Openfind™ Software Engineered for Growth™

Email Threats Analysis Report

Q4 2013

2013 第四季 Openfind 郵件威脅分析報告

目錄

一、全球垃圾信發送來源地區

2013 第四季垃圾信來源國家的前三名分別為中國、日本與美國，依序佔整體垃圾信的 53.8%、12.6%與 5.8%。延續上一季前三名寶座的順位，而在上季與美國並列第三的台灣，雖然本季跟美國相差了 1.6%位居第四名的位置，但美國跟台灣都分別提高了 1.9%跟 0.3%，有著比重上升的趨勢。而佔比重上升最明顯的地區，即是本季佔比超過一半的中國(53.8%)，比前一季提升了 19.4%之多！

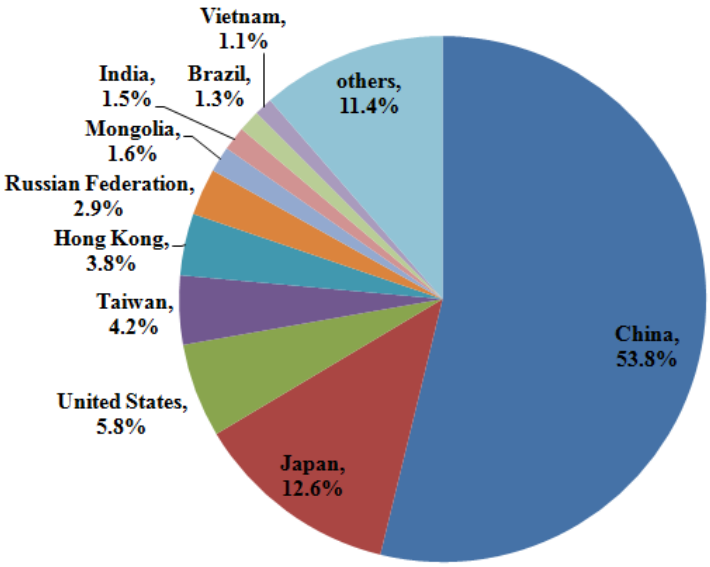

圖 1.2013 年第四季垃圾信來源國家分布

細部觀察 10 月、11 月及 12 月來源比例，可發現中國的垃圾信件量大約都佔整體比重的一半左右，而日本的垃圾信件量有逐漸下降的趨勢，到 12 月時已由原本的 17.3%降至 10.3%。中國垃圾信件量相較於前幾季，有大幅提高的趨勢，且主要是以商業類別的廣告信居多。

表 1.2013 年第四季垃圾信來源國家比例

國家	10 月	11 月	12 月	季平均	季排名
中國	49.5%	56.1%	55.1%	53.8%	1
日本	17.3%	10.9%	10.3%	12.6%	2
美國	5.1%	3.6%	9.1%	5.8%	3
台灣	4.4%	4.2%	4.1%	4.2%	4
香港	4.5%	4.8%	1.9%	3.8%	5
俄羅斯	2.5%	3.3%	2.7%	2.9%	6
孟加拉	0.8%	1.5%	2.5%	1.6%	7
印度	1.6%	1.6%	1.2%	1.5%	8
巴西	1.7%	1.2%	1.1%	1.3%	9
越南	1.1%	1.4%	0.7%	1.1%	10
其他	11.3%	11.5%	11.3%	11.4%	

台灣目前在本季排名位居第四，垃圾郵件來源比例不低，穩定維持在 4%的水平，且相較於前一季有提高的趨勢，值得重視。過去一季，美國與台灣的垃圾郵件來源每月比重的差距穩定，皆在 1.5%以內。但是在本季 12 月時，美國的比重明顯上升，與台灣有 5%的顯著差距，推測可能是 12 月的聖誕節慶或是適逢過年，來到了美國的商業活動最頻繁的月份。Openfind 電子郵件威脅實驗室會持續觀察與監控全球各國垃圾郵件發布狀況，掌握威脅趨勢，透過雲端防護技術，第一時間有效讓 MailGates 的用戶免除垃圾郵件困擾。

