電腦病毒科技發展史之研究

孫郁興
（清雲科技大學，本會會員）

本論文以年代史縱觀的方式，羅列電腦病毒科技發展史的緣起，論及 DOS 時代，Windows 時期著名的電腦病毒，Linux 的電腦病毒，與網際網路蠕蟲木馬及後門程式等論題，周易的窮則變變則通哲理即是其遵循的理則。本文對於有興趣想通盤了解電腦病毒科技發展史者，有著重要的指引作用。

關鍵詞：電腦病毒，蠕蟲，特洛依木馬，後門程式，科技發展史

壹、歷史緣起

1960 年，美國著名的 AT&T 貝爾實驗室中，三個年輕人(Victor Vyssotsky, Robert Morris Sr., 與 Doug McIlroy)在無聊的工作之餘，使用 IBM 7090 電腦玩起一種遊戲叫"Darwin",彼此比賽撰寫出能夠吃掉別人程式的程式來互相作戰。

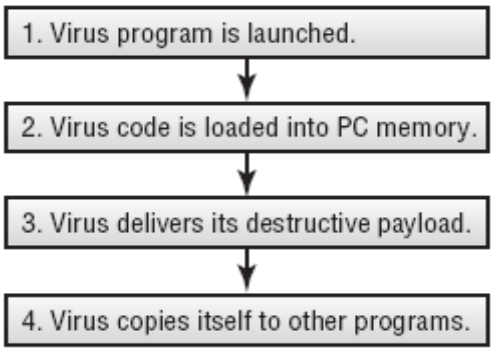
1983 年，南加州大學的學生 弗雷德・科恩（Fred Cohen）在 UNIX 系統下，寫了一個會引起系統當機的程式。科恩爲了證明其理論而將這些程式以論文發表出來，科恩的程式使電腦病毒具備破壞性的概念成形。

1984 年杜特尼 A. K. Dewdney 專欄作家在 Scientific American（《科學美國人》）上，推廣一種能於蘋果二號電腦上執行叫做「磁芯大戰」（core war）的遊戲時，開始把這種程式稱之爲"virus"（病毒）〔註 1〕。此後對於這種具感染或破壞性的程式皆被稱呼爲「病毒」。此一年代則進一步將電腦病毒具「感染性」的特性概念指出。對於此一磁芯大戰的原始定義如下: "Core Wars is a game played by two or more programs (and vicariously by their authors) written in an assembly language called Red code and run in a virtual computer called MARS (for Memory Array Red code Simulator). The object of the game is to cause all processes of the opposing program to terminate, leaving your program in sole possession of the machine".

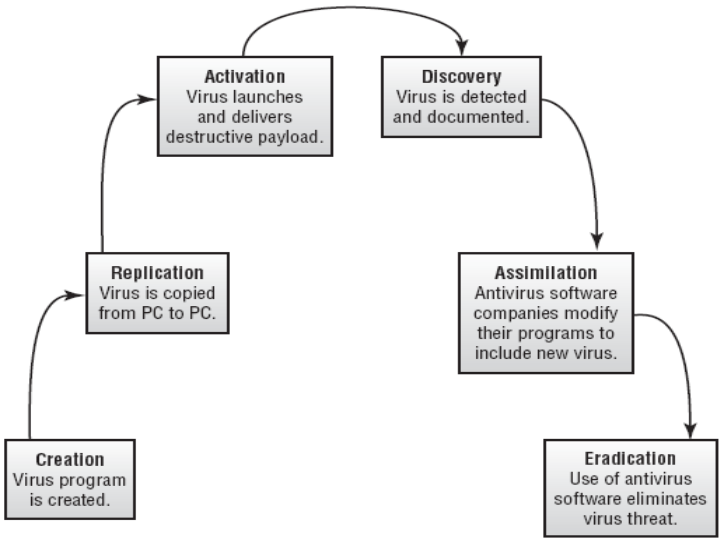
1985 年 Thomas J. Ryan 寫了一本科幻小說《P-1 的春天》（The Adolescence of P-1），成爲美國的暢銷書，作者在這本書中描寫了一種可以在電腦中互相傳染的病毒，此一病毒最後控制了約 7,000 台的電腦，遂造成了一場災難。

