運用監控工具與入侵偵測於即時通訊以防治蠕蟲之設計

陳炳彰
南台科技大學資訊傳播系
bcchen@mail.stut.edu.tw

張耀升
南台科技大學資訊傳播所
m96f0207@webmail.stut.edu.tw

摘要

即時通訊(Instant Message, IM)軟體可說是現今最熱門的網路商品之一，根據相關研究報導，即時通訊(Instant Message, IM)軟體在 2006 年將達到 42 億美金的市場規模，而全球使用人數更將突破億人大關，也因此成為網路攻擊的主要標的。攻擊者利用惡作劇的社交工程（social engineering）技倆來欺騙電腦使用者下載能自我快速複製的蠕蟲，開啟病毒感染的檔案或網路，或是在毫無防備的情況下安裝惡意程式。因此本研究運用 MSN Sniffer 與入侵偵測系統來防護即時通訊上蠕蟲的攻擊。

關鍵詞：即時通訊(IM)、入侵偵測、蠕蟲、MSN Sniffer。

Abstract

IM (Instant Message, IM) software is popular of network goods, according to research reports, in 2006, IM (Instant Message, IM) software will reach 4.2 billion dollars in the size of the market, and the users of the worldwide will exceed 100 million people, making it the main subject of Internet attacks. Attack is use the mischievous social engineering (social engineering) tricks to deceive computer users can download copies of the worm of self-fast, open-infected files or the Internet, Perhaps in the situation which does not guard against installs the malicious programs . this study use MSN Sniffer intrusion detection and protection system to instant messaging IM-WORM avoid the attack.

Keywords: Instant Message(IM) 、 Intrusion Detection、Worm、MSN Sniffer.

1. 前言

隨著網際網路的普及應用，網路得以蔓延至各個家庭、個人，乃至於各大、中、小型企業及政府機構，隨著網路使用人口的增加，網際網路服務與流量也與之劇增，其中讓世界各地最為喜愛的服務就是即時通訊，為什麼它令人喜愛呢？是因為它具有以下幾個特色(鄭進興 郭洺坤 程毓明，2008)：

1.即時性:IM 之所以可以那麼普遍最主要的原因就是其即時性的功能所致，能夠讓大家可以於第一時間內溝通，而不需要像傳統 e-mail 之溝通方式一般，一來一返，往往都要耗上個一、兩天的時間。

2.便利性:IM 的另一項功能就是，當需要聯絡相關人員時，只要開啟 IM 視窗哪位人員是否在線上都可以一目瞭然。減去了電話通知的費用，也更節省了時間。

3.娛樂性:現在的 IM 因為越來越受時下年輕人所喜愛，因此也推出了不少附加的娛樂功能，如表情符號、動畫傳遞、自訂畫像、視訊功能等。

加上由於即時通訊應用的高普遍性且廣受歡迎，使得安全攻擊獲得了擁有了極大的發展空間和破壞能力。豐富的功能是即時通訊吸

引使用者的主要手段之一，但從安全的角度來講，功能的豐富化恰恰是與嚴格的安全準則背道而馳的。作為一種為了最大化溝通能力而存在的應用系統，其認證機制和保護手段是相對比較薄弱的，很容易為惡意攻擊行為所利用。

2. 相關文獻研究

2.1 OMS 簡介

因此便有學者針對即時通訊蠕蟲做一個警示系統，其系統主要是利用重新導向的方式對使用者發出警告該連結並不安全，以可降低使用者在不知情的情況下誤點惡意連結(鄭進興 郭沼坤 程毓明，2008)。

