危機四伏：即時傳訊面臨的威脅

賽門鐵克安全機制應變中心　Neal Hindocha

簡介

即時傳訊即將成為惡意軟體(malware)的傳播媒介。越來越多人使用即時傳訊，不論是作為個人聯繫或企業商務用途。即時傳訊網路不只提供文字訊息的傳遞，也可以作為檔案傳輸之用。因此，即時傳訊也可傳輸病蟲與惡意軟體。即時傳訊也可以成為特洛依木馬的進入點。駭客可以透過即時傳訊，使用後門來存取電腦，而不需開

啟一個接聽埠(listening port)，就可以有效地繞過桌上型電腦與閘道防火牆。而且，駭客並不需要去掃描未知的 IP 位址，就可以輕易地從一個更新的好友名單資料庫中選出一個受害者。當即時傳訊新增的功能越來越多(例如：點對點的檔案分享)，即時傳訊也將會變得更容易傳遞惡意軟體。

而且，在使用如防火牆等傳統安全防護的企業中，即時傳訊是很難被攔截的。此外，一般而言，伺服器層級的防毒軟體不會監控即時傳訊的網路通訊。這意味著，只有在桌上型電腦上安裝防毒軟體才能抓到即時傳訊的病蟲。

幸運的是，防毒廠商已經瞭解到即時傳訊的危險，且已經開始在桌上型電腦用的防毒產品設計外掛程式(plug-ins)，以保護各種即時傳訊用戶端的安全。Norton AntiVirus 2003 即是一例，它可以掃描任何即時傳訊用戶端收進來的檔案。

當電子郵件變成我們日常生活的一部份時，它也變成大量病蟲的傳播媒介。即使已有許多電子郵件病蟲疫情的爆發，但還是有許多人沒有真正瞭解使用電子郵件的潛在危害。我們很希望這樣的狀況不會在即時傳訊上重演。

即時傳訊的威脅

即時傳訊的威脅不僅限於病蟲，也包括會匯出資料，並在系統安裝後門的特洛依木馬。而且，使用即時傳訊最大的威脅便是隱私權的問題。

病蟲

藉由電子郵件擴散的病蟲已成為任何電腦安全專家日常生活的一部份。某些病蟲因為社交工程術(social engineering)或者利用駭客工具(exploits)成功達到大量擴散的目的。但是，因為防毒軟體可以監控電子郵件流量，而且一般使用者也已經知道電子郵件病毒的威脅，因此通常可以快速的處理這些威脅。即時傳訊病蟲的數量持續成長，但目前還沒有防毒軟體可以直接監控即時傳訊的流量，而且只有少數是可以直接外掛到即時傳訊用戶端，並即時的監控接收的檔案。部分原因是因為：監控即時傳訊流量的難度，就跟監控它們所使用之不固定的用戶端與通訊協定是一樣的。

不幸的是，這使得即時傳訊變成進出電腦的任意門；因為它的流量會繞過大多數無法掃描到潛在病蟲的伺服器端安全工具。因此只有安裝在電腦上的防毒軟體才能抓到病蟲。

以下是某些利用各種即時傳訊來自行擴散的病蟲：

W95.SoFunny.Worm@m

W32.Aplore@mm

W32.Goner.A@mm

W32.Choke

JS.Menger.Worm

W32.FunnyFiles.Worm

W32.Annoying.Worm

W32.Mylife

W32.Maldal (some versions)

W32.Seesix.Worm

W32.Led@mm

VBS.Msnb.Worm

您可在以下網址找到更多關於這些病蟲的資訊：

http://securityresponse.symantec.com.

特洛依木馬

使用即時傳訊你就可以分享某人電腦上的每個檔案。所有熱門的即時傳訊都有檔案分享的功能，或者讓您可以運用修補程式或外掛程式來增加這樣的功能。駭客以即時傳訊取代在遠端電腦安裝後門木馬來存取檔案的好處在於：即使電腦使用的是動態 IP 位址，它的用戶名稱(screen name)也可能不會改變。再者，只要每次受害者上線，駭客就會收到通知。因此，這使得駭客可以更輕易的持續追蹤並存取被感染的電腦。另外，駭客不需要開啟一個新的可疑埠來進行通訊，只要透過已經開啟的即時傳訊埠就可以了。

