新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/8/13- 2007/8/19 第38期

## 網路記錄器 / IR 系列報導

# 技術淺談與應用 - Web IM 的及時監控

隨著科技發展迅速，使用網路來傳遞資料、溝通訊息也越來越便捷，其中最多人使用的溝通管道就是即時通訊（Instant Message，簡稱 IM）。就是因為其安裝簡易、使用方便、不需付費...，所以現今全球已有超過 75% 的網路人口在使用即時通訊來做為傳遞文字訊息、檔案、語音與視訊交流的重要途徑。

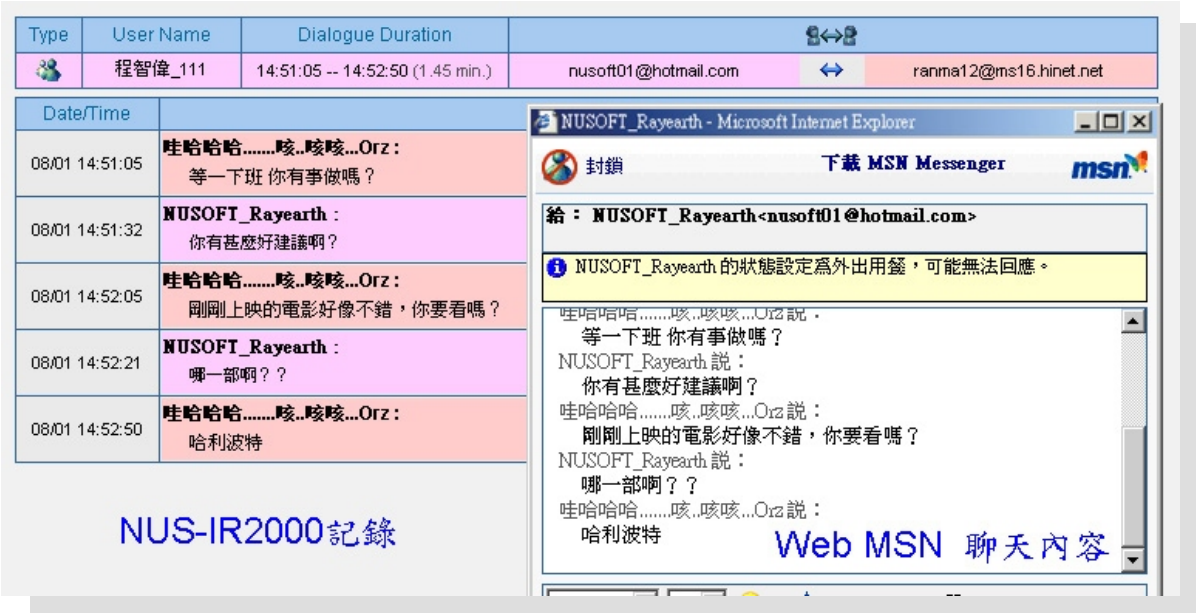
雖然即時通訊使用上如此簡單、又不需要付費使用，對於企業來說應該是行銷、溝通的極佳利器，但往往也成為員工打混摸魚的最佳管道。經由即時通訊傳送文件檔案可能包含病毒、有害程式碼或外洩企業機密，造成企業嚴重的資訊安全風險。就因為即時通訊對企業營運來說像是一把兩面刃；可為企業帶來豐厚商機，亦有降低員工工作效率的潛在問題。因此，有部分的企業開始採用資訊安全設備管制或記錄員工使用即時通訊。

這些資訊安全設備是針對即時通訊軟體的連線特徵（Pattern）來阻擋或是記錄聊天訊息，讓企業可掌握目前常用即時通訊軟體之使用狀況。但正所謂上有政策，下有對策，即時通訊又不是一定要安裝軟體方能使用－目前各家即時通訊廠商相繼推出了 Web IM（Web Instant Messenger），可以讓使用者透過 Web 介面，使用諸如 MSN、Yahoo...即時通訊服務。Web IM 是採用 HTTP 之方式連接至 Web IM 網頁，因而導致一般資訊安全設備無法正常阻擋或是記錄，造成即時通訊管理上的嚴重漏洞。