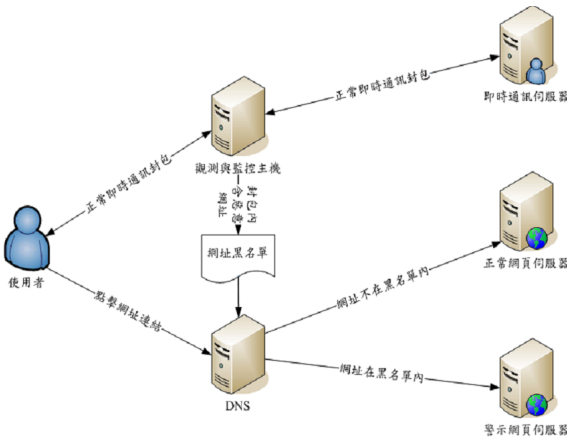

圖 1 網路架構圖

其系統的網路架構如圖 1，建置了一台觀測與監控主機在路由器之前，使用兩張網路卡，使得所有出入口的封包都必須經過該觀測與監控主機，用來分析與判斷封包內容。

因此本研究即針對(點對點蠕蟲防治研究-以即時通訊蠕蟲防治為例)做了其改善的方式。此篇爲了能夠防禦點對點蠕蟲攻擊所帶來的釣魚網站，構想出一個防禦的方法，並且由一台觀測主機，及網址黑名單的建立與 DNS 的配合來防治釣魚網站。

首先需要架設觀測主機，觀測主機需能夠發現出封包內是否有網址，如有網址出現的話就與白名單做比對，白名單是由一些網站需要用到帳號密碼登錄的網頁，記錄下他們的 1.IP 位址、2.領域名稱、3.CSS 參數等三項資料的特徵庫。如果有進行比對後出現類似不符合以上三個條件的可疑網頁，

觀測系統就會將此網頁加入黑名單，並且將黑名單傳送至 DNS，DNS 則會依此黑名單作依據，讓有人點入黑名單網站的時候引導到警示網頁，此作法能夠讓釣魚網站區隔開來讓人避免受騙。

2.2 MSN Sniffer

MSN Sniffer 是一個輕巧的網路控制程式，可以攔截、監測網路上的 MSN 聊天對話。它會自動紀錄對話，而且所有被攔截的訊息都能用 HTML 格式儲存，便於日後的執行和分析。只要在任何電腦網路上執行 MSN Sniffer，就能開始攔截，不需要在監視目標電腦上安裝額外的程式如圖 2。

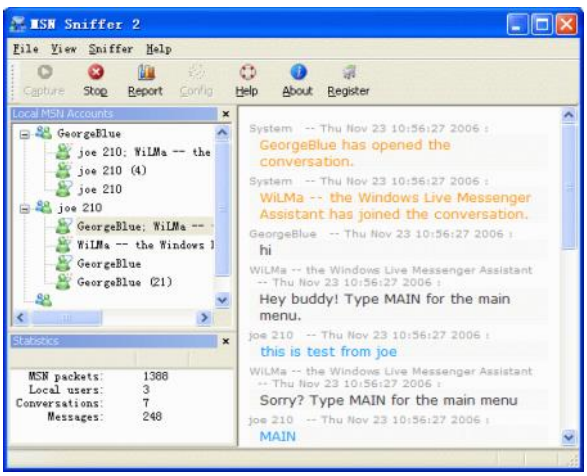

圖 2 MSN Sniffer 系統畫面

2.3 入侵偵測簡介

入侵偵測系統(Intrusion Detection System，IDS)(D.Anderson、T.Frivold、A.Valdes，1995)在網路裡扮演著監控網路中各項活動的警衛，大部分的 IDS 都是以解讀各種封包內容、執行網路流量監測或是分析系統紀錄等方式來找尋可能入侵的行為，並且做出適

當的反應(Dong Seong Kim、 Ha-Nam Nguyen,、Jong SouPark，2005) 、(Joseph S. sheriff'、 Rod Ayers, 2003)。根據這種特性可以發現 IDS 需要一套規則來判定是否該行為已達到入侵的意圖，這些規則就是所謂的特徵(signatures)，符合特徵就可以判定為蓄意的入侵或有攻擊的意圖。若是特徵定得太鬆或者太嚴，都會失去使用的意義，因此，IDS 最重要的部分就是在於特徵的訂定(陳毓璋、李俊毅、高志孝、楊陳俊，2007)。

2.3.1 入侵偵測技術介紹

一. Signature-based detection

類似病毒軟體掃描的方式，將每一個入侵事件事先定義好，並且給予它們識別標誌或序號，當攻擊發生時，系統便可立即發現進而保護系統。其優點是降低攻擊誤判率（false positive rate），因為攻擊手法都是定義完整的，但缺點是若出現尚未定義過的入侵攻擊事件時就無法正確的判定。