1987 年，第一個電腦病毒 C-BRAIN 誕生。此一電腦病毒始祖是附生於磁碟開機磁區,並具備完整自我繁殖的特徵。這個病毒程式是由巴斯特（Basit）和阿姆捷特（Amjad）

所撰寫，他們於巴基斯坦經營一家販賣個人電腦的商店，由於盜拷軟體的風氣非常盛行，因此他們撰寫的目的是爲了防止他們販賣的軟體被任意盜拷。只要有人盜拷他們販賣的軟體，C-BRAIN 就會發作，將盜拷者的硬碟空間給刪除。 其後，一些人士則以 C-BRAIN 的技術爲藍圖，製作其變形的病毒。易云:窮則變。因應有窮而化生，各種掃毒、防毒、與防毒軟體以及以電腦病毒爲業的專業公司如曇花般湧現。圖一及圖二則分別顯示電腦病毒如何感染你的電腦及電腦病毒的生命週期關係。



圖一：電腦病毒如何感染你的電腦



圖二：電腦病毒的生命週期

貳、DOS 的電腦病毒

米開朗基羅（Michelangelo）病毒: 此一米開朗基羅病毒的殺傷力驚人:每年 3 月 6 日米開朗基羅生日時，這個病毒就會以 Format 硬碟來爲這位元大師祝壽。於是乎辛苦建立的所有資料全毀於一旦。

耶路撒冷（Jerusalem）病毒： 這個病毒有個更廣爲人知的別稱，叫做「黑色星期五」。每逢十三號又是星期五的日子，這個病毒就會發作。發作時將會終止所有使用者所執行的程式。

音樂蟲病毒（Music Bug）:這個病毒發作時會大聲唱歌，甚至使資料流失且無法開機。此一病毒是臺灣土產的病毒，發作時會高唱著「兩隻老虎」。所以，當你聽到電腦

自動傳來一陣音樂聲時，有可能是電腦中毒了。

猴子（Monkey）病毒: Monkey 是第一個「引導型」的病毒，只要你使用被 Monkey 感染過的系統軟碟開機，病毒就會入侵到你的電腦中，伺機刪除硬碟的 FAT 分區表，使電腦一開機就出現 Invalid drive specification 的訊息。

Burglar 病毒:因病毒中有字串 Grave，又稱 Grave 病毒，病毒長度爲 1150 位元組，所以有的地方又稱它爲 1150 病毒，它可感染 DOS 的.EXE 檔。由於病毒將最後一塊記憶體控制塊打斷，造成系統常規記憶體跟 UMB 分離;結果當病毒駐留記憶體時，用 MEM 或 MI 將看不到 UMB，病毒在送回目錄項之前先將染毒檔長度減去 1150 位元組，結果用 DIR 命令看不到染毒檔長度的增加，病毒在打開檔，執行檔，提交檔，修改檔屬性，取磁碟空間等功能都要進行傳染，而這些功能在一個普通檔的執行過程中,幾乎百分百的被用到，造成病毒的傳播很快。

DOS 時期的病毒種類繁雜，且有多種的病毒被多人改寫。於 DOS 時期的後期甚至出現"病毒多體引擎"，此一多體引擎可以將病毒碼自動改易其特徵碼， 並創造出更多不同特徵的面貌，讓防毒軟體無法辨識！病毒發作的症狀更是迥異，有的會唱歌、有的會刪除檔案、有的會格式化(Format)硬碟、有的還會在螢幕上顯出各式各樣的圖形與音效。

參、Windows 的電腦病毒

風行全球的 Windows 3.1 作業系統的出現，正式宣告個人電腦的操作環境進入 Windows 時代。Windows 95/98 於其後的大暢銷，更使得現在所有個人電腦的操作環境幾乎都是在 Windows 狀態。在 Windows 環境下最知名的病毒，就屬「巨集病毒」與「32 位元病毒」。