有少數的特洛依木馬程式是針對即時傳訊。某些會改變組態的設定，所以可以分享整個硬碟的檔案。這種型態的特洛依木馬會造成很大的威脅，因為它們允許任何人可以完全的存取電腦裡的檔案。

也有許多傳統的特洛依木馬會使用即時傳訊來傳送訊息給特洛依木馬的作者，提供駭客被感染電腦的相關資訊。此資訊會包括被感染電腦的 IP 位址以及已經被開啟的埠號碼。

特洛依木馬藉由使用即時傳訊用戶端來存取電腦的檔案，這可能會比用傳統(classic)的特洛依木馬更難被發現。傳統的特洛依木馬會在電腦上開啟一個收聽或對外的埠(listening or outgoing port)，以連上遠端電腦。桌上型防火牆可以有效地攔截這些傳統的特洛依木馬。

然而，如果特洛依木馬透過即時傳訊用戶端來操作的話，它就不會開啟一個新的埠，因此，就不會被傳統的桌上型防火牆所攔截。

今日的特洛依木馬已經會利用即時傳訊。最近便發現有一個特洛依木馬會傳送 ICQ pager 訊息給特洛依木馬作者。它被命名為 Backdoor.AIMvision，會讓駭客竊取儲存在 Windows 登錄檔(register)的 AIM 相關資訊。也會讓駭客可以架構 AIM 用戶端。

另一個使用 ICQ 傳訊來聯絡作者的特洛依木馬稱為 Backdoor.Sparta.C。

劫奪與冒名(Hijacking and Impersonation)

駭客可以用許多不同的方法來假冒其他使用者。最常用的攻擊手法就是竊取沒有戒心的使用者(unsuspecting user)的帳號資訊。

帳號資訊遭竊對任何即時傳訊來說都是非常危險的。受害者好友名單上的人會信任駭客。因此，對駭客來說，這會使他們更容易說服好友名單上的人在電腦上執行某些檔案，或者公開機密資訊。因此遺失即時傳訊帳號密碼所造成的危險並不只限於遺失密碼的人，而是會影響更多人。

如果駭客想要取得使用者的帳號資訊，他們可以使用竊取密碼的特洛依木馬。假使即時傳訊用戶端的密碼儲存在電腦上，駭客就可以傳送特洛依木馬給沒有戒心的使用者。當此特洛依木馬執行時，它會找到受害者的即時傳訊密碼，並將密碼傳送給駭客。有很多工具都可以將資訊傳回給駭客，包括使用即時傳訊本身、IRC以及電子郵件。

因為這四家即時傳訊(AIM、Yahoo! Messenger、ICQ、MSN Messenger)通訊協定都沒有將他們的網路流量加密，因此駭客可以透過攔截式攻擊(man-in-the-middle attacks)來劫奪連線。駭客可以藉由插入訊息到進行中的聊天連線(chat-session)，以假冒在聊天室裡的人。

雖然這很困難，但駭客也可以使用攔截式攻擊(man-in-the-middle attacks)來劫奪整個連線。例如，一個離線的訊息看起來會像是來自伺服器，但有可能是駭客寄給受害者的。這有可能會導致用戶端斷線。駭客也可以使用簡單的拒絕服務駭客工具，或是其他無關的駭客工具(unrelated exploits)使用戶端斷線。

因為伺服器會維持連線狀態(keeps the connection open)，而它並不知道用戶端已經離線，因此駭客就可以假冒受害者。再者，因為所有的資料都沒有加密或者認證，駭客就可以使用像 ARP 欺騙的傳統攔截式攻擊(man-in-the-middle attacks)。

拒絕服務 (Denial of Service)

駭客可以使用許多方式來造成即時傳訊用戶端的拒絕服務(denial of service)。

某些拒絕服務攻擊會使即時傳訊當機。而有些型態的攻擊則會讓用戶端暫停(hang)，有時會消耗大量的 CPU，讓整個電腦變得很不穩定。

另一個常見的攻擊型態是用大量的訊息來灌爆特定使用者。許多即時傳訊用戶端會藉由允許受害者忽略某個特定的使用者，以避免遭到流量攻擊(flood-attacks)。但是，有許多工具讓駭客可以同時地使用許多帳號，或者自動地建立大量帳號以達到流量攻擊的目的。而且，在流量攻擊開始之後，當被攻擊的使用者瞭解發生什麼時，電腦可能已經沒有回應了。因此，你很難將攻擊的使用者帳號加到即時傳訊用戶端黑名單中(ignore list)。