二、URL 內容分類解析

Openfind 電子郵件威脅實驗室與鴻璟科技共同合作，深入觀察垃圾郵件內含之 URL 網頁內容，並將網頁進行分類，下表為本季網頁內容分類狀況。最多的網頁主題為商業相關類別，顯示約有 4 分之 1 的垃圾郵件網址會導引收件人前往商業相關網頁。

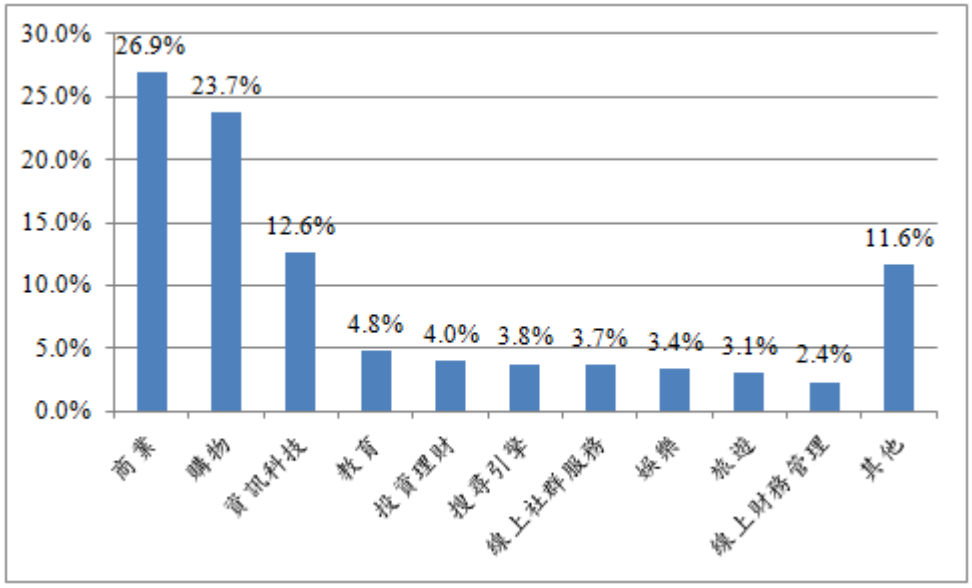

圖 2.2013 年第四季垃圾信 URL 網頁內容分類

本季前三名依舊為商業、購物與資訊科技，且垃圾信 URL 種類與上一季完全相同，順序稍作改變而已。前十名的類別中，多數與金流相關，包含：商業、購物、投資理財、以及線上財務管理。值得注意的是，線上社群服務從上一季的第五名退到本季第七名的位置，不過在比重上只退了 2%。而排名較前的資訊科技、教育、投資理財則都微幅上升。

表 2.2013 年第三季與第四季 URL 網頁內容分類比較

第三季			第四季	
排名	類別	比例	類別	比例
1	商業	27.2%	商業	26.9%
2	購物	24.4%	購物	23.7%
3	資訊科技	11.9%	資訊科技	12.6%
4	教育	4.4%	教育	4.8%
5	線上社群服務	3.9%	投資理財	4.0%
6	投資理財	3.9%	搜尋引擎	3.8%
7	搜尋引擎	3.4%	線上社群服務	3.7%
8	娛樂	3.4%	娛樂	3.4%
9	旅遊	2.7%	旅遊	3.1%
10	線上財務管理	2.3%	線上財務管理	2.4%

觀察第三季與第四季 URL 網頁內容，可發現兩季前十大排名主題完全相同，只有線上社群服務的比重稍降，顯示部分線上社群服務的熱潮有稍退的跡象，建議持續於下季關注確認是否有逐步退燒的趨勢。近期若要著手處理垃圾郵件防護過濾困擾時，仍建議先從商業、購物及資訊科技相關議題進行處理，設定特殊關鍵字或進行相關樣本訓練，可有效預防大多數垃圾郵件問題。Openfind 電子郵件威脅實驗室將持續研究垃圾郵件網頁分類趨勢，以期達成對症下藥，有效屏除垃圾郵件所帶來的種種威脅。

