MSN 病毒簡介

楊慶隆
東華大學資工系助理教授
電算中心網路組組長
E-mail: cnyang@mail.ndhu.edu.tw

MSN 是一個傳遞文字、程式、影音圖片的平台，故可以將每一部有執行 MSN 的電腦當作是一部網路主機看待。目前透過 MSN 傳遞的病毒形式有幾種，最早的 MSN 病毒是透過 MSN 可以與朋友分享檔案的特性，將病毒本身透過檔案傳遞的方式送到 MSN 好友名單中的好友手中。倘若此時對方不注意的直接執行該檔案，則病毒就會感染該電腦中的 MSN 平台，並且將病毒本身再一次的傳遞給好友名單中的人員，以此達到散播病毒的目的。而最近的病毒則將傳遞檔案的方式改變為傳遞網址，倘若使用者點選從好友端所接收到的網址，由於 MSN 會將所接收到的網址透過內訂的瀏覽器開啟，因此，所連結到的網站會自動的將病毒下載到電腦中並感染 MSN 平台。受到感染的 MSN 平台則會繼續將這個含有病毒檔案的網址發送給 MSN 中的好友列表人員，使病毒擴散。總括來說，目前透過 MSN 傳遞並感染的途徑並不是 MSN 平台本身的程式漏洞，而是利用 MSN 平台的特性來達到病毒傳播的目的。

也因為如此，在 MSN 平台中可以傳遞的病毒特性將可以與傳統病毒結合，只要該病毒擁有傳遞訊息或是檔案給 MSN 平台中好友的能力，則任何形式的病毒傳播與感染都是有可能的。對於這些病毒的應應對策各家防毒軟體都已經有提出相對的解毒與防範措施，也都一再提醒使用者需要再三確認好友所傳遞的檔案或是連結是否有機會隱含病毒。其相對應的解毒方式除了使用者自行注意好友所傳送過來的檔案狀況外，也可使用掃毒軟體或是註冊表監控軟體，使其可以針對此類病毒於更動與 MSN 相關之註冊表時可以及時攔截，以避免遭受感染。由於此類病毒的傳遞並非是透過軟體漏洞造成(EX:疾風病毒)，而是透過平台來傳遞

病毒，所以對於未使用 MSN 的使用者將不會有所影響。

就如同之前席捲全球的 E-mail 形式病毒(I love You)相似，電子郵件本身所夾帶的檔案以及一些特殊的控制指令才是造成病毒傳播的主因，這些檔案或是指令都需要使用者將檔案開啟或是使用者的收信軟體自動化的完成某些具有威脅性的命令才能達成感染，使用者所採用的收信軟體功能越強相對的風險也就越大。回過頭來看到近日在 MSN 中所傳遞的病毒(EX:Bropia 病毒)，也是透過 MSN 傳遞訊息的特性來達到感染，而日後許多自動與多元化的服務，也將存在很高的風險提供病毒一個傳遞的平台。日後病毒的傳遞模式有很大的機會是轉移到每個人身邊所使用的訊息傳遞工具，舉凡手機、PDA、行動電腦等，有能力透過網路連接使用者或是可完成訊息傳遞的工具，越臻完備且多功能的裝置或是通訊平台都將成為病毒散播的媒介。所以建議有藍芽功能的手機，不使用藍芽功能時應該關閉以確保安全。

總括而言，由於 MSN 病毒的傳遞方式與 E-mail 病毒類似，也因此對於這些病毒的追蹤非常困難，且就算是能有機會追蹤到病毒的散播處，其也有可能是一部放置在某辦公室中早已被入侵當成傳遞跳板而不自知的一部電腦，因此，對於病毒確切發源的追蹤是一件十分不容易的事。只是現在傳撥的媒介換成 MSN 而已，現在的 MSN 病毒大部分都是 Worm(蠕蟲)，具有自行複製傳播的能力，所以只要中了這種病毒，就會不斷的散撥。寫病毒的人可能只是為了證明自己的能力，所以當然會往容易散撥成功或是方便散撥的方向去寫，所以未來，病毒還是透過 MSN 等等軟體傳播。

最近常出現的 MSN 病毒名稱，感染方式及解毒工具整理如下表。

MSN 病毒統計表

日期	MSN 病毒名稱	感染方式	解毒工具
2002/7/12	WORM_SURNOVA.A	透過 msn 傳送病毒檔案	手動清除
2002/10/9	即時通訊病毒 WORM_RODOK.A	透過 msn 傳送病毒訊息	手動清除
2003/1/10	莉娃病毒 WORM_LIRVA.C	由網路芳鄰上資源分享的資料夾、ICQ、IRC 甚至如 KaZaA	註(1)

		點對點檔案傳輸程式所分享的資料夾感染到其他電腦	
2003/6/6	頑皮熊 PE_BUGBEAR.B	感染特定執行檔如 ICQ、MSN 和 Outlook Express 等	手動清除
2003/7/29	WORM_SINIS.A	透過 msn 傳送病毒檔案	
2003/9/26	WORM_SMIBAG.A	透過 msn 傳送病毒檔案	註(2)
2003/12/12	TROJ_MSNMASMSG.A 我愛你 MSN 網路版病毒	透過 msn 傳送 “I Love You !!!” 訊息	手動清除
2004/7/9	TROJ_FLOODER.B MSN 結婚病毒	透過 msn 傳送 “明天我結婚”訊息	手動清除
2004/10/11	MSN 玩笑病毒 Worm_Funner.A	透過 msn 傳送訊息如：朋友，多注意休息啊，可以到這裡放鬆放鬆哦 http://www.**.com	註(2)
2005/02/03	MSN 火雞病毒 WORM_BROPIA.F	透過 msn 傳送檔案，並顯示裸體火雞圖片	註(2)
2005/03/07	WORM_KELVIR.A	超連結病毒	註(2)
2005/03/08	WORM_FATSO.A	接收檔案	註(2)

註(1): http://www.trendmicro.com/ftp/products/tsc/sysclean.com

註(2): http://www.trendmicro.com/ftp/products/tsc/tsc.zip

附錄(電腦病毒簡介)

病毒的設計原理?