在即時傳訊用戶端造成拒絕服務的只是一般的駭客工具。這些駭客工具極有可能變成最危險的拒絕服務攻擊類型，因為它是很難防範的。再者，某些駭客工具並不會真正的讓用戶端當機。相反的，它們會讓即時傳訊用戶端消耗大量的 CPU 時間。這會讓電腦變得沒有回應，而不只是即時傳訊用戶端暫停而已。

儘管拒絕服務攻擊的惱人程度大於實際的危害，但他們可以和其他攻擊結合，例如：劫奪連線等。

資訊洩漏 (Information Disclosure)

試圖從即時傳訊使用者找到系統資訊是現今很常使用的工具。IP address retriever 即是一例。

IP address retrievers 可以被用來達到許多目的。例如，如果 IP address retriever 與特洛依木馬一起使用，每一次只要受害者一上線，駭客就可以收到包含受感染電腦 IP 位址的訊息。

這樣一來，駭客就會知道被感染使用者的 IP 位址，即使使用者用的是動態 IP 位址。

駭客有許多像是 IP address retriever 等方式可以傳送資料，匯出特洛依木馬給沒有戒心的使用者(unsuspecting user)。藉由利用社交工程術(social engineering)或者潛在無關的駭客工具(unrelated exploits)，駭客可以讓沒有戒心的使用者執行檔案。該資料匯出特洛依木馬找到使用者電腦上的資料，並且透過即時傳訊網路將它回傳給駭客。

有許多針對各種即時傳訊用戶端之不同類型的資料竊取特洛依木馬。

例如，駭客可能會竊取使用者帳號的密碼。當使用者登出時，駭客就有該帳號的完全控制權。駭客可以執行各種工作，諸如改變密碼並傳送檔案給好友名單上的人。

另外，駭客無須使用特洛依木馬也有可能達到資訊洩漏的目的。因為透過即時傳訊網路傳送的資料是沒有加密的，所以駭客可以 sniff 封包，監控整個即時傳訊的通訊。這會非常危險，例如：假使企業內的員工使用即時傳訊來溝通敏感的企業資料，駭客就可以看到這個通訊，因此取得資訊。

針對 AIM 的特定威脅

病蟲

有許多病蟲使用各種即時傳訊網路來擴散蔓延。W32.Aplore@mm 是使用 AIM 網路來擴散蔓延的病蟲。該病蟲藉由傳送訊息到 AIM 好友名單上的所有聯絡人來擴散。

會出現以下訊息之一：

' btw, download this,

' I wanted to show you this,

' please check out,

' hey go to,

' see if you can get this to work,

' this is cool,

' tell me what you think about,

' try this,

' I almost forgot about,

' I like this,

' what about,

' have you seen,

' interesting,

' lol,

' wow,

' whoa,

' neat,

' cool,

' hmm,

' psst,

' hehe,

' haha,

' silly,

' weird,

在訊息中也會提供一個網頁參考訊息。此網頁是在一個被感染的電腦上，因為病蟲在埠 8180 上就像是個網頁伺服器。

網頁會出現以下資訊：

Browser Plugin Required

You may need to restart your browser for changes to take affect.

Security Certificate by Verisign 2002.

MD5:9DD756AC-80E057FC-E00703A2-F801F2E3

Click HERE and choose "Run" to install.

當然，您所下載的檔案會是病毒的副本。

你可在以下網址找到更多該病蟲的相關資訊：

http://securityresponse.symantec.com/avcenter/venc/data/w32.Aplore@mm.html.

