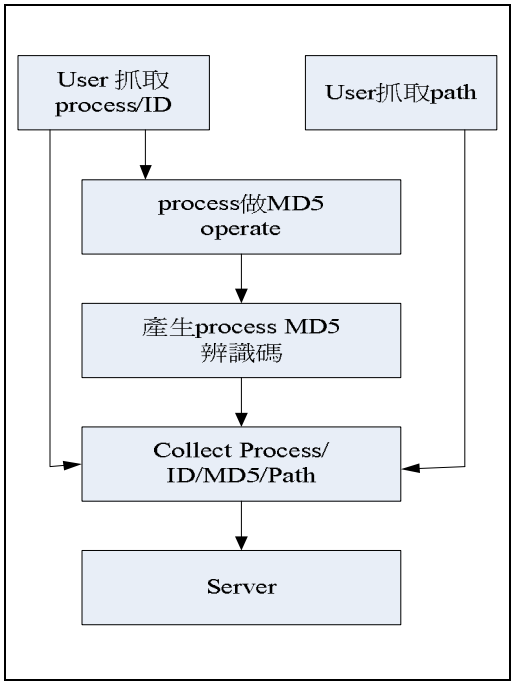

圖 3 Client 端

Client 端的設計最主要就是當有新程式或是開新檔案的時候，會去主動抓取這些 Process name，還有它所在的路徑，並且會把 Process name 轉成 MD5 驗證碼，當收集到 Process name、Path、還有 MD5 驗證碼後，會把所收集到的資料傳送到 Server 端去做比較， Client 端最主要就是在抓.exe 檔，把它做 MD5 的運算，其實，並不一定要用 MD5 的運算方式，有很多可以取得驗證碼的方式，只是在這裡我們採用 MD5 的方法是因為它只需要 128 bits，而且它的運算方式也比較簡單，但是要如何把正在執行中的 process 轉成 MD5 的值?因正在執行中的 process 不能直接轉，所以，必須要先把 process 做 copy，必須要先把 process 做副本，再把 copy 的 process 轉成 byte[ ]data 後，傳給 MD5，這樣就可以求出 hash value，如此一來，就可以把抓到的 process、PID 及 path 收集好後傳給 Server 端去做比對。

假如 Client 端它並沒有一直開檔案，那是不是這個系統就不會運作而導致會有漏洞呢?其實不會，因為在這個系統中，是設定每三秒它會重新抓取一次，也就是說每三秒它會自動抓取這些 Processs，然後再去做運算，送到 Server 端做比對，避免會有漏網之魚，所以，它會一直不停的回送資料給 Server 端去做比對，已達到最好的防護效果。

3. 系統實做範例

本系統實作，是以 TSPY_SUFIAGE.G 為惡意程式，Client 端一開啟檔案，系統主動抓取 process 進行 MD5 驗證碼運算，當偵測 TSPY_SUFIAGE.G 時，系統資料庫比對出此為惡意程式，及時通知管理者及 Client 端，管理者會使用防毒軟體進行掃毒，確定該為惡意程式後會拒絕並移除該程式，管理者可經由網頁可查看相關 log 檔資訊及擁有修改權限。

3.1 杜絕惡意程式

在資料庫設 TSPY_SUFIAGE.G 為惡意程式，當一開機或執行此程式，用戶端會把抓到的.exe 檔跟路徑及 MD5 驗證碼送到 Server 端的資料庫做比對，Server 端的資料庫經過比對，發現 MD5 的驗證碼不同，判斷此為惡意程式，並經由管理者使用防毒軟體進行掃毒，確定該為惡意程式，會即時移除該程式，該程式發作的行為會竄改執行檔，更改檔名為 svchost.exe，讓使用者不察，再進行攻擊行為，在圖 6.可以清楚的看到一開始的情形，當這些程式都是正常的情況所產生的畫面。

