I435236

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I435236 B**

(45)公告日： 中華民國 103 (2014) 年 04 月 21 日

(21)申請案號：099143955 (22)申請日： 中華民國 99 (2010) 年 12 月 15 日

(51)Int. Cl.： *G06F21/00 (2013.01)*

(71)申請人：財團法人資訊工業策進會 (中華民國) INSTITUTE FOR INFORMATION INDUSTRY (TW)

臺北市大安區和平東路 2 段 106 號 11 樓

(72)發明人：戴士堯 DAI, SHIH YAO (TW) ；鄒耀東 TSOU, YAO TUNG (TW) ；李庭宇 LEE, TING YU (TW) ；顏新晨 YEN, CASTLE (TW) ；郭斯彥 KUO, SY YEN (TW) ；吳建興 WU, JAIN SHING (TW)

(74)代理人：陳翠華

(56)參考文獻：

TW 200919251A TW 201035795A

US 2007/0240217A1

審查人員：林信宏

申請專利範圍項數：18 項 圖式數：6 共 0 頁

(54)名稱

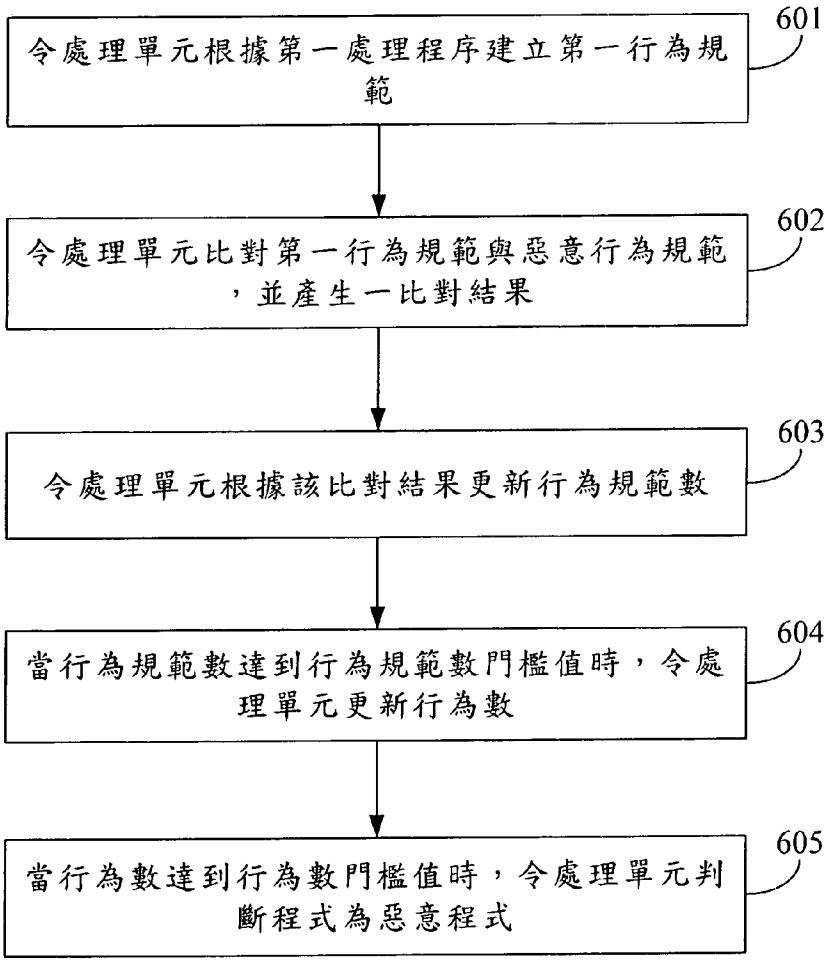
惡意程式偵測裝置、惡意程式偵測方法及其電腦程式產品

MALWARE DETECTION APPARATUS, MALWARE DETECTION METHOD AND COMPUTER PROGRAM PRODUCT THEREOF

(57)摘要

一種惡意程式偵測裝置、惡意程式偵測方法及其電腦程式產品。該惡意程式偵測裝置用以偵測一程式，該程式執行一第一處理程序。該惡意程式偵測裝置包含一儲存單元以及一處理單元，該儲存單元用以儲存一惡意程式之一惡意行為規範；該處理單元用以根據該第一處理程序建立一第一行為規範；比對該第一行為規範與該惡意行為規範，並產生一比對結果；根據該比對結果更新一行為記錄表；以及根據該行為記錄表判斷該程式為該惡意程式。

A malware detection apparatus, a malware detection method, and a computer program product thereof are provided. The malware detection apparatus is used to detect a program. The program executes a first process. The malware detection apparatus comprises a storage unit and a processing unit. The storage unit is configured to store a malicious behavior profile of a malware. The processing unit is configured to generate a first behavior profile according to the first process, compare the first behavior profile with the malicious behavior profile and generate a comparison result. The processing unit updates a behavior record table according to the comparison result, and determines that the program is the malware according to the behavior record table.


令處理單元根據第一處理程序建立第一行為規範
601
令處理單元比對第一行為規範與惡意行為規範，並產生一比對結果
602
令處理單元根據該比對結果更新行為規範數
603
當行為規範數達到行為規範數門檻值時，令處理單元更新行為數
604
當行為數達到行為數門檻值時，令處理單元判斷程式為惡意程式
605

第 6 圖

I435236

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：99143955

※申請日：99. 12. 14　※IPC分類：G06F21/00 (2013.01)

一、發明名稱：（中文/英文）

惡意程式偵測裝置、惡意程式偵測方法及其電腦程式產品/MALWARE DETECTION APPARATUS, MALWARE DETECTION METHOD AND COMPUTER PROGRAM PRODUCT THEREOF

二、中文發明摘要：

一種惡意程式偵測裝置、惡意程式偵測方法及其電腦程式產品。該惡意程式偵測裝置用以偵測一程式，該程式執行一第一處理程序。該惡意程式偵測裝置包含一儲存單元以及一處理單元，該儲存單元用以儲存一惡意程式之一惡意行為規範；該處理單元用以根據該第一處理程序建立一第一行為規範；比對該第一行為規範與該惡意行為規範，並產生一比對結果；根據該比對結果更新一行為記錄表；以及根據該行為記錄表判斷該程式為該惡意程式。

三、英文發明摘要：

A malware detection apparatus, a malware detection method, and a computer program product thereof are provided. The malware detection apparatus is used to detect a program. The program executes a first process. The malware detection apparatus comprises a storage unit and a processing unit. The storage unit is configured to store a malicious behavior profile of a malware. The

processing unit is configured to generate a first behavior profile according to the first process, compare the first behavior profile with the malicious behavior profile and generate a comparison result. The processing unit updates a behavior record table according to the comparison result, and determines that the program is the malware according to the behavior record table.