漏洞(Exploits)

駭客常用的威脅型態是漏洞(exploit)。有幾個已知的 AIM 漏洞。AOL 藉由過濾惡意流量來快速修復伺服器端上大多數的漏洞。因此，在大多數的狀況下，使用者不需要更新他們的用戶端以免於漏洞的威脅。但是，有些漏洞需要使用者在用戶端上執行修補程式。

以下所列為近期的漏洞：

1. AIM Link Special Character Remote Heap Overflow Vulnerability

- ' 一個設計精巧特殊的 URL 字串可以導致 AIM 用戶端當機。

- 資料來源：http://online.securityfocus.com/bid/5492/info/

2. AIM Unauthorized Actions Vulnerability

- 藉由增加 AIM 資訊到網頁上的 meta refresh tag (重新整理標籤)，AIM 用戶端可以強制加到 AIM 好友名單上的群組與好友名單。

- 資料來源：http://online.securityfocus.com/bid/5246

3. AIM AddBuddy Hyperlink Vulnerability

- 大型目標：在網頁新增好友連結可能會導致 AIM 用戶端當機。

- 資料來源：http://online.securityfocus.com/bid/4709/info/

在 1999 年底，一種稱為 AIMThief 的工具被用來竊取 AIM 帳號。在 AIM 通訊協定使用駭客工具，該工具讓駭客可以輸入受害者的用戶名稱(screen name)。然後此工具會改變用戶名稱的密碼。

即使此工具無法再運作，它也會顯示出即時傳訊系統的弱點。再者，像這樣的弱點需要即時傳訊廠商採取某些行動，而且目前沒有暫時性的解決方案或修補程式可以提供給一般使用者。

針對 Yahoo! Messenger 的特定威脅

病蟲

目前尚未有病蟲利用 Yahoo! Messenger 來進行擴散。

漏洞

1. Yahoo!Messenger Call Center Buffer Overflow Vulnerability

- 它可能會在網頁上插入 ymsgr:// 以連結 Yahoo! 。Yahoo! Messenger 應用程式就會處理這些問題。如果有出現大量連結的要求，就有可能在 Yahoo! Messenger 的用戶端造成緩衝區溢位。

- 資料來源：http://online.securityfocus.com/bid/4837

2. Yahoo!Messenger Script Injection Vulnerability

- 如果 Yahoo!Messenger 與網頁瀏覽器整合，此弱點會在即時傳訊用戶端建立一個可以開啟網頁的連結，並且執行選擇的程序檔(script)。

- 資料來源：http://online.securityfocus.com/bid/4838

針對 ICQ 的特定威脅

病蟲

W32.Goner.A@mm是會利用 ICQ 即時傳訊網路來大量發送郵件以擴散蔓延的病蟲。它是以 Visual Basic 寫成的病蟲，並已使用 UPX 壓縮過。

如果電腦上已安裝了 ICQ，該病蟲就會執行以下動作：

1. 檢查 ICQ DLL 檔案的版本並確認該檔案包含了此病蟲想要利用的 APIs 。如果

   它找到一個正確的版本，此病蟲就會繼續進行。

2. 取得目前在線上所有聯絡人的清單。

3. 取得每個使用者的個別資訊，而此資訊是傳送檔案必要的。

4. 病蟲會將自己傳送給清單上的所有使用者。

你可在以下網址找到更多 W32.Goner.A@mm 的相關資訊：

http://securityresponse.symantec.com/avcenter/venc/data/w32.goner.a@mm.html.

特洛依木馬

ICQ 讓使用者可以使用網頁瀏覽器傳送訊息。特洛依木馬的作者開始利用這個功能。例如，名為 Backdoor.Sparta.C 是一隻傳統的特洛依木馬，它會在電腦上開啟埠，以接收傳送進來的連線。然而，在感染某個使用者後，Backdoor.Sparta.C 將會在網站上使用 ICQ 傳送一個訊息給後門作者。該訊息傳送的資訊包括 IP 位址，有哪些埠被開啟以及一些關於被感染電腦的資訊。

你可在以下網址找到更多這個特洛依木馬的相關資訊：

http://www.sarc.com/avcenter/venc/data/backdoor.sparta.c.html.