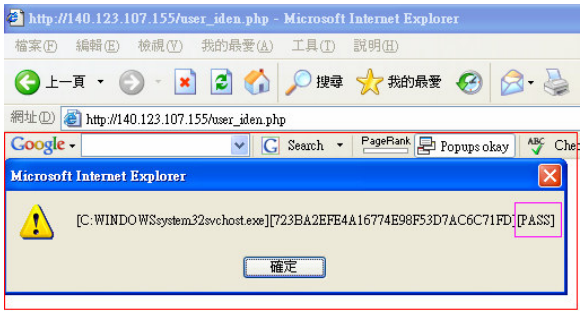

圖 6 PASS 情形

圖 6 可以看到 Server 端的訊息它會顯示出 Process 的路徑跟此 Process 的 MD5 驗證碼，及判斷結果，可以看到顯示結果如圖 6.視窗顯示 PASS 的訊息，代表經 Server 端比對結果為正面表列。

假設 Server 端的資料庫把 TSPY_SUFIAGE.G 比對為惡意程式，由圖 7 看出，它會直接跳出視窗畫面說此為惡意程式，此時系統會找出惡意程式列表，並顯示目前可以移除的程式，直接把它 delete 掉並進行移除，但是它仍會顯示出此程式所在的路徑及檔案名稱，以便管理者查看。

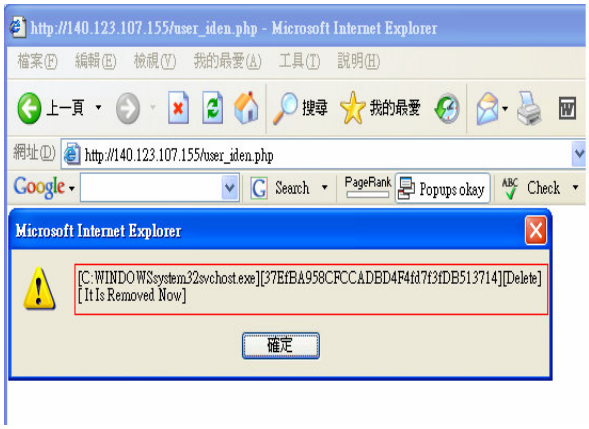

圖 7 Delete 情形

3.2 資料庫和 log 檔相關資料

本系統主要是以 Heritrix 網頁做管理，在主網頁除了可以看執行結果，管理者可查看有關它所偵測到的畫面，像是 log 檔，Database Rule 相關資訊，由圖 8 看出，相關的管理畫面。

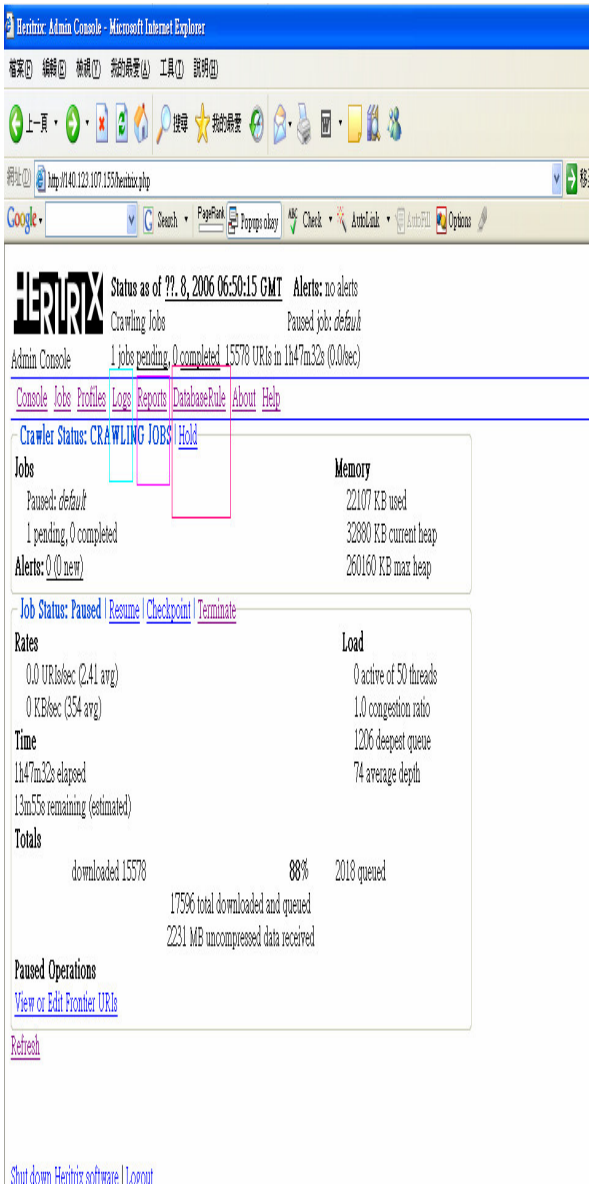

圖 8 Heritrix 主網頁

圖 9 是有關 Heritrix 比對結果，系統會秀出所有經過比對的 Process 及它所在的路徑和 MD5 驗證碼跟比對結果，可以看出何者 PASS，何者 Delete，相關資訊可以從圖 9 看出。