四、指定代表圖：

(一)本案指定代表圖為：第（ 6 ）圖。

(二)本代表圖之元件符號簡單說明：

無

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【發明所屬之技術領域】

本發明係關於一種惡意程式偵測裝置、惡意程式偵測方法及其電腦程式產品。更詳細地說，本發明係關於一種用以偵測一程式之惡意程式偵測裝置、惡意程式偵測方法及其電腦程式產品。

【先前技術】

隨著數位資訊的應用層面日益廣泛，資訊安全防護的意識逐漸受到重視，帶動資訊安全防護技術的發展，目前資訊安全防護之方式中，普遍利用防毒軟體針對病毒程式進行偵測。詳細來說，為了避免資料遭到竊取或破壞，一般電腦中通常搭載具有病毒資料庫之防毒軟體。其中，病毒資料庫係用以記錄目前已知之病毒程式特徵碼（signature）。如此一來，防毒軟體將可利用特徵碼比對之方式，一一針對電腦內之檔案進行偵測。若比對結果發現有與特徵碼相同之檔案，則可確認其為病毒程式。

然而，隨著病毒程式之迅速發展，以及各種加殼變種病毒程式的衍生，防毒軟體之病毒資料庫更新病毒程式特徵碼之速度將不足以應付惡意程式之成長速度。具體而言，習知的防毒軟體係利用特徵碼比對技術進行病毒程式的偵測比對，惟特徵碼比對技術會受限於病毒資料庫的完整性，若病毒資料庫未更新一加殼變種之病毒程式之特徵碼，則防毒軟體即無法偵測出該加殼變種之病毒程式，此外，防毒軟體使用特徵碼比對技術進行病毒程式的偵測亦需要花費較長的時間。如此一來，將會降低病毒程式之偵測率，造成資訊安全防護的漏洞，而為了不斷更新病毒資料庫，亦

必須負擔高昂的成本。

綜上所述，如何加速惡意行為之比對效率以及提高病毒程式之偵測率，實為該領域之技術者亟需解決之課題。

【發明內容】

本發明之一目的在於提供一種惡意程式偵測裝置。該惡意程式偵測裝置用以偵測一程式，該程式執行一第一處理程序，該惡意程式偵測裝置包含一儲存單元以及一處理單元。該儲存單元用以儲存一惡意行為資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範。該處理單元與該儲存單元關聯性連接，並用以根據該第一處理程序建立一第一行為規範；比對該第一行為規範與該惡意行為規範，並產生一比對結果；根據該比對結果更新一行為記錄表；以及根據該行為記錄表判斷該程式為該惡意程式。

本發明之另一目的在於提供一種用於前述惡意程式偵測裝置之惡意程式偵測方法。該惡意程式偵測裝置用以偵測一程式，且包含一儲存單元以及一處理單元，該儲存單元用以儲存一惡意行為資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範，該處理單元與該儲存單元關聯性連接，該程式執行一第一處理程序，該惡意程式偵測方法包含下列步驟：(a)令該處理單元根據該第一處理程序建立一第一行為規範；(b)令該處理單元比對該第一行為規範與該惡意行為規範，並產生一比對結果；(c)令該處理單元根據該比對結果更新一行為記錄表；以及(d)令該處理單元根據該行為記錄表判斷該程式為該惡意程式。

本發明之又一目的在於提供一種電腦程式產品，內儲一種用於

一惡意程式偵測裝置之惡意程式偵測方法之程式指令，該惡意程式偵測裝置用以偵測一程式，且包含一儲存單元以及一處理單元，該儲存單元用以儲存一惡意行為資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範，該處理單元與該儲存單元關聯性連接，該程式執行一第一處理程序，該程式指令包含：一程式指令 A，令該處理單元根據該第一處理程序建立一第一行為規範；一程式指令 B，令該處理單元比對該第一行為規範與該惡意行為規範，並產生一比對結果；一程式指令 C，令該處理單元根據該比對結果更新一行為記錄表；以及一程式指令 D，令該處理單元根據該行為記錄表判斷該程式為該惡意程式。

本發明之惡意程式偵測裝置儲存一惡意行為資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範。當一程式於本發明之惡意程式偵測裝置執行一第一處理程序時，惡意程式偵測裝置係可根據該第一處理程序建立一第一行為規範，比對該第一行為規範與該惡意行為規範，並產生一比對結果；接著，根據該比對結果更新一行為記錄表，並根據該行為記錄表判斷該程式為該惡意程式。藉此，本發明係可克服習知防毒軟體之更新速度無法跟上加殼變種惡意程式之增加速度的缺點，同時具有加速惡意行為之比對效率以及提高病毒程式之偵測率之優點。

在參閱圖式及隨後描述之實施方式後，該技術領域具有通常知識者便可瞭解本發明之其他目的，以及本發明之技術手段及實施態樣。

【實施方式】

以下將透過實施例來解釋本發明之內容，本發明的實施例並非用以限制本發明須在如實施例所述之任何特定的環境、應用或特殊方式方能實施。因此，關於實施例之說明僅為闡釋本發明之目的，而非用以限制本發明。須說明者，以下實施例及圖式中，與本發明非直接相關之元件已省略而未繪示，且圖式中各元件間之尺寸關係僅為求容易瞭解，非用以限制實際比例。

本發明之第一實施例為一惡意程式偵測裝置 1，其示意圖描繪於第 1 圖。惡意程式偵測裝置 1 包含一儲存單元 11、一處理單元 13、以及一輸出單元 15，其中儲存單元 11 以及輸出單元 15 分別與處理單元 13 電性連接。儲存單元 11 可為記憶體、軟碟、硬碟、光碟、隨身碟、磁帶、可由網路存取之資料庫或所屬技術領域中具有通常知識者可輕易思及具有相同功能之儲存媒體；處理單元 13 可為目前或未來的各種處理器、中央處理器、微處理器、計算器或所屬技術領域中具有通常知識者所能輕易思及具有計算能力之裝置。