漏洞

1. ICQ 2001/2002 Malformed Message Denial Of Service Vulnerability

- ICQ 允許在訊息中插入笑臉的圖案。如果大量的笑臉被插進訊息中，則接收該訊息的 ICQ 用戶端就會暫停 10~20 秒，消耗掉所有的 CPU 時間。它也可能會當機而不只是暫停。
- 資料來源：http://online.securityfocus.com/bid/5295

2. Mirabilis ICQ Soundscheme Predictable File Location Vulnerability

- ICQ soundscheme (scm) 檔案預設的動作是：開啟它並且將包含 scm 檔案的聲音檔放在硬碟的一個已知位置。此檔案將會被下載並且安裝在下列的位置：

C:\ProgramFiles\ICQ\Sounds\[name]。如果知道檔案會被儲存在哪裡，檔案執行弱點就可以被利用。有幾個利用 Internet Explorer 已經被提報出來。

- 資料來源：http://online.securityfocus.com/bid/5247

迴避認證工具(Authorization Bypassing Tools)

在 ICQ 裡，您可以在將某個使用者加到另一個使用者的好友清單前，設定是否需要認證。但是，有許多工具可以迴避認證的要求，這會讓未經授權的使用者可以決定另一個使用者的狀態是在線上或是離線。

這些工具可以繞過認證的要求，因為 ICQ 將好友清單儲存在本機電腦上，但是其他所有的即時傳訊都是將好友清單儲存在伺服器上。伺服器ICQ 的最新版也使用伺服器來儲存好友清單。但是，因為回溯相容性(backwards compatibility)的緣故，存放在本機電腦的好友清單就可以被送到伺服器。

針對 MSN Messenger 的特定威脅

病蟲

已有許多病蟲利用MSN Messenger 即時傳訊網路擴散。這可能是因為 MSN Messenger 提供大量的文件服務、以及讓應用程式和服務互動的簡便性。

W32.Choke.Worm 是利用 MSN Messenger 網路來擴散蔓延的病蟲。

此病蟲會鉤住(hook) MSN Messenger，因此當某好友首次開始和一個被感染的系統進行文字交談時，遠端的系統會傳送以下文字訊息：

President bush shooter is game that allows you to shoot Bush balzz hahaha

和訊息同時出現的是邀請使用者下載一個名為 ShootPresidentBUSH.exe 的檔案。如果好友拒絕下載，此病蟲就會重複傳送此邀約。此病蟲會記得每一個已經接受病蟲副本的好友名稱，並以笑臉回應他們所傳回的每個訊息。

你可在以下網址找到更多關於該病蟲的資訊：

http://securityresponse.symantec.com/avcenter/venc/data/w32.choke.worm.html.

漏洞

1. Microsoft MSN Messenger Malformed Invite Request Denial of Service

- MSN Messenger 中會有一個遭破壞的標頭(corrupted header)，它的邀請需求會導致 MSN Messenger 用戶端當機。
- 資料來源：http://online.securityfocus.com/bid/4827/info/

2. Microsoft MSN Messenger Message Spoofing Vulnerability

- 資料來源：http://online.securityfocus.com/bid/4316/info/

3. Microsoft MSN ActiveX Object Information Disclosure Vulnerability

- 因為文件開啟功能中的軟體錯誤，您將可以讀取某個使用者的好友清單，並假冒該使用者。該惡意程式碼會與病蟲使用的駭客工具一起傳送出去。此病蟲稱為 JS.Menger.Worm。您可在以下網址找到更多關於該病蟲的資訊：

  http://securityresponse.symantec.com.

- 資料來源：http://online.securityfocus.com/bid/4028/info/

攔截即時傳訊

我們很難避免使用即時傳訊。如果用戶端可以使用如 HTTP port 80 與 FTP port 21 等一般的通訊埠(destination ports)，則簡易的埠攔截防火牆會法無效攔截它，。如果用戶端無法透過預設的埠來進行溝通，則大多數的用戶端都會自動架構(auto-configure)以使用其他非預設的埠。

具備通訊協定分析的防火牆，可防止即時傳訊用戶端透過如 port 80 的一般目的地埠來進行通訊，因為即時傳訊的流量與 HTTP 流量是不同的。然而，所有的用戶端將通訊資料嵌入在一個 HTTP 連線要求裡，以避開通訊協定的分析。

用戶端與回應基本上必須預先擱置(prepend) HTTP 標頭到每一個傳送的封包，因此巧妙地避開任何通訊協定分析的防火牆。例如 ICQ 與 AIM 的用戶端，只有在必須使用 HTTP proxy 時，HTTP 標頭才會被加上去。雖然，AOL提供免費的 proxy 存取，(網址為：www.proxy.aol.com)，如果所有的埠都會攔截直接存取的話，那麼用戶端就會自動架構(auto-configure)以使用這個 proxy。