有鑑於此，新軟系統在其網路記錄器－IR 系列中，加入了 Web IM 分析引擎。透過引擎的分析，IR 系統可明確分辨出哪些 HTTP 連線屬於網頁瀏覽、哪些連線屬於Web IM 聊天，再經由 IR 系統內建的記錄分析、行為管理兩大功能做以下之動作（以 NUS-IR2000 為例）：

記錄分析－ NUS-IR2000 目前可記錄 MSN 官方的 Web IM 聊天內容。當系統擷取到 Web IM 的聊天連線時，NUS-IR2000 內建的記錄分析功能會先以使用者為記錄之依據，並詳細記錄聊天雙方的帳號、暱稱、聊天時間、聊天內容...重要資訊。管理人員可清楚得知員工於上班時間如何使用Web IM，亦可藉此記錄做為日後評鑑考績之依據。（如圖一）

行為管理－ NUS-IR2000 可阻擋員工使用 Web IM，讓公司員工無法連結至其服務網頁。如此一來，員工僅無法連線至 Web IM，但仍可以正常上網。




圖一 可清楚記錄 Web MSN 聊天內容

| | 新軟網路記錄器 | 一般市售網路側錄設備 |
|---|---|---|
| IM | 可阻擋與記錄聊天內容 | 可阻擋與記錄聊天內容 |
| Web IM | 可記錄 Web IM<br>MSN Web Messenger（官方）<br><br>可阻擋 Web IM<br>Buddy. com　Imunitive<br>I Love IM　Wablet<br>Meebo　Gooway<br>IM haha　MSN2go<br>Kool IM　Totmomo<br>messengerFX　Mobile<br>communi　webQQ<br>Mabber | 不可記錄資料，甚至無法阻擋 |

表一 新軟網路記錄器與一般市售網路側錄設備之比較表

文 卓冠倫 aaron@nusoft.com.tw

## 市場行銷報導 - 如何有效利用網路記錄器的硬碟容量

在企業大量使用網路傳輸訊息的同時，為了對這些往來的資料把關，市面上出現了許多網路側錄相關產品。這些產品可記錄所有員工的網路行為，但所記錄之資料卻往往都缺乏系統歸類或過於草率。導致獲得的只是一堆龐大卻難以調閱之資訊，並無法針對記錄特性有效分配儲存空間。

有鑑於此，新軟網路記錄器於研發之初即採用深入擷取、過濾、分析、歸納封包的方式，發展出獨特之資料探勘技術。管理人員可針對記錄資料內容做全方位檢索，即時調閱所需資料。然而，為了詳細記錄資訊來支援“調閱資料的便利性”，新軟網路記錄器勢必需要建置龐大的記錄分類資料庫。

此時，有人不禁會問，新軟網記錄器內建硬碟的儲存空間，總有使用完畢的時候，難道此時側錄動作就此停擺？為了避免此情形的發生，在新軟網路記錄器中，管理人員可依企業需求調整各種記錄（SMTP、POP3、HTTP、IM、Web SMTP、Web POP3、FTP、TELNET）的保存期限（一般企業會優先保存郵件記錄）。新軟網路記錄器會利用管理人員所設定的保存期限與該服務的實際流量估算各項網路服務之儲存空間值，有效分配各類記錄於其內建硬碟中的使用率。

新軟網路記錄器除了使用保存期限方式來確保硬碟之空間外，同時也採用了儲存空間臨界值預防機制。當新軟網路記錄器的記錄資料，達到設定的保存期限時，即會將其立即清除；若是在資料保存期滿前，儲存空間就已飽和，新軟網路記錄器會依照儲存資料的歷史排序，從目前保留最久的記錄開始刪除的動作，騰出一定比例的空間，以維持後續側錄動作。

所以，當企業網路環境中，配置了新軟網路記錄器。在運作一段時間後，即可依照其所計算出來的每日平均流量，和儲存資料的重要性，設定記錄保存的期限，以制定彈性的空間使用率。

為了因應企業在各法規的實行下，要長時間保留所有往來資料以供查閱的需求；同時防止用戶端郵件遺失或誤刪的情形，則可應用新軟網路記錄器內建的遠端備份機制，將記錄資料備份至遠端的 NAS、File Server. . .，來確保重要記錄可長期保存。

文 程智偉 rayearth@nusoft.com.tw