於本實施例中，惡意程式偵測裝置 1 係為一電腦。於其它實施例中，惡意程式偵測裝置 1 亦可為伺服器、筆記型電腦、個人數位助理（Personal Digital Assistant, PDA）、手機、遊戲機、數位媒體播放機或其它可用以偵測惡意程式之惡意程式偵測裝置。惡意程式偵測裝置 1 之實施態樣並不用以限制本發明之範圍。

一般而言，一惡意程式通常包含一個或複數個惡意行為，各個惡意行為更包含一個或複數個處理程序（process）。而為了有效偵測惡意程式，必須使用特定的規則來描述惡意程式之各個處理程

序，因此，本發明定義了一種用以描述一處理程序之行為規範（behavior profile）。

請參閱第 2 圖，其係描繪本發明之行為規範之示意圖。本發明針對一處理程序所定義之行為規範 2 包含三個部分，分別為執行標的、執行動作以及鏈結資訊，其中執行動作係指該處理程序所進行的一動作，執行標的係指該處理程序進行該動作的一標的，鏈結資訊係指該處理程序對該標的進行該動作所涉及的執行資訊。舉例而言，假設一處理程序為「創造一個隨機名稱的 htm 檔」，意指該處理程序所要進行的是創造一個檔案名稱為隨機名稱，副檔名稱為.htm 的檔案，因此，此處理程序的執行標的為「File」，執行動作為「Creat」，於此實例中鏈結資訊為創造該隨機名稱 htm 檔的路徑「C\DOCUME~\NTU\LOCALS~1\Temp\XXX.htm」。

更具體來說，處理程序通常會透過系統呼叫（system call）的方式來完成所要進行的操作，而系統呼叫則帶有進行處理程序相關必要的資訊，因此，行為規範 2 中的執行標的以及執行動作便可自處理程序所進行的系統呼叫中擷取。行為規範 2 中的鏈結資訊則依據處理程序而有所不同，不同的處理程序因涉及不同的執行資訊，故鏈結資訊可以是任何相關的執行資訊，端視實際應用情況而定，鏈結資訊的形式及內容並不用以限制本發明之範圍。

本發明之惡意程式偵測裝置 1 之儲存單元 11 中儲存一惡意行為資料庫，該惡意行為資料庫記錄了各種惡意程式之各種惡意行為規範，以下將詳述本發明之惡意程式偵測裝置 1 如何建立該惡意行為資料庫。當一惡意程式於惡意程式偵測裝置 1 上執行時，該

惡意程式會進行一個或複數個惡意行為，各個惡意行為則藉由執行一個或複數個處理程序來完成。據此，當一惡意程式於惡意程式偵測裝置 1 上執行一處理程序時，處理單元 13 便依據前述方式擷取該處理程序之執行標的、執行動作以及鏈結資訊以建立該處理程序之一惡意行為規範，同時，處理單元 13 根據該惡意行為規範產生一與該惡意行為規範相對應之一編碼，該編碼用以表示該惡意行為規範，以便後續處理單元 13 可根據該編碼偵測一程式是否為一惡意程式。

以下舉例說明惡意行為資料庫之內容，以及行為規範的編碼方式。一惡意程式 A 具有一惡意行為 A-1 以及一惡意行為 A-2，惡意行為 A-1 為「修改 Internet Explorer 瀏覽器」，且更執行一處理程序 A-1:1「打開 Internet Explorer 中的 KEY」，以及一處理程序 A-1:2「勾選建議密碼欄位」；惡意行為 A-2 為「開啟 Internet Explorer 並嘗試連線」，且更執行一處理程序 A-2:1「創造一個隨機名稱的 htm 檔」，以及一處理程序 A-2:2「寫入隨機名稱的 htm 檔」。處理單元 13 分別擷取處理程序 A-1:1、處理程序 A-1:2、處理程序 A-2:1 以及處理程序 A-2:2 中的執行標的、執行動作以及鏈結資訊，並分別建立其惡意行為規範；接著，處理單元 13 產生一編碼 A-1:1 代表處理程序 A-1:1 之惡意行為規範，產生一編碼 A-1:2 代表處理程序 A-1:2 之惡意行為規範，產生一編碼 A-2:1 代表處理程序 A-2:1 之惡意行為規範，產生一編碼 A-2:2 代表處理程序 A-2:2 之惡意行為規範。

根據上述方式所建立之惡意行為資料庫如第 3 圖所示，其係描

繪惡意行為資料庫之示意圖。惡意行為資料庫 3 中包含惡意程式 A 中各處理程序之惡意行為規範，即各處理程序之即執行標的、執行動作、鏈結資訊，以及與各處理程序相對應之編碼。

如前所述，一惡意程式包含一個或複數個惡意行為，各個惡意行為更包含一個或複數個處理程序，因此，當欲判斷一程式是否為該惡意程式時，則需判斷該程式是否執行該一個或複數個處理程序，接著判斷該程式所執行的處理程序是否累積構成該一個或複數個惡意行為，進而判斷該程式所進行的惡意行為是否累積構成該惡意程式。據此，本發明之惡意程式偵測裝置 1 之儲存單元 11 中更儲存一門檻資料庫，該門檻資料庫記錄了構成一惡意程式所需要的行為數門檻值、行為規範數門檻值以及行為規範種類。

具體而言，請參閱第 4 圖，其係描繪本發明之門檻資料庫之示意圖。門檻資料庫中的「惡意行為編碼」欄位係記錄各種惡意行為的種類，並且以前述之編碼方式記錄；「惡意行為規範編碼」欄位係記錄一惡意行為所包含之惡意行為規範的種類，並且以編碼方式記錄；「行為規範數門檻值」欄位係記錄構成一惡意行為所需要的惡意行為規範數；「行為數門檻值」欄位係記錄構成一惡意程式所需要的惡意行為數。