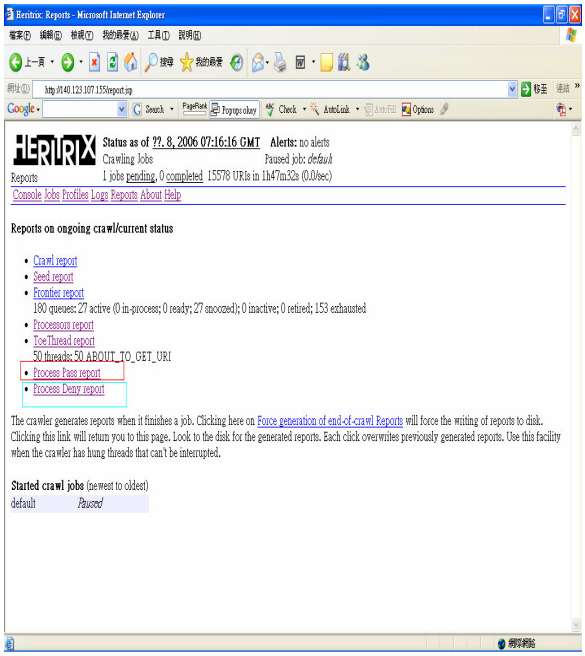

圖 9 Heritrix report

圖 10 可以看到經比對後的 log 檔，在下圖，看到 Process 及 MD5 和狀態，管理者經這個畫面，對相關的 log 檔，經由此網頁查看所有 Process 的資訊，可得知比對結果，問題程式的所在路徑等，以便及時進行處理。

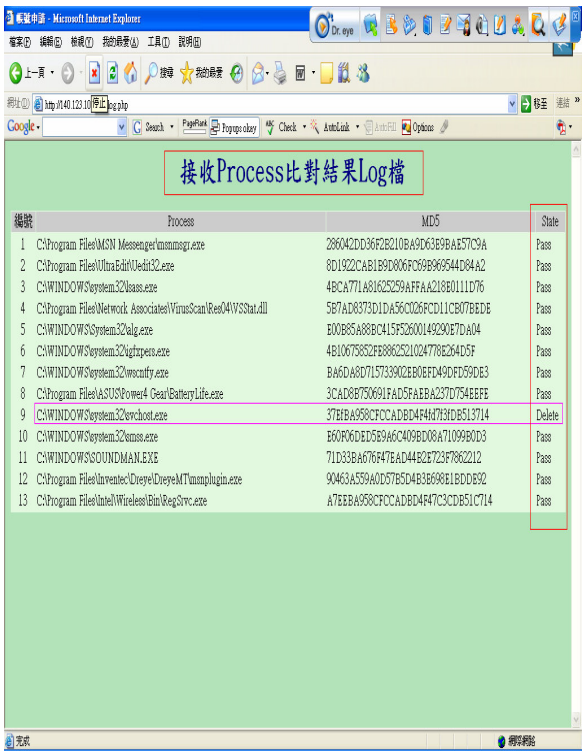

圖 10 惡意程式相關資料

圖 11. 可以看到有關於惡意程式的一些 rule，當我們設為 0 則代表此為惡意程式，那 Server 端就會把它 Delete 掉，那如果為 1 的話，則會讓它通過，代表此為正常的程式，管理者藉由此畫面可以自行設定正面表列和負面表列，對惡意程式做適度的防範，也可藉此對內部的網路系統做更好的控管。