二. Anomaly-based detection

事先將正常的操作行為定義成範本（profile），把其他的偏差行為(deviations)當成是入侵事件，並會隨即對正常行為範本做更新。其優點是可偵測出以往從沒發生過的攻擊，缺點則是攻擊誤判率較高，因為使用者的行為模式很難預測。

三. Specification-based detection

是先定義出程式或通訊協定正確運作的限制條件（constraints），並根據這些條件監控程式的執行狀況。此偵測技術不但可偵測出以往從沒發生過的攻擊，同時它也能降低攻擊誤判率。

3. 系統架構與演示

3.1 系統架構

關於 OMS 的防禦蠕蟲攻擊釣魚網站的方法，本研究提出了一些改善的地方，包含 1.安裝較為方便 2.成本降低 3.更新較為迅速 4.可行性高。在文獻資料中我們對於 OMS 的方式發現其系統具有幾項缺失，首先是對於網路釣魚之網站並無法馬上得知進而預防，其次系統並無法監控內部人員是否與外界人員進行連線之內容，因此無法得知是否危及到內部的機器與系統。因此我們提出一個更為安全及便利且因此本研究提一個在實務上可行性高且具低成本的系統，圖 3 為其示意圖。

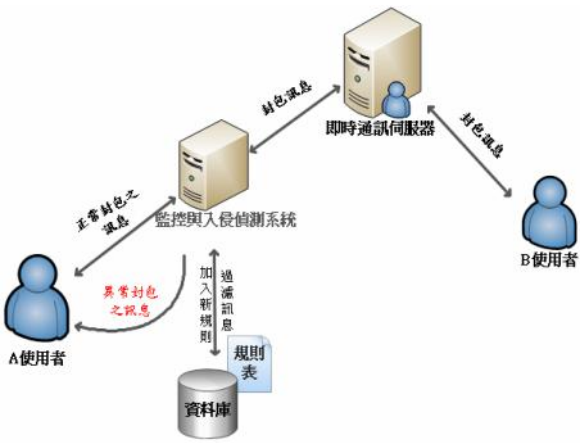

圖 **3** 系統架構

在圖 3 中，A 使用者與 B 使用者之間傳送封包之訊息會透過我們所設立的監控與入侵偵測之系統來檢查 B 使用者所傳送給 A 使用者的訊息是否是異常，當 B 使用者受到蠕蟲的侵入之後傳送有包含網址的的訊息給使用者 A，監控與入侵偵測系統會偵測出封包內有沒有含網址的訊息，如果檢查出有含網址訊息後，會與後方資料庫的規則表下去做比對，規則表內有正常的操作行為定義成範本，把其他的偏差行為當成是攻擊事件，還有把以前攻擊事件的特徵也存入規則表，當然網管人員也能自行把可疑的網站加入規則表中。當有異常之訊息發生時，例如最近常見的即時通訊息攻擊“這張照片好像是你乙 http://www.tw-msn.com/love/index.asp?=hgtht.jpg”，他其實是一個內含病毒的網頁，當 B 使用者傳送給 A 使用者這一類的攻擊時，間控與入侵偵測系統會檢查封包，如有網址的封包便

會跟資料庫裡的規則表做比對，進而通知 A 使用者這個網頁是釣魚網站。如有網頁不在規則表中，網管人員也能透過監控與入侵偵測之系統將此次攻擊方式新增到規則表中，來做為即時通訊上蠕蟲或是病毒...等相同攻擊的防治方法。

3.2 系統演示

在此安全機制中，我使用 MSN Sniffer 做為監控之工具，此監控工具是安裝在圖 3 的監控與入侵偵測系統裡面，一但發現可疑封包便會跟後方資料庫做配合，進行黑名單比對如有問題便會警告這是一個釣魚網頁。圖 4 是在安裝 MSN Sniffer 時的設定過程，圖中我們可以設定對全部內部人員做監視。假設以圖 3 中我們把 A 使用者之 IP 做為鎖定監控來了解她的一舉一動。便可以了解 B 使用者是否傳送了具有異常之資料，來做安全性的防範工作。