巨集病毒(Macro Virus)：因應 Windows 套裝軟體的發展，許多軟體廠續提供「巨集」的功能，讓使用者可運用「巨集」的方式，將一些繁瑣的過程記錄成一個簡單的巨集指令備方便操作。然此種方便操作的功能，在歷經有心人士的設計之後，使原 DOS 時代著名的「檔案感染型」病毒進入一個新的里程碑：傳統的檔案感染型病毒只會感染附檔名爲 exe 和 com 的執行檔，而此一新型的巨集病毒則會感染 Word、Excel、AmiPro、Access 等軟體儲存的資料檔。此巨集病毒可跨不同版本的操作平臺仍能工作。以 Word 的巨集病毒爲例，可感染 DOS、Windows 3.1/95/98/NT、OS/2、麥金塔等等系統上的 Word 檔及通用範本。巨集病毒中，最有名的除了 Melissa 巨集病毒之外就是令人聞之色變的 Taiwan NO.1B 巨集病毒及 SetMode WORD 巨集病毒。Taiwan NO.1B 巨集病毒的發作情形如下：每月的十三號，只要您隨便開啓一份 Word 檔，螢幕上會出現一對話視窗，詢問你一道龐雜的算數題。答錯的話就會連續開啓二十個視窗，然後又出現另一道問題，如此重複下去，直到耗盡系統資源當機爲止。巨集病毒雖有高的傳染能力，但它的破壞力並不強，且解毒也較容易，不用防毒軟體亦可經由手動的方式解毒。

32 位元病毒：「32 位元病毒」是在 Windows 95 之後所產生的一種新型態檔案感染型病毒，它同樣是感染 exe 執行檔，但這種病毒專挑 Windows 的 32 位元程式下手，其中最著名的就是 CIH （陳盈豪）病毒了。CIH 病毒的厲害處，在於其可以把自己的病

毒本體拆散後填充在被感染的 exe 執行檔中，因此作爲, 使受感染的檔案大小不會有所變化，防毒軟體不易察覺。最後版本的 CIH 病毒，除了每月 26 日發作將硬碟 Format 外，並改寫主機板 BIOS 內的資料，讓你無法開機。

病毒入侵之共同必要特徵：取得 CPU 控制權。文件巨集型病毒和傳統型 病毒的共同特徵，就是凡病毒都必須要取得最上層的控制權才能在無形中去感染 其他檔案，傳統型病毒感染檔案的方法是從使用者(USER)發出指令和 DOS I/O（存取）之間切入來取得控制權，而文件巨集型病毒則是透過 NORMAL.DOT 來取 得控制權，所以在這一點上就和傳統型病毒有異曲同工之妙，因爲 Word 啓 動之後便會自動載入 NORMAL.DOT，如果您的 NORMAL.DOT 含有巨集病毒， 那麼進入 Word 後，您在 Word 中的一舉一動便全在病毒的掌握之下，就好比 電腦中了開機型病毒而不自覺，只要電腦一開機病毒自動就常駐在您的記憶體 中。就破壞方面而言，事實上 Microsoft 在設計 WordBasic 的同時，已就呼叫 DOS 指 令及檔案的能力都考慮進去，使得原先在 DOS 下的 FORMAT.COM、 DEBUG.EXE 都可以在 Word 裡被呼叫使用，也就是說在 Word 裡巨集病毒可以 呼叫 FORMAT.COM 來 FORMAT 您的硬碟，也可以呼叫 DEBUG.EXE 來產生 檔案型病毒，自動幫您放在 AUTOEXEC.BAT 中，讓您每次開機就會自動執行到病毒，在 WordBasic 所提供的磁碟存取函數之中，還包括了刪除、拷貝、建 立目錄、更改檔案屬性、甚至連線網路磁碟機（MAP）…等等功能。

肆、Linux/Unix 的電腦病毒

Staog 病毒: 1996 年發現的 Staog 病毒是 Linux 系統下的第一個病毒，它出自澳大利亞一個叫 VLAD 的組織。Staog 病毒是用組合語言編寫，專門感染二進位檔，並通過三種方式去嘗試得到 root 許可權。 Staog 病毒並不會對系統有什麼實質性的損壞。它向世人揭示了 Linux 可能被病毒感染的潛在危險。

Bliss 病毒: Linux 系統上第二個被發現的病毒是 Bliss 病毒，它是一個不小心被釋放出來的實驗性病毒。與其他病毒不同的是，Bliss 本身帶有免疫程式，只要在運行該程式時加上 “disinfect-files-please”選項，即可恢復系統。

Ramen worm 雷門蠕蟲〔註 2〕：2001 年發現 Ramen 蠕蟲。Ramen 蠕蟲可以自動傳播。它只感染 Red Hat 6.2 和 7.0 版使用匿名 FTP 服務的伺服器，它通過兩個普通的漏洞 RPC.statd 和 wu-FTP 感染系統。這不是一個危險的蠕蟲，且不會對伺服器做出任何有破壞性的事情。但是當它開始掃描時，將消耗大量的網路帶寬。