三、垃圾信發布模式觀察

延續以往一貫的垃圾信散布趨勢，轉址服務仍為主要手法，其他相關模式說明如下：

1. **巧用「填表免費送」或「拒收請按此」名目，藉以獲得可用信箱**
   點擊垃圾郵件內藏之連結開啟該廣告網頁後，常可見填寫表格後的行銷優惠活動，吸引收信者填個人資料。此外有些還會附上「拒收請按此」等類似文字的超連結，再請收信者填入電子郵件地址，這些都是常見的獲取使用者信箱的手法。當遇到類似情況時，建議使用者不要填取任何資料，直接關掉頁面以保安全。

2. **行動裝置上的郵件閱讀習慣帶領垃圾郵件益趨手機化**
   隨著智慧型手機的快速發展，對於日常事務繁忙、常有舟車勞頓或出外洽公頻繁的忙碌現代人來說，他們已逐漸養成於行動裝置閱讀郵件的收信習慣。因應此趨勢，有部分垃圾信所夾帶的網址，會導向狹長型的網頁，如.mobi 等網域，便於在手機等裝置進行閱讀。

3. **面對陌生網頁，請先測試，無誤後再登入**
   垃圾郵件所導入的網頁連結，乍看之下，您覺得可信度很高但又不確定是否安全時，強烈建議使用者不要點取。若因為種種原因還是想試著登入看看時，可以先利用假的帳號密碼登入，確認是否有異狀，如：網頁正常啟動、或按下提交按鈕後導入如您預期的網頁等，初步降低可能的風險，但請注意這個步驟還是有風險存在！陌生網頁，建議不填入真實帳密以防資訊外洩！

四、垃圾信樣本詳細說明

以下我們將介紹並說明本季中收集到常見的釣魚信件案例，以及台灣地區、中國地區和日本地區等具代表性的垃圾信樣本。

● 常見釣魚信件

以往常見的釣魚信件，大多都是仿造銀行通知信、電子郵件通知信及社群網站訊息等各式通知信，等使用者依信中超連結連到釣魚頁面後，再盜取使用者的帳密，如下圖便是常見的釣魚信件之一：

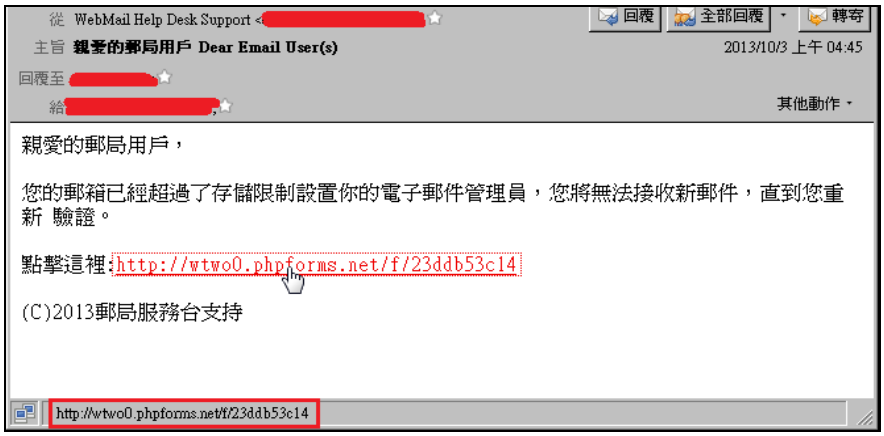

圖 3.語法不順的網頁郵件服務釣魚信範例

從邏輯不通且語法不順的信件內文，再加上無法正常辨識的超連結來判斷，可見此釣魚信件的發信者應不諳中文，甚至有可能是透過翻譯軟體翻出的中文，這點也是此類釣魚信件的特色之一。