舉例來說，一惡意程式 A 具有一惡意行為 A-1，因此「惡意行為編碼」欄位記錄 A-1，惡意行為 A-1 會執行五個處理程序，因此「惡意行為規範編碼」欄位記錄 1、2、3、4 及 5，分別為與該五個處理程序所對應之五個惡意行為規範之編碼，即 1 代表惡意行為 A-1 之第一惡意行為規範，2 代表惡意行為 A-1 之第二惡意

行為規範，以此類推。由於惡意行為 A-1 包含五個惡意行為規範，因此惡意行為 A-1 之「行為規範數門檻值」欄位為 5，代表若執行了與該五個惡意行為規範相對應之五個處理程序即構成惡意行為 A-1；由於惡意程式 A 包含惡意行為 A-1 與惡意行為 A-2，因此「行為數門檻值」欄位為 2，代表若進行了惡意行為 A-1 與惡意行為 A-2 二個惡意行為即構成惡意程式 A。

更進一步地，一惡意行為所包含之惡意行為規範可區分為基本惡意行為規範與選擇性惡意行為規範。具體來說，基本惡意行為規範係指構成一惡意行為所不可或缺的惡意行為規範，而選擇性惡意行為規範則並非為構成一惡意行為所必要的惡意行為規範。舉例而言，請參閱第 4 圖中的惡意行為 C-4，其「惡意行為編碼」欄位記錄 1、2、3、4、5、6 及 7，其中 1、2、3、4 及 5 屬於基本惡意行為規範，亦即欲構成惡意行為 C-4 必須包含 1、2、3、4 及 5 此五個惡意行為規範，缺一不可；而 6 及 7 則屬於選擇性惡意行為規範，欲構成惡意行為 C-4 只需包含 6 及 7 此二個惡意行為規範其中之一即可。據此，惡意行為 C-4 之行為規範數門檻值為 6，其係由五個基本惡意行為規範加上一個選擇性惡意行為規範計算而得。基本惡意行為規範及選擇性惡意行為規範之種類與個數端視實際應用時各個惡意程式之特性而定，並不用以限制本發明之範圍。

須特別說明者，前述儲存單元 11 中所儲存之惡意行為資料庫 3 以及門檻資料庫 4 除了可由本發明之惡意程式偵測裝置 1 建立並儲存於儲存單元 11 中外，亦可由其它裝置（如電腦、伺服器、運

算裝置等）事先建立後再傳送至惡意程式偵測裝置 1，並儲存於儲存單元 11；或者可由其它裝置建立後儲存於一儲存裝置，惡意程式偵測裝置 1 便透過與該儲存裝置連線以存取儲存於該儲存裝置之惡意行為資料庫 3 以及門檻資料庫 4。因此，建立與儲存惡意行為資料庫 3 以及門檻資料庫 4 之裝置並不用以限制本發明之範圍。

接著，以下將詳述本發明之惡意程式偵測裝置 1 如何偵測惡意程式，為便於理解，以下將偵測惡意程式之流程搭配實例作說明。首先，當一程式於惡意程式偵測裝置 1 上執行時，該程式執行一第一處理程序，此時，處理單元 13 便自該第一處理程序擷取該第一處理程序之一第一執行標的、一第一執行動作以及一第一鏈結資訊，其分別為「Reg」、「Openkey」以及「Software\Microsoft\Internet Explorer\Main」，並建立一第一行為規範「Reg|Openkey|Software\Microsoft\Internet Explorer\Main」。接著，處理單元 13 便自惡意行為資料庫 3 中搜尋是否有與該第一行為規範相同之惡意行為規範，由第 3 圖之惡意行為資料庫 3 可知，該第一行為規範與編碼為 A-1:1 之惡意行為規範相同，於是處理單元 13 便自惡意行為資料庫 3 擷取出編碼 A-1:1，並將編碼 A-1:1 暫存於一串列表中。

另一方面，惡意程式偵測裝置 1 亦可能於一時間週期內同時執行複數個程式，各程式更包含複數個處理程序，而惡意程式之偵測係針對單一個程式作比對，以偵測各個程式是否為惡意程式；因此，惡意程式偵測裝置 1 必須辨識一處理程序係由哪一個程式所執行。據此，處理單元 13 更用以將與該程式相對應之一程式辨

識資訊（process ID）附加於該第一行為規範。舉例而言，處理單元 13 附加一代碼 70 於編碼 A-1:1，此時該第一行為規範以編碼 A-1:1,70 表示，其中代碼 70 表示第一行為規範係由該程式所執行。程式辨識資訊之形式與附加方式可視實際應用情形而調整，並不用以限制本發明之範圍。

處理單元 13 接著根據前述之比對結果建立並更新一行為記錄表，例如一雜湊列表（hash table），請參閱第 5 圖，其係描繪本發明之行為記錄表之示意圖。雜湊列表 5 係用以統計經處理單元 13 比對過後之惡意行為規範數是否累積構成一惡意行為，以及統計惡意行為之數目是否累積構成一惡意程式。如第 5 圖所示，雜湊列表 5 之「惡意程式/惡意行為」欄位用以記錄處理單元 13 已比對到的惡意程式編碼或惡意行為編碼，「程式辨識資訊」欄位用以記錄一比對到的惡意程式或惡意行為係由哪一程式所執行，「累積數」欄位則記錄已比對到的惡意行為規範累積數目或已比對到的惡意行為累積數目。

舉例來說，處理單元 13 於比對該第一處理程序符合編碼 A-1:1,70 之惡意行為規範後，便於雜湊列表 5 的「惡意程式/惡意行為」欄位記錄 A-1，於「程式辨識資訊」欄位記錄 70，以及將「累積數」欄位之數目增加 1，於此實施例中，A-1 之累積數由 4 增加至 5，代表處理單元 13 已比對到五個屬於惡意行為 A-1 的惡意行為規範。接著，處理單元 13 根據門檻資料庫 4 中惡意行為 A-1 的行為規範數門檻值為 5 判斷此五個比對到的惡意行為規範已構成惡意行為 A-1，因此，處理單元 13 更進一步將雜湊列表 5