電腦病毒在技術上來說，是一種會自我複製的可執行程式。大部份的電腦病毒都有一個共通的特性 - 它們通常都會發病。當病毒發病時，它很可能會破壞硬碟中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。

自從 Internet 盛行以來,，Java 和 ActiveX 的網頁技術逐漸被廣泛使用，一些有心人士利用 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，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。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。

病毒傳染的方式相當多，先前最為流行就是使用 E-Mail 的方式來傳染，但這一、兩年影音傳訊軟體、像 ICQ、MSN、Skype 等軟體開始運用的越來越廣泛，加上微軟在 Windows 系統提供 MSN 軟體後，成為目前使用人數最多的影音傳訊軟體，也因此改變了網路用戶們的生活及工作方式，有很多的工作在很多工作溝通和聯繫都透過 MSN 完成，所以就像先前使用 E-mail 的方式寄送病毒信的方

式，病毒利用通訊錄內的名單來寄發，所以一個人中毒之後往往會造成所有的 MSN 聯繫人都中毒。而且，很多後門程式會借助此病毒在網絡中廣泛傳播。

病毒碼又要如何解開呢?

當你使用 MSN 發現有以下幾種狀況，可能要小心……

- 發現一直有人傳檔案給你。
- 或是別人傳附檔名為 “.pif” 檔案給你。
- MSN 無法關閉，一直顯示正在與連絡人傳輸。

以上的狀況可能有心人士正在利用 MSN 傳播病毒或後門程式給你，這時千萬不要開啟或接收檔案，如果不小心中毒時，請依下列步驟進行….

1. 關閉 MSN Messenger。
2. 安裝防毒軟體並立刻更新防毒引擎與病毒碼。
3. 若不慎中毒請上網下載病毒清除工具。
4. 平日養成習慣，對於朋友傳送檔案之前先詢問對方，確認無誤後才下載檔案。
5. 養成每日備份資料。
6. 隨時上網了解病毒最新狀況。
7. 訂閱各家防毒公司的電報。

。

未來病毒設計的趨向？

目前病毒的型態依據寄宿及破壞的方式可以分成巨集病毒、開機型病毒、檔案型病毒、複合型病毒、隱型飛機式病毒及千面人病毒等，介紹如下：

一、巨集病毒 (Macro Virus)：

巨集病毒是目前最熱門的話題，它主要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、AmiPro 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。

二、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 的各類中斷 (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。

三、檔案型病毒 (File Infector Virus)：

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。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)。

四、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, *.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。

五、隱型飛機式病毒 (Stealth Virus):

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

六、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

未來病毒設計的趨勢將朝向自動大量散播、嚴重影響網路運作、中毒後難以根除等，特性並且隨著科技產品的普遍性提昇，病毒入侵的管道也趨向多元。

有否可能追蹤到設計病毒的駭客呢!

網路的世界雖快速連結遠距兩端的距離，但遠距兩端並不能真實的確定對方的身份，所以有很多網路的犯罪行為就是使用這種網路的特性來進行犯罪，但是凡走

過必留下痕跡，追蹤網路犯罪可以分析主機紀錄的 Log 檔案，找出蛛絲馬跡沿路追查，但到高一尺魔高一丈，駭客會使用攻擊跳板主機的方式進行犯罪，讓追查的困難度增加，大部分也使用公用電腦來進行攻擊，例如網咖等，目前追蹤駭客的方式如下：

- 誘陷裝置系統

  誘陷的目的是追查入侵來源。目前網路犯罪破案率相當低，誘陷與追蹤的相關性與重要性明顯可見，一般建議的方法是建立各重要網路出口監視系統，並配合網管系統，建立即時 caller ID 追蹤。這方面的成果主要是 NAI 的 CyberCop Sting Server，具有模仿 Windows NT、Solaris、以及 Cisco Router 等作業環境。是如何建置 Honey Pots 環境，則是更動 Inetd 或所有會洩漏系統資訊的地方，顯示令入侵者混淆的資訊，例如原是 Linux ，則換裝為 FreeBSD 或 Solaris。[8] 是偽裝成中 Back-Orifice 病毒的主機，引誘在網路專門掃瞄 BO 的受害者上門。[9] 介紹在 FreeBSD 如何建立如 Jail 的環境。

- 流量分析

  Thumbprint 的觀念在未來入侵線索的建立上將有極大助益。所謂 Thumbprint 是分析入侵者各種獨特可區分之特點，例如其打字速率、連線狀況、系統特有狀況，雖經網路大量 traffic 等 noise 影響，仍可經過濾後找出可供識別的特徵。這些特徵稱為 Thumbprint。類似的研究有別於一般網路證據蒐集的方法，必須監視及記錄入侵者通過的所有路徑，反而回到傳統現實環境的方法，盡可能只依賴犯罪現場所遺留的證據。更以流量分析的方法建立 passive filter，分析非互動 port 連線卻呈現互動連線流量，藉此偵測後門程式的存在。

- 稽核記錄

  一般遭受後門「污染」之系統，就不能確信任何稽核記錄檔。Bruce Schnier 最近則致力於 Forensics 的主題，研究如何保護不安全、或不能完全信賴主機上的系統記錄資料。

所以要如何追蹤駭客是一個困難度很高的行為，有時需要動用傾國之力才能完成，而這場矛與盾的戰爭會一直持續下去。