即使如此，在 AIM 與 ICQ 的中，還是可以藉由攔截位址來防止存取 proxy，網路上有許多其他免費提供的 proxy 伺服器。您只要在網路上稍微搜尋一下，就會出現上百個免費提供的 proxy 伺服器。要攔截每個 proxy 伺服器是很困難的，而且也會是管理上的惡夢。

制定企業政策是防止內部員工使用即時傳訊的最佳方法。

即時傳訊的未來

即時傳訊已經被證明是人們進行溝通的良好輔助工具，而且它兼具隱密性與專業性。即時傳訊用戶端已經變得更好使用，而且它們也開始運用如語音通訊與檔案傳輸等其他功能。

即時傳訊使用者的數量目前已有上百萬，而且越來越多人申請這四家主要即時傳訊網路的服務。

即時傳訊有許多問題，但提供這些服務的公司若能加以教育與提供更好的回應，將可協助減少這些問題。許多公司修復伺服器端的漏洞(exploits)，因此可以避免使用者在用戶端執行修補程式的問題。

令人訝異的是，目前只有少數的病蟲與其他型態的惡意軟體利用即時傳訊來進行擴散；但在未來，這種情況卻會越來越多。而且我們也可以看到這些網路有更多的協同運作。AOL 已經和 ICQ 合作，我們很快的就可以看到 AIM 與 ICQ 的協同運作。但是，此協同運作卻可能會讓病蟲可以游走於這四個網路之間，而不僅限於一個單一的網路。

隱私議題與記錄即時傳訊流量的能力對企業來說也是重要的功能，某些即時傳訊提供用戶端加密的通訊。然而，當這些功能被整合進合法的用戶端以及它們使用的網路時，企業就會更依賴即時傳訊來進行通訊。

結論

因為目前駭客針對的是個人使用者，所以整體而言，駭客對任何即時傳訊網路並不是大威脅。從另一方面來說，病蟲會針對特定網路的所有使用者，因此在未來它們顯然會造成更大的威脅。

我們已經可以看到使用安全漏洞(security exploits)的病蟲可在短時間內迅速擴散蔓延。紅色警戒(Code Red)與寧達病蟲(Nimda)就是利用安全漏洞(security exploits)來迅速擴散蔓延。

即時傳訊不太可能在短期內變成像今日電子郵件般的成為病蟲主要的傳播媒介。今日使用電子郵件的人數多於即時傳訊，因此病蟲利用電子郵件才能使擴散範圍更大。如果病蟲將自己傳送給通訊錄上的所有聯絡人，則它也有潛力將自己傳送給您企業中的每個員工。然而，如果相同的病蟲將自己傳送給即時傳訊好友名單上的所有聯絡人，則它可能只會接觸到幾個人而已。

再者，主要的即時傳訊網路仍然使用專屬的通訊協定(proprietary protocols)。所以，使用 MSN Messenger 的病蟲不會影響使用 Yahoo! Messenger 服務的使用者。因此，如果用戶端變得可以彼此協同運作，或使用者利用某個主要的網路，則即時傳訊病蟲可能會變得更容易擴散。

然而，以上的討論並不表示您就可以無視於即時傳訊可能造成的威脅。目前已有超過 20 隻的病蟲可以透過即時傳訊擴散，同時也有許多針對各種即時傳訊用戶端的漏洞(exploits)。

未來，系統漏洞(exploits)將會變成駭客攻擊系統的主要方式。如果不同的即時傳訊可以協同運作，即時傳訊廠商的安全追蹤紀錄就可能是企業決定用哪一種即時傳訊的關鍵因素。

企業內的電子郵件流量通常是由防毒軟體來監控。因此，一旦偵測到特定的病蟲，被感染的電子郵件會在伺服器被阻斷。但就即時傳訊而言，防毒軟體目前無法監控閘道端的流量。如果病蟲開始使用即時傳訊擴散，我們就無法在它到達使用者電腦前加以阻止。

即時傳訊病蟲的數量正在逐月增加中，再看看這些得逞的病蟲，我們可以想像即時傳訊很快的就會成為惡意威脅的溫床。

我們應該更小心地使用即時傳訊，教育使用者是我們可以確保安全使用它們的最佳方式。我們誠心希望，在未來不會看到任何即時傳訊被病蟲利用而造成可怕的疫情。