Lion.worm 獅子蠕蟲： 2001 年 3 月，美國 SANS 學院的全球事故分析中心(Global Incident Analysis Center, GIAC)發現，一種新的針對使用 Linux 系統的電腦的蠕蟲病毒正通過網際網路迅速蔓延，它將有可能對用戶的電腦系統造成嚴重破壞。這種蠕蟲被命名爲獅子蠕蟲，與 Ramen 蠕蟲非常相似。獅子蠕蟲能通過電子郵件把一些密碼和配置檔發送到一個位於 china.com 的功能變數名稱上。Dartmouth 學院安全技術研究所工程師威廉・斯蒂恩斯說：「攻擊者在把這些檔發回去之後就可以通過第一次突破時的缺口再次進入整個系統。」這就是它與 Ramen 蠕蟲的不同之處。Ramen 蠕蟲是一種比較友善的病毒，它在侵入系統後會自動關閉其中的漏洞，而這個獅子蠕蟲卻讓那些漏洞敞開並開

闢新的漏洞。以至於如果系統感染了這個獅子蠕蟲，不能百分之百確信這個系統有挽救的價值，更加合理的猜測其動作很有可能是蠕蟲轉移你的資料並且重新格式化硬碟。一旦電腦被感染，獅子蠕蟲就會強迫電腦開始搜尋別的受害者。不過，感染獅子蠕蟲的系統少於感染 Ramen 蠕蟲的系統，但是獅子蠕蟲所造成的損失卻比 Ramen 蠕蟲大得多。除上述之外，其他 Linux/UNIX 平臺的主要威脅有：Klez、OSF.8759、Slapper、Scalper、Svat 和 BoxPoison 等病毒。

Unix Invader (入侵者): 1995 年 6 月 UNIX 下的電腦病毒 Unix Invader (入侵者)誕生, 是由 htk 所撰寫, 其特點有:1.具有 daemon process 的特性(lose control tty)故該 process owner 沒上線該病毒依舊能作用執行,不會被系統終結.2.其可感染 UNIX 上 script file 和各型 binary file(要屬性得宜) ,不重複感染.感染完後,該執行檔或 script file 依舊可執行 3.在記憶體上所用的隱藏方法是,掃描 passwd file,取用該 user 的 login shell base name 作爲程式名,故,用 ps -aux(ps 看不到)或 top 之類的程式,要仔細看,才會被發現 4.不重複長駐,頂多一個 user 一隻,目地是爲擴大感染能力。

Linux 平臺下的病毒茲羅列如下：

可執行檔型病毒：可執行檔型病毒是指能夠寄生在檔中的，以檔爲主要感染物件的病毒。病毒製造者們無論使用什麼武器，彙編或者 C，要感染 ELF 檔都是輕而易舉的事情。這方面的病毒如 Lindose，當其發現一個 ELF 檔時，它將檢查被感染的機器類型是否爲 Intel 80386，如果是，則查找該檔中是否有一部分的大小大於 2,784 位元組（或十六進位 AEO），如果滿足這些條件，病毒將用自身代碼覆蓋它並添加宿主檔的相應部分的代碼，同時將宿主檔的入口點指向病毒代碼部分。

蠕蟲（worm）：Ramen 蠕蟲爆發後，Eugene H. Spafford 爲了區分蠕蟲和病毒，給出了蠕蟲的技術角度的定義，「電腦蠕蟲可以獨立運行，並能把自身的一個包含所有功能的版本傳播到另外的電腦上。」（worm is a program that can run by itself and can propagate a fully working version of itself to other machines. ）。

腳本病毒：目前出現比較多的是使用 shell 腳本語言編寫的病毒。此類病毒編寫較爲簡單，但是破壞力同樣驚人。Linux 系統中有許多的以.sh 結尾的腳本檔，而一個短短十數行的 shell 腳本就可以在短時間內遍曆整個硬碟中的所有腳本檔，進行感染。其破壞性可以是刪除檔，破壞系統正常運行，甚至下載一個木馬到系統中等等。