我們嘗試點擊超連結，前往該網頁時，發現其連結已失效了，回傳的結果是 404，找不到頁面：

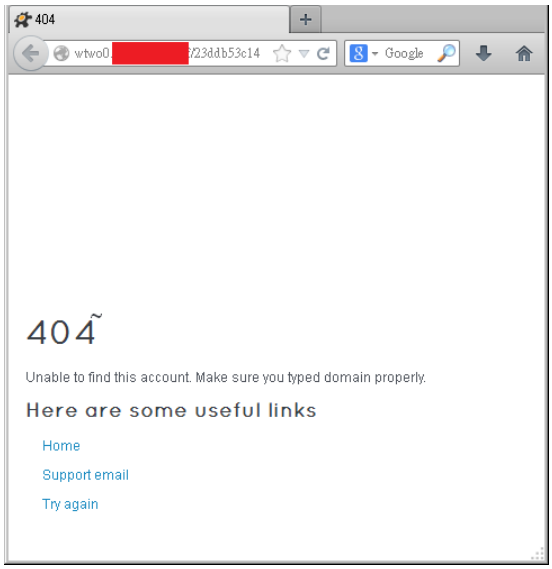

圖 4.釣魚信連結所引導至的無效網頁

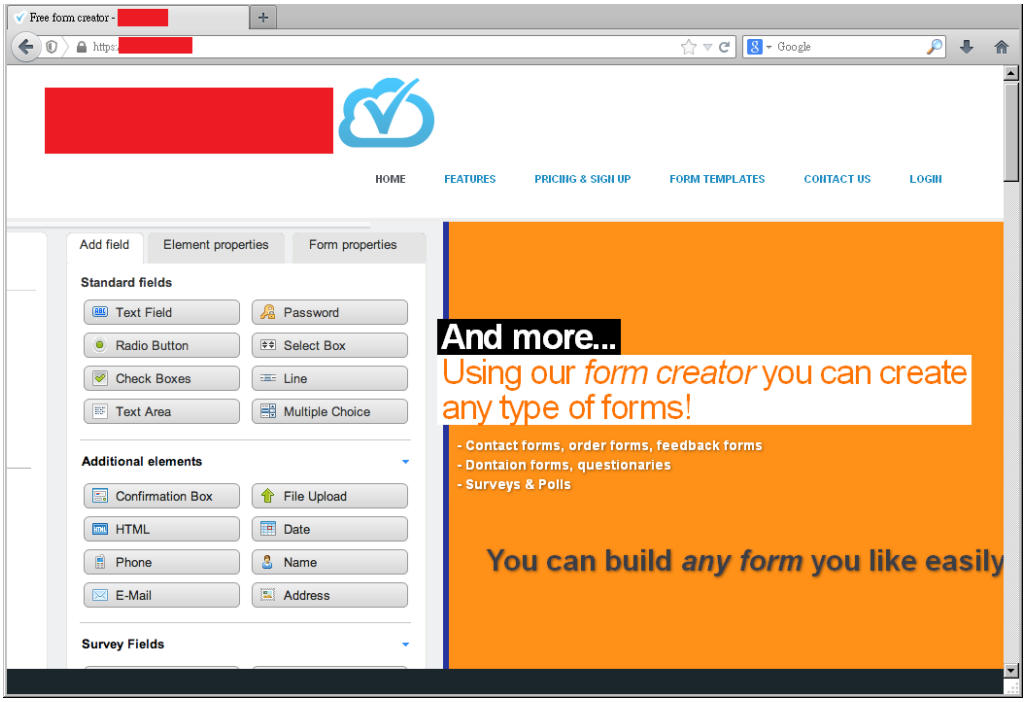

圖 5.網頁郵件服務釣魚信超連結的主網域網頁

接著再嘗試前往該超連結的主網域頁面，發現是一個正常的網站（phpforms.net），此網站專門提供線上表單服務，有免費的基本功能，也有付費的進階功能，猜想應該是由於該釣魚網頁被 PHPForms 查獲，進而被刪除才找不到網頁，或是已經達成釣魚目的而刪除。雖然此一類提供線上表單的網站會定期清除釣魚頁面，但釣魚信發送者仍不時利用這些網站作網頁，屢試不爽，可見免費的頁面站台仍舊是很好利用的工具。