中惡意程式 A 的累積數增加 1，代表處理單元 13 目前已比對到屬於惡意程式 A 的一個惡意行為。

同理，當該程式執行一第二執行程序，處理單元 13 更根據上述流程比對該第二執行程序是否符合一惡意行為規範，並根據比對結果更新雜湊列表 5；最後，處理單元 13 更可根據門檻資料庫 4 中「行為數門檻值」欄位中的數值判斷已比對到的惡意行為數目是否構成一惡式程式。藉由上述方式，本發明之惡意程式偵測裝置 1 可逐一比對一程式中的各處理程序，並判斷該程式是否為一惡意程式。

此外，由第 4 圖之門檻資料庫 4 可得知，惡意行為 A-1 所包含的惡意行為規範為 1、2、3、4 及 5，處理單元 13 比對到此五種惡意行為規範其中之一便會更新雜湊列表 5 中惡意行為 A-1 的累積數，然而一程式亦可能重複執行了相同的處理程序兩次，舉例來說，一程式執行了兩次惡意行為 A-1 所包含的惡意行為規範 1，但此情況下惡意行為 A-1 的累積數只能增加 1，否則將造成比對上的誤判。因此，為了避免這樣的情況，處理單元 13 必須進一步確認是否重複比對。

如前所述，處理單元 13 於自惡意行為資料庫 3 擷取出一第一編碼後，便將該第一編碼暫存於一串列表中，該串列表即可用以核對相同的編碼是否重複出現，當處理單元 13 自惡意行為資料庫 3 擷取出一第二編碼後，處理單元 13 首先比對該第二編碼是否已出現於該串列表中；若是，代表比對到相同的惡意行為規範，此時處理單元 13 即不更新雜湊列表 5；若否，代表比對到不同的惡意

行為規範，此時處理單元 13 即會更新雜湊列表 5。藉由此方式，本發明之惡意程式偵測裝置 1 可避免因重複比對所造成的誤判。

於前述比對方式中，處理單元 13 係根據一程式之一處理程序建立一行為規範，並比對該行為規範是否符合一惡意行為規範，其中，比對的方式為比對該行為規範之執行標的、執行動作以及鏈結資訊是否符合惡意行為資料庫 3 中所記錄之惡意行為規範。惟部分加殼變種惡意程式之處理程序中的鏈結資訊亦可能是隨機變動的，換言之，所建立出來的行為規範可能無法於惡意行為資料庫 3 比對到完全符合的惡意行為規範，造成比對上的漏洞。

據此，為了克服此一缺點，本發明之惡意程式偵測裝置 1 更將惡意程式之處理程序中的鏈結資訊分為三類，其分別為固定式鏈結資訊、隨機式鏈結資訊以及隨機且連續式鏈結資訊，以下將分別詳述針對此三類鏈結資訊的比對方式。首先，當一處理程序被歸類為固定式鏈結資訊時，代表該處理程序的鏈結資訊是固定不變的，亦即該處理程序每次執行時皆會產生相同的鏈結資訊，處理單元 13 根據該處理程序所產生的行為規範每次皆相同，因此處理單元 13 可直接將該處理程序之執行標的、執行動作以及鏈結資訊與惡意行為資料庫 3 作比對，亦即屬於固定式鏈結資訊之行為規範的比對係同時比對執行標的、執行動作以及鏈結資訊。

其次，當一處理程序被歸類為隨機式鏈結資訊時，代表該處理程序的鏈結資訊是隨機變動的，即鏈結資訊內容中的文字是隨機產生的，並且只會出現一次而不會重複使用。舉例來說，鏈結資訊內容中包含一檔案名稱為隨機命名的.exe 檔，該.exe 檔的檔案

名稱為隨機產生，因此該檔案名稱每次皆不同。簡言之，該處理程序每次執行時分會產生不同的鏈結資訊，處理單元 13 根據該處理程序所產生的行為規範每次皆不相同，因此處理單元 13 於比對此類的處理程序時，只將處理程序之執行標的以及執行動作與惡意行為資料庫 3 作比對，亦即屬於隨機式鏈結資訊之行為規範的比對只比對執行標的以及執行動作。

最後，當一處理程序被歸類為隨機且連續式鏈結資訊時，代表該處理程序的鏈結資訊是隨機變動且會連續出現的，即鏈結資訊內容中的文字是隨機產生的，但會重複使用。舉例來說，一惡意程式的一第一處理程序為「創造隨機名稱的 htm 檔」，其鏈結資訊中即包含一檔案名稱為隨機命名的.htm 檔，假設為 abc.htm，而該惡意程式的一第二處理程序為「寫入隨機名稱的 htm 檔」，其鏈結資訊亦會包含 abc.htm，因此 abc.htm 雖然為隨機命名，但會重複出現於該惡意程式之不同的處理程序中。據此，當一程式的一第一處理程序被歸類為隨機且連續式鏈結資訊時，處理單元 13 會將該第一處理程序的鏈結資訊暫存於一暫存雜湊列表中，當比對該程式的一第二處理程序時，處理單元 13 會比對該第二處理程序是否具有與暫存雜湊列表中相同的鏈結資訊，若有，即代表該第二處理程序符合一惡意行為規範。據此，藉由上述的比對方式，本發明之惡意程式偵測裝置 1 將可有效地偵測各種加殼變種的惡意程式。

當一程式被比對為符合一惡意程式時，處理單元 13 更用以傳送一偵測結果至輸出單元 15，輸出單元 15 更用以產生一影像或一音

效以通知一使用者偵測到一惡意程式，輸出單元 15 可為顯示器、揚聲器或其它可以用以呈現偵測結果之裝置，並不以此為限。

本發明之第二實施例如第 6 圖所示，其係為一種用於如第一實施例所述之惡意程式偵測裝置之惡意程式偵測方法。該惡意程式偵測裝置用以偵測一程式，且包含一儲存單元以及一處理單元，該儲存單元用以儲存一惡意行為資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範，該處理單元與該儲存單元電性連接，該程式執行一第一處理程序。

此外，第二實施例所描述之惡意程式偵測方法可由一電腦程式產品執行，當惡意程式偵測裝置經由一電腦載入該電腦程式產品並執行該電腦程式產品所包含之複數個程式指令後，即可完成第二實施例所述之惡意程式偵測方法。前述之電腦程式產品可儲存於電腦可讀取記錄媒體中，例如唯讀記憶體（read only memory；ROM）、快閃記憶體、軟碟、硬碟、光碟、隨身碟、磁帶、可由網路存取之資料庫或熟習此項技藝者所習知且具有相同功能之任何其它儲存媒體中。