後門程式：在廣義的病毒定義概念中，後門也已經納入了病毒的範疇。活躍在 Windows 系統中的後門這一入侵者的利器在 Linux 平臺下同樣極爲活躍。從增加系統超級用戶帳號的簡單後門，到利用系統服務載入，共用庫檔注射，rootkit 工具包，甚至可裝載內核模組（LKM），Linux 平臺下的後門技術發展非常成熟，隱蔽性強，難以清除。是 Linux 系統管理員極爲頭疼的問題。

伍、網際網路的蠕蟲木馬及後門程式

Internet 的盛行更使資訊大量流通，但對於散播病毒、盜取他人帳號密碼的電腦駭客來說，網路正好提供了一個絕佳的秘密管道。由於網際網路的便利，電腦病毒傳染的途徑更是多元。傳統的病毒可運用磁片或其他存儲媒體的方式散佈，現在只要在電子郵

件, SKYPE, MSN 或 ICQ 中，夾帶一個檔案寄給朋友，就可能把病毒一起傳染給他；甚至從網路上下載免費的檔案中，都可能夾帶一個含有病毒的檔案。不隨便從無關的網站下載文件，安裝防毒軟體並隨時更新病毒碼，對於下載後的所有檔案不要執行，先啓動查毒的步驟，中毒的情形多半可避免。爲區分 Internet 蓬勃發展之後所出現的新病毒，這種新出現的病毒本質上與傳統病毒有著頗大的差異。Internet 病毒傳染的途徑是依附於網際網路的流覽器，網路協定漏洞，及作業系統漏洞上。初始爲方便網頁設計者能在網頁上能造出更精彩的動畫及音效，使網頁能更具空間感，使用 Active X 及 Java 的技術，能夠分辨你使用的軟體版本，可建議使用者應該下載哪些軟體來更新版本，對於大部分的使用者來說頗爲方便。但若要讓這些網頁的動畫能夠正常執行，流覽器會自動將 Active X 及 Java applets 的程式下載到硬碟中。在此一運作的過程中，惡性程式的開發者也同樣利用此一管道，經由網路滲透到個人電腦之中。這就是近來崛起的「網路病毒」。

典型的作法與因應:透過網路傳送微軟系統的「說明檔」CHM (Complied HTML)格式，夾帶惡意程式檔案，透過網路寄送惡意電子郵件，以社交工程手法誘使收件人開啓說明檔，以達到入侵收件人電腦的目的。可能運用的手法如下：1. 透過惡意電子郵件:(1). 夾帶附檔：以附件檔(*.chm)型式，直接寄給收件人。(2). 郵件內文：在信件內文，以聳動或動人用語隱藏惡意網頁連接，誘使收件人點選下載。2. 透過網頁上的惡意網址以聳動或動人字彙隱藏惡意網頁連接，誘使瀏覽者點選下載。可採取作法如下：1. 郵件伺服器應禁止傳送夾帶*.CHM 等附件類型的檔案。2. 加強對使用者宣導，針對網路上下載的檔案，除了在確認來源及用途的情況下，勿開啓上述類型之檔案。3. 在管理上，建議用戶端的使用者帳號，不應具備本機最高管理權限(Administrators 群組)，避免惡意程式啓動與取得控制權。VBS_BubbleBoy蠕蟲:**為一**Internet郵件蠕蟲，無需用戶點擊附件就可自動執行。含有VBS_BubbleBoy的郵件主題是"BubbleBoy is back!"； 郵件內容包含一個無效URL和“The BubbleBoy Incident, pictures and sounds.”文本內容。在Outlook Express中，若用戶通過“預覽視窗（Preview Pane）”閱讀郵件時，BubbleBoy就會被啓動。而在Microsoft Outlook中，一旦染毒郵件被開啓，BubbleBoy就會自動執行蠕蟲程式。BubbleBoy 一旦發作，就是在C:\WINDOWS\START MENU\PROGRAMS\STARTUP 目錄中釋放一個名爲UPDATE.HTA 文件。

網路病毒可以偷偷地與設定的相關電腦連絡，因此病毒不再只是單槍匹馬的闖盪江湖，它也許只是一個偵查兵，小到只負責潛入的動作，蒐集足夠的資訊以提供網 路駭客們可以遠端遙控破壞。列舉典型如下:

工行釣魚木馬：這是一個十分狡猾的盜取網上銀行口令的木馬病毒。病毒運行後，在系統目錄下生成svchost.exe文件，然後修改註冊表啓動項以使病毒文件隨作業系統同時運行。病毒運行後，會監視微軟IE瀏覽器正在訪問的網頁，如果發現用戶在工行網上銀行個人銀行登錄頁面上輸入了帳號、口令，並進行了提交，就會彈出僞造的IE窗，內容如下： “爲了給您提供更加優良的電子銀行服務，6月25日我行對電子銀行系統進行了升級。請您務必修改以上資訊！”病毒以此誘騙用戶重新輸入口令，並將竊取到的口

令通過郵件發送到一個指定的163信箱。該病毒同時還會下載灰鴿子後門病毒，感染灰鴿子的用戶系統將被駭客遠程完全控制。

從病毒的傳染媒介來看，Active X被認爲是比Java更危險的感染途徑。基本上Active X可直接進入核心的呼叫功能，再連接到任何系統功能中。相對的，Java在設計上是利用Java虛擬機器(Virtual Machine)與作業系統服務隔離的。由於實行Java虛擬機器上的多種變化，使得Java可以用多種方式進入系統功能。事實上Netscape及微軟都把Java併到它們的瀏覽器上，這使得靠applet滋生的病毒得以繁殖。特洛依木馬程式〔註3〕則並不自我繁殖，也不去感染其他文件，其主要作用是竊取你的網遊帳號、口令和裝備，盜竊你的網上銀行口令、QQ口令、設計檔等隱私資料，可帶來被植入者巨大的經濟損失。

陸、結論

電腦病毒的破壞行爲體現了病毒的殺傷力。病毒破壞行爲的激烈程度取決於病毒作者的主觀願望和他所具有的技術。數以萬計、不斷發展擴張的病毒，其破壞行爲千奇百怪，難以做全面的描述。病毒破壞目標和攻擊部位主要是：系統資料區、檔、記憶體、系統運行、運行速度、磁片、螢幕顯示、鍵盤、喇叭、印表機、CMOS、主板等。病毒、蠕蟲、和木馬基本上意味著自動化的駭客行爲，也許被病毒攻擊比被駭客攻擊更可能發生。直接的駭客攻擊目標一般是伺服器，而病毒是等機會的麻煩製造者。選擇一個適合你系統的防毒產品，它們能幫你防止病毒的傳播。隨著科技的日新月異，更新、破壞性更大病毒的出現是必然。整個電腦發展史上，病毒與防毒軟體的對抗一直持續的進行，周易的窮則變變則通哲理即是其遵循的理則。

參考文獻

[1] http://mcraeclan.com/Graeme/CoreWars.htm

[2] http://tech.ccidnet.com/art/1099/20060111/412467_1.html

[3] http://computer.howstuffworks.com/virus.htm

[4] http://www.antivirus.com/vinfo/

[5] http://media.wiley.com/product_data/excerpt/77/07821412/0782141277-2.pdf

[6] Vesselin Bontchev, "Possible Virus Attacks Against Integrity Programs And How To Prevent Them", Proc. 2nd Int. Virus Bulletin Conf.,pp.131-141, September 1992.

[7]Vesselin Bontchev, "MtE detection test", Virus News International, pp. 26-34,January 1993.

[8]Vesselin Bontchev, "Analysis and Maintnance of a Clean Virus Library",Proc. 3rd Int. Virus Bulletin Conf., pp. 77-89, September 1993.

[9]David Ferbrache, "A Pathology of Computer Viruses", Springer-Verlag,1991.

註釋

[註1] 電腦病毒(Virus)：電腦病毒即是一支電腦的程式，不需要經由使用電腦者的同意，此一程式能經由許多不同結構的電腦間及不同架構的網路間，散佈複製其自己者謂之。

[註2] 電腦蠕蟲(Worm)：電腦蠕蟲類似於電腦病毒，然蠕蟲並不需要經由一個主動攜帶者的攜帶(蠕蟲能主動利用各種通信媒介於許多不同結構的電腦間完整的拷貝傳播其自己)。

[註3] 電腦特洛依木馬(Trojan Horse)：電腦特洛依木馬是一支電腦的程式,其所執行的部份特定工作並未被誠實的描述於其所宣稱的規格中(例如：宣稱程式能維護修正某一程式的小錯誤,實際上卻是順便執行偷取電腦中的特定資料遞送至遠方或執行覆蓋硬碟等未於規格所宣稱的動作)。