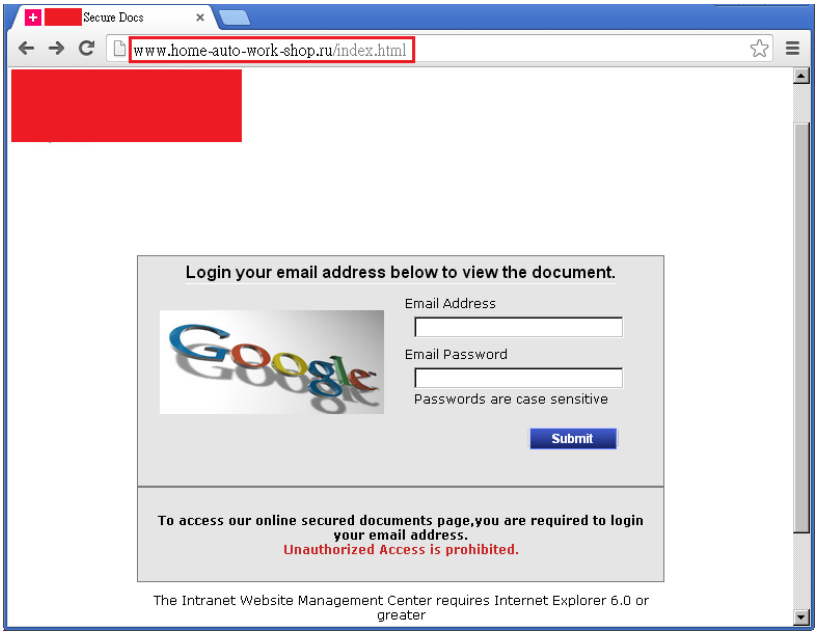

圖 6.使用新域名的釣魚網頁

如上圖，除了利用免費的頁面站台，部份釣魚信發送者會買或租網域來當作釣魚頁面的網域，但是此方法較花錢，因此也相對少見；最常見的還是駭入別的正常的網站(通常是小型網站)，將該網站空間當作自己的釣魚頁面的存放處，不用花錢租網域，也可降低被網路警察查緝的機率。如下例：

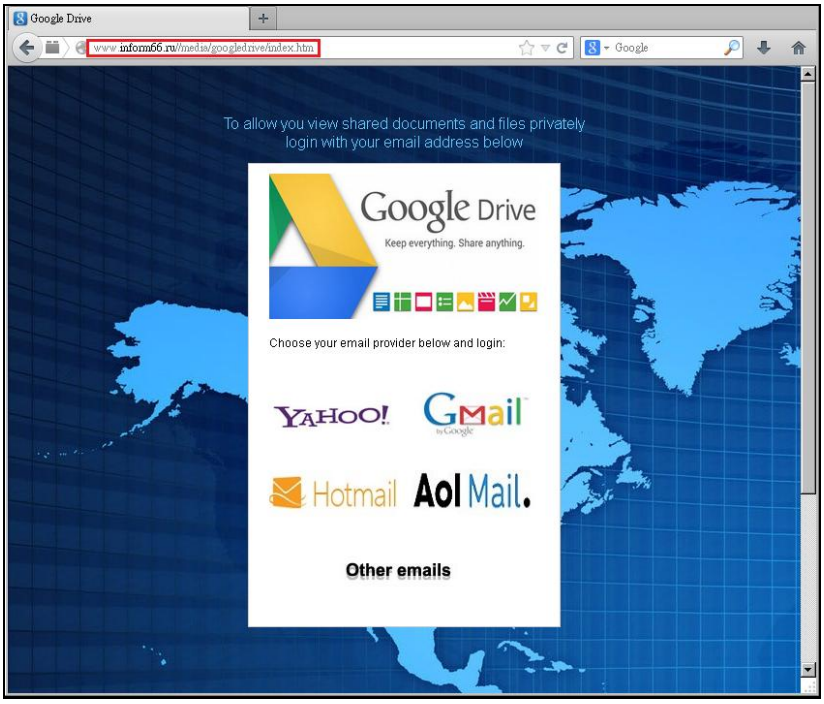

圖 7.利用被駭網站的釣魚網頁