第 6 圖係描繪第二實施例之惡意程式偵測方法之流程圖。首先，此惡意程式偵測方法執行步驟 601，令該處理單元根據該第一處理程序建立一第一行為規範。接著，執行步驟 602，令該處理單元比對該第一行為規範與該惡意行為規範，並產生一比對結果。

該惡意程式偵測裝置之該儲存單元更儲存一門檻資料庫，該門檻資料庫記錄該惡意程式之一行為規範數門檻值以及一行為數門檻值，該行為記錄表記錄一行為規範數以及一行為數，該惡意程

式偵測方法接著執行步驟 603，令該處理單元根據該比對結果更新該行為規範數。以及，執行步驟 604，當該行為規範數達到該行為規範數門檻值時，令該處理單元更新該行為數。最後，執行步驟 605，當該行為數達到該行為數門檻值時，令該處理單元判斷該程式為該惡意程式。

此外，前述之該惡意程式係包含一惡意行為，該惡意行為執行一第二處理程序，此惡意程式偵測方法於步驟 601 前更可執行一步驟 606（第 6 圖中未繪示），令該處理單元根據該第二處理程序建立該惡意行為規範。

於步驟 602 中，係令該處理單元比對該第一行為規範與該惡意行為規範，並產生一比對結果。更詳細而言，該第一行為規範包含該第一處理程序之一第一執行標的、一第一執行動作以及一第一鏈結資訊，該惡意行為規範包含該第二處理程序之一第二執行標的、一第二執行動作以及一第二鏈結資訊，此惡意程式偵測方法於步驟 602 係執行，令該處理單元透過比對該第一執行標的與該第二執行標的，比對該第一執行動作與該第二執行動作，以及比對該第一鏈結資訊與該第二鏈結資訊以產生該比對結果。

除了上述步驟外，此惡意程式偵測方法更可執行一步驟 607（第 6 圖中未繪示），令該處理單元將與該程式相對應之一程式辨識資訊附加於該第一行為規範，俾該處理單元可根據該程式辨識資訊判斷該第一行為規範對應至該程式；以及一步驟 608（第 6 圖中未繪示），令該處理單元產生與該惡意行為規範相對應之一編碼，並以該編碼表示該惡意行為規範。

除了上述步驟，第二實施例亦能執行第一實施例所描述之操作及功能，所屬技術領域具有通常知識者可直接瞭解第二實施例如何基於上述第一實施例以執行此等操作及功能，故不贅述。

綜上所述，本發明係為事先建立一惡意行為資料庫以及一門檻資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範，該門檻資料庫記錄該惡意程式之一行為規範數門檻值以及一行為數門檻值。當一程式於本發明之惡意程式偵測裝置執行一處理程序時，惡意程式偵測裝置根據該處理程序建立一行為規範，比對該行為規範與該惡意行為規範，並產生一比對結果；接著，根據該比對結果更新一行為規範數，當該行為規範數達到該行為規範數門檻值時，更新一行為數，當該行為數達到該行為數門檻值時，判斷該程式為該惡意程式。藉此，本發明係可克服習知防毒軟體之更新速度無法跟上加殼變種惡意程式之增加速度的缺點，同時具有加速惡意行為之比對效率以及提高病毒程式之偵測率之優點。

上述之實施例僅用來例舉本發明之實施態樣，以及闡釋本發明之技術特徵，並非用來限制本發明之保護範疇。任何熟悉此技術者可輕易完成之改變或均等性之安排均屬於本發明所主張之範圍，本發明之權利保護範圍應以申請專利範圍為準。

【圖式簡單說明】

第 1 圖係為本發明第一實施例之示意圖；

第 2 圖係為本發明行為規範之示意圖；

第 3 圖係為本發明惡意行為資料庫之示意圖；

第 4 圖係為本發明門檻資料庫之示意圖；

第 5 圖係為本發明行為記錄表之示意圖；以及

第 6 圖係為本發明第二實施例之流程圖。

【主要元件符號說明】

1：惡意程式偵測裝置	11：儲存單元
13：處理單元	15：輸出單元
2：行為規範	3：惡意行為資料庫
4：門檻資料庫	5：雜湊列表

七、申請專利範圍：

1. 一種用以偵測一程式之惡意程式（malware）偵測裝置，該程式執行一第一處理程序，該惡意程式偵測裝置包含：

一儲存單元，用以儲存一惡意行為資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範；以及

一處理單元，與該儲存單元電性連接，並用以：

產生與該惡意行為規範相對應之一編碼，並以該編碼表示該惡意行為規範；

根據該第一處理程序建立一第一行為規範；

比對該第一行為規範與該惡意行為規範，並產生一比對結果；

根據該比對結果更新一行為記錄表；以及

根據該行為記錄表判斷該程式為該惡意程式。

2. 如請求項 1 所述之惡意程式偵測裝置，其中該惡意程式包含一惡意行為，該惡意行為執行一第二處理程序，該處理單元係根據該第二處理程序建立該惡意行為規範。

3. 如請求項 2 所述之惡意程式偵測裝置，其中該第一行為規範包含該第一處理程序之一第一執行標的以及一第一執行動作，該惡意行為規範包含該第二處理程序之一第二執行標的以及一第二執行動作，該處理單元更用以透過比對該第一執行標的與該第二執行標的，以及比對該第一執行動作與該第二執行動作以產生該比對結果。

4. 如請求項 2 所述之惡意程式偵測裝置，其中該第一行為規範包含該第一處理程序之一第一鏈結資訊，該惡意行為規範包

含該第二處理程序之一第二鏈結資訊，該處理單元更用以透過比對該第一鏈結資訊與該第二鏈結資訊以產生該比對結果。

5. 如請求項 1 所述之惡意程式偵測裝置，其中該儲存單元更用以儲存一門檻資料庫，該門檻資料庫記錄該惡意程式之一行為規範數門檻值以及一行為數門檻值，該行為記錄表記錄一行為規範數以及一行為數，該處理單元更用以：