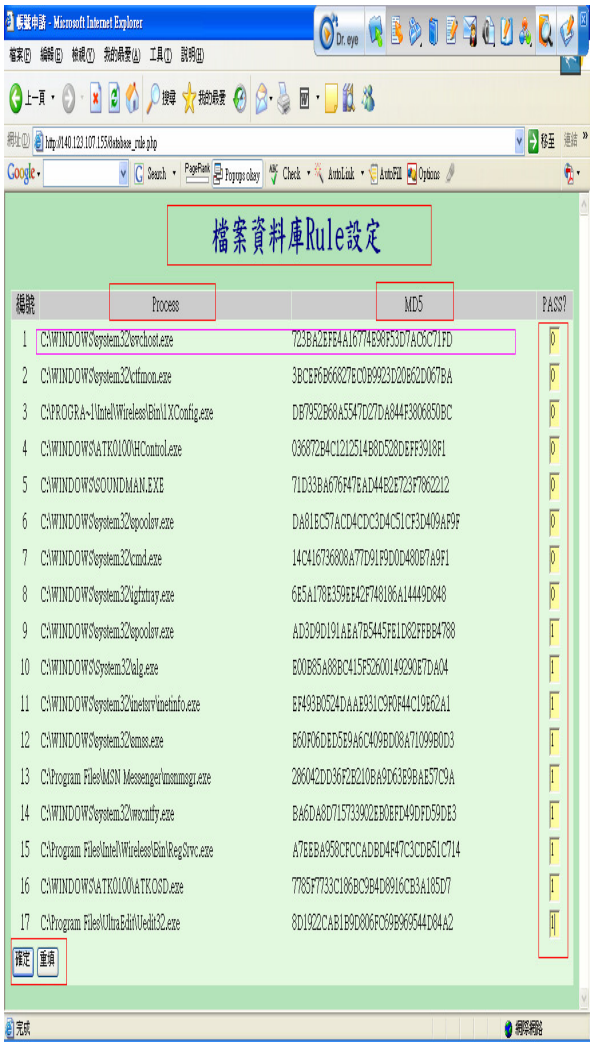

圖 11 設定的 rule 表

4. 結論

這個系統只是一個初步的系統，藉由它來達到一個即時的防護機制，使用者只要一開機，可以立刻抓取 Process 並且去作一個驗證的動作，最大的優點在於，只要一發現惡意程式就會通知使者者及管理者，進行防護措施，是一個即時性的系統，管理者可以藉由網頁進行監控，對惡意程式執行必要的措施，提高系統的安全性，避免病毒交叉感染，或是遭竊取重要資料而不自知，造成不可挽回的損失。

現在很多資料都是藉由網路傳輸，許多病毒伺機而動，例如夾帶在執行檔或是夾帶檔案，只要使用者疏忽就會遭受攻擊，藉由本系統，在第一時間與資料庫進行比對，且資料庫也會透過網路做更新動作，假如發現惡意程式，會拒絕該惡意程式，並通知管理者進行即時性的處理，管理者經防毒程式掃瞄，確認該程式為惡意程式，會把該程式移除，且把該惡意程式的路徑通知使用者，降低感染的風險，並把比對完的結果存成 log 檔放在網頁上，供管理者參考。

本系統，最大的挑戰是現在的木馬程式及病毒變種的太快，惡意程式變種的速度讓人措手不及，在我們的資料庫裡，必須要做到即時性的更新，這一點是要再加強，這套系統最主要是可以幫助企業和個人對整個網路系統有很好的控管，因為我們可以掌握到及時的資訊，監控看是否有被惡意程式入侵，也可以避免一些漏洞，讓有心人士有機可乘，以提高整體的安全性。

5. 參考文獻

[1]朱家聰、黃明達，2001 年12 月，駭客入侵方法與對策之研究，淡江大學資訊管理學系研究所碩士論文

[2]賴守全、謝木政 “校園網路安全事故自動防制之設計與實作”， TANET 2002。

[3]陳培德、賴溪松，2002 年3 月，入侵偵測系統簡介與實現，資訊安全通訊，卷8 期2，頁8-20。

[4]梁宏一、田筱榮、黃世昆，2000 年7 月，一個給入侵偵測系統用的特徵選取導引，中原大學資訊工程學系研究所碩士論文。

[5] Computer Economics(2001)，” 電腦病毒攻擊事件在今年造成的損失已達107 億美元，路透社舊金山電”，
http://tw.news.yahoo.com/2001/09/01/technology/reuters/2341821.html , 9 月。