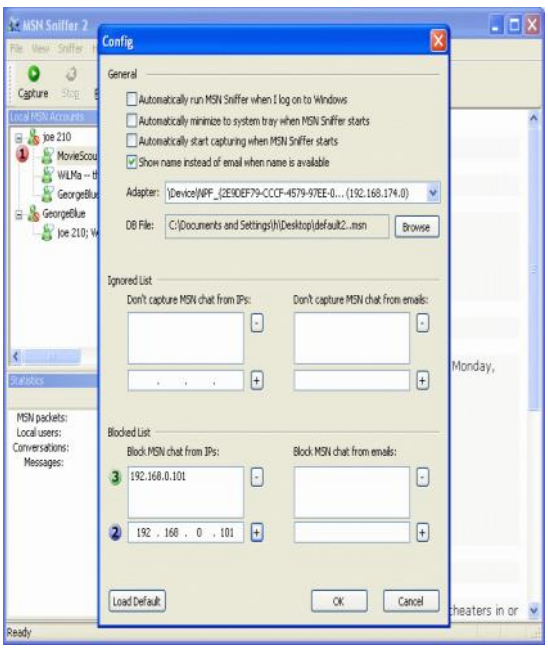

圖 **4** 設定監控工具之方法

圖 5 為本研究中入侵偵測所設定之不合法規則，除了一般常見之項目也可以根據監控系統中所發現的異常封包之特徵如上一小節中所描述之訊息，並且將其訊息之特徵來訂定在規則表之中。如圖 3 監控與入侵偵測系統安裝完 MSN Sniffer 後能夠選取圖 5 的入侵偵測之規則，就能使偵測系統對於選取出的入侵攻擊做防範，可以讓使用者能更方便的設定入侵偵測系統。

圖 **5** 入侵偵測之規則

4. 結論

即時通訊系統仍處於高速發展之中，很可能明天就會湧現出新的安全問題，有新的攻擊手段被設計出來。包括使用者、即時通訊服務提供者及相關廠商全體，都應該以積極的態度去面對這種形勢，並履行自己的職責，以保證即時通訊應用在更健康的狀態下成長。但是不管對企業或個人而言由於 IM 是免費的，卻要企業業主花費大筆金錢來買解決方案確實是滿困難的，但一般人總是在事情發生之後才會去正視問題的嚴重性，出事了以後才知道資安產品的效益。正因為如此本研究主要以監控工具與入侵偵測系統之使用來防預蠕蟲對即時通訊的迫害。本研究改善了之前 **OMS[2]**的點對點蠕蟲防禦方式， OMS 的防禦方式是使用觀測主機以及黑名單的建立，並且跟 DNS 作

配合把有問題的網頁傳到 DNS，使問題網頁無法開啟。我們改善它讓成本能夠讓降低，並且安裝較為方便只需安裝在監控主機上便可阻擋 MSN 上蠕蟲攻擊，不用在跟 DNS 做黑名單的通知，這樣也能使的更新能夠更迅速更安全。

參考文獻

[1] 陳毓璋、李俊毅、高志孝、楊陳俊，2007，「入侵防禦系統設計之研究」，TANET 研討會。

[2] 鄭進興 郭洺坤 程毓明，2008，「點對點蠕蟲防治研究-以即時通訊蠕蟲防治為例」，ICIM 研討會。

[3] D.Anderson, T.Frivold and A.Valdes, “Next-generation Intrusion Detection ExpertSystem(NIDES)”, Technical report,SRI-CSL-95-07, Computer Sience Lab, SRIInternational, 1995.

[4] Dong Seong Kim, Ha-Nam Nguyen, Jong SouPark ,“Genetic Algorithm to Improve SVMBased Network Intrusion Detection System”,Advanced Information Networki ng andApplications, 19th International Conference on, 2005,pp155-158.

[5] Joseph S. sheriff, Rod Ayers, “Intrusiondetection: Methods and system. Part II ” ,Information Management and computer security, 2003,pp222-229.

[6] http://www.effetech.com/msn-sniffer/

[7] http://taiwan.cnet.com/downloads/utility/0,2000071099,20013408s,00.htm

[8] http://www.softking.com.tw/soft/clickcount.asp?fid3=21006

[9] http://net.stuun.com/im/qq/45295.html

[10] http://www.cert.org.tw/document/column/show.php?key=95