根據該比對結果更新該行為規範數；

當該行為規範數達到該行為規範數門檻值時，更新該行為數；以及

當該行為數達到該行為數門檻值時，判斷該程式為該惡意程式。

6. 如請求項 1 所述之惡意程式偵測裝置，其中該處理單元更用以將與該程式相對應之一程式辨識資訊附加於該第一行為規範，俾該處理單元可根據該程式辨識資訊判斷該第一行為規範對應至該程式。

7. 一種用於一惡意程式偵測裝置之惡意程式偵測方法，該惡意程式偵測裝置用以偵測一程式，且包含一儲存單元以及一處理單元，該儲存單元用以儲存一惡意行為資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範，該處理單元與該儲存單元電性連接，該程式執行一第一處理程序，該惡意程式偵測方法包含下列步驟：

(a1)令該處理單元產生與該惡意行為規範相對應之一編碼，並以該編碼表示該惡意行為規範

(a2)令該處理單元根據該第一處理程序建立一第一行為規範；

(b)令該處理單元比對該第一行為規範與該惡意行為規範，並產生一比對結果；

(c)令該處理單元根據該比對結果更新一行為記錄表；以及

(d)令該處理單元根據該行為記錄表判斷該程式為該惡意程式。

8. 如請求項 7 所述之惡意程式偵測方法，其中該惡意程式包含一惡意行為，該惡意行為執行一第二處理程序，該惡意程式偵測方法更包含下列步驟：

(e)令該處理單元根據該第二處理程序建立該惡意行為規範。

9. 如請求項 8 所述之惡意程式偵測方法，其中該第一行為規範包含該第一處理程序之一第一執行標的以及一第一執行動作，該惡意行為規範包含該第二處理程序之一第二執行標的以及一第二執行動作，該惡意程式偵測方法更包含下列步驟：

(f)令該處理單元透過比對該第一執行標的與該第二執行標的，以及比對該第一執行動作與該第二執行動作以產生該比對結果。

10. 如請求項 8 所述之惡意程式偵測方法，其中該第一行為規範包含該第一處理程序之一第一鏈結資訊，該惡意行為規範包含該第二處理程序之一第二鏈結資訊，該惡意程式偵測方法更包含下列步驟：

(g)令該處理單元透過比對該第一鏈結資訊與該第二鏈結資訊以產生該比對結果。

11. 如請求項 7 所述之惡意程式偵測方法，其中該儲存單元更儲存一門檻資料庫，該門檻資料庫記錄該惡意程式之一行為規範數門檻值以及一行為數門檻值，該行為記錄表記錄一行為規範數以及一行為數，該惡意程式偵測方法更包含下列步驟：

(h)令該處理單元根據該比對結果更新該行為規範數；

(i)當該行為規範數達到該行為規範數門檻值時，令該處理單元更新該行為數；以及

(j)當該行為數達到該行為數門檻值時，令該處理單元判斷該程式為該惡意程式。

12. 如請求項 7 所述之惡意程式偵測方法，更包含下列步驟：

(k)令該處理單元將與該程式相對應之一程式辨識資訊附加於該第一行為規範，俾該處理單元可根據該程式辨識資訊判斷該第一行為規範對應至該程式。

13. 一種電腦程式產品，內儲一種用於一惡意程式偵測裝置之惡意程式偵測方法之程式指令，該惡意程式偵測裝置用以偵測一程式，且包含一儲存單元以及一處理單元，該儲存單元用以儲存一惡意行為資料庫，該惡意行為資料庫記錄一惡意程式之一惡意行為規範，該處理單元與該儲存單元電性連接，該程式執行一第一處理程序，該程式指令包含：

一程式指令 A1，令該處理單元產生與該惡意行為規範相對應之一編碼，並以該編碼表示該惡意行為規範；

一程式指令 A2，令該處理單元根據該第一處理程序建立

一第一行為規範；

一程式指令 B，令該處理單元比對該第一行為規範與該惡意行為規範，並產生一比對結果；

一程式指令 C，令該處理單元根據該比對結果更新一行為記錄表；以及

一程式指令 D，令該處理單元根據該行為記錄表判斷該程式為該惡意程式。

14. 如請求項 13 所述之電腦程式產品，其中該惡意程式包含一惡意行為，該惡意行為執行一第二處理程序，該程式指令更包含：

一程式指令 E，令該處理單元根據該第二處理程序建立該惡意行為規範。

15. 如請求項 14 所述之電腦程式產品，其中該第一行為規範包含該第一處理程序之一第一執行標的以及一第一執行動作，該惡意行為規範包含該第二處理程序之一第二執行標的以及一第二執行動作，該程式指令更包含：

一程式指令 F，令該處理單元透過比對該第一執行標的與該第二執行標的，以及比對該第一執行動作與該第二執行動作以產生該比對結果。

16. 如請求項 14 所述之電腦程式產品，其中該第一行為規範包含該第一處理程序之一第一鏈結資訊，該惡意行為規範包含該第二處理程序之一第二鏈結資訊，該程式指令更包含：

一程式指令 G，令該處理單元透過比對該第一鏈結資訊與該第二鏈結資訊以產生該比對結果。

17. 如請求項 13 所述之電腦程式產品，其中該儲存單元更儲存一門檻資料庫，該門檻資料庫記錄該惡意程式之一行為規範數門檻值以及一行為數門檻值，該行為記錄表記錄一行為規範數以及一行為數，該程式指令更包含：

一程式指令 H，令該處理單元根據該比對結果更新該行為規範數；

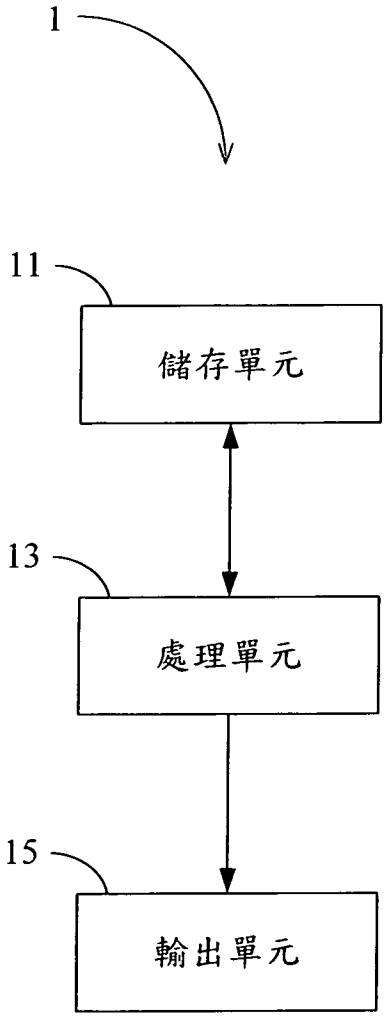
一程式指令 I，當該行為規範數達到該行為規範數門檻值時，令該處理單元更新該行為數；以及

一程式指令 J，當該行為數達到該行為數門檻值時，令該處理單元判斷該程式為該惡意程式。

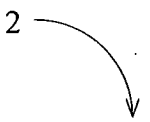
18. 如請求項 13 所述之電腦程式產品，該程式指令更包含：

一程式指令 K，令該處理單元將與該程式相對應之一程式辨識資訊附加於該第一行為規範，俾該處理單元可根據該程式辨識資訊判斷該第一行為規範對應至該程式。

八、圖式：



第 1 圖



執行標的	執行動作	鏈結資訊
File	Creat	C\DOCUME~\NTU\LOCALS~1\Temp\XXX.htm

第 2 圖

執行標的	執行動作	鏈結資訊	編碼
Reg	Openkey	Software\Microsoft\Internet Explorer\Main	A-1:1
Reg	SetValue	FormSuggest Passwords	A-1:2
File	Creat	C\DOCUME~\NTU\LOCALS~1\ Temp\MyMalware.htm	A-2:1
File	Write	|<HTML><HEAD><TITLE>xIEPo$ter1</ TITLE></HEAD><BODY><script>function qqw(){self.parent.location="http:// www.globaltourswest.com/ wcmd.txt";}setTimeout("qqw()",10000);</script></ BODY></HTML>	A-2:2

第 3 圖

4

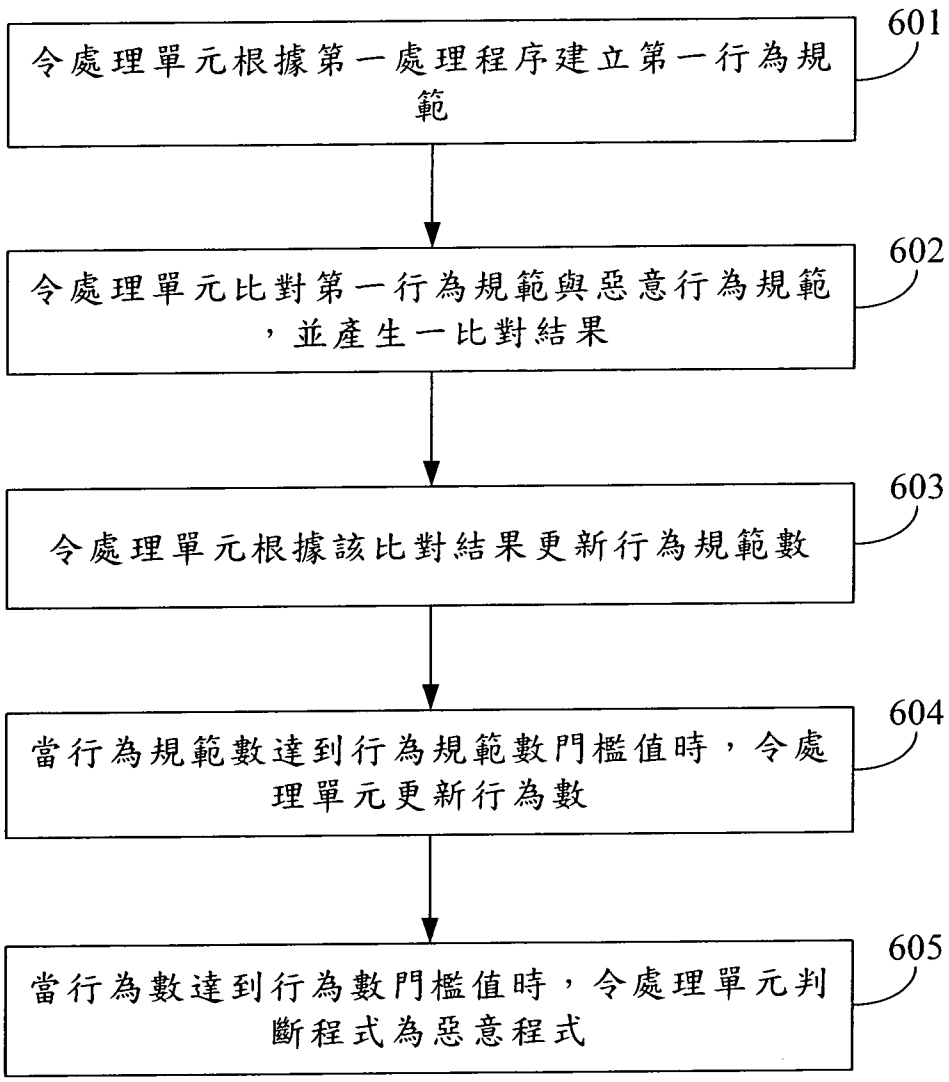
惡意行為編碼	惡意行為規範編碼	行為規範數門檻值	行為數門檻值
A-1	1, 2, 3, 4, 5	5	2
A-2	1, 2	2	2
B-1	1, 2, 3	3	3
B-2	1, 2, 3, 4	4	3
B-3	1, 2	2	3
C-1	1, 2, 3, 4	4	5
C-2	1, 2, 3	3	5
C-3	1, 2, 3, 4	3	5
C-4	1, 2, 3, 4, 5, 6, 7	6	5
C-5	1, 2, 3, 4	4	5

第 4 圖

5

惡意程式/惡意行為	A-1	A-2	A
程式辨識資訊	70	70	70
累積數	4	1	1

第 5 圖


令處理單元根據第一處理程序建立第一行為規範
601
令處理單元比對第一行為規範與惡意行為規範，並產生一比對結果
602
令處理單元根據該比對結果更新行為規範數
603
當行為規範數達到行為規範數門檻值時，令處理單元更新行為數
604
當行為數達到行為數門檻值時，令處理單元判斷程式為惡意程式
605

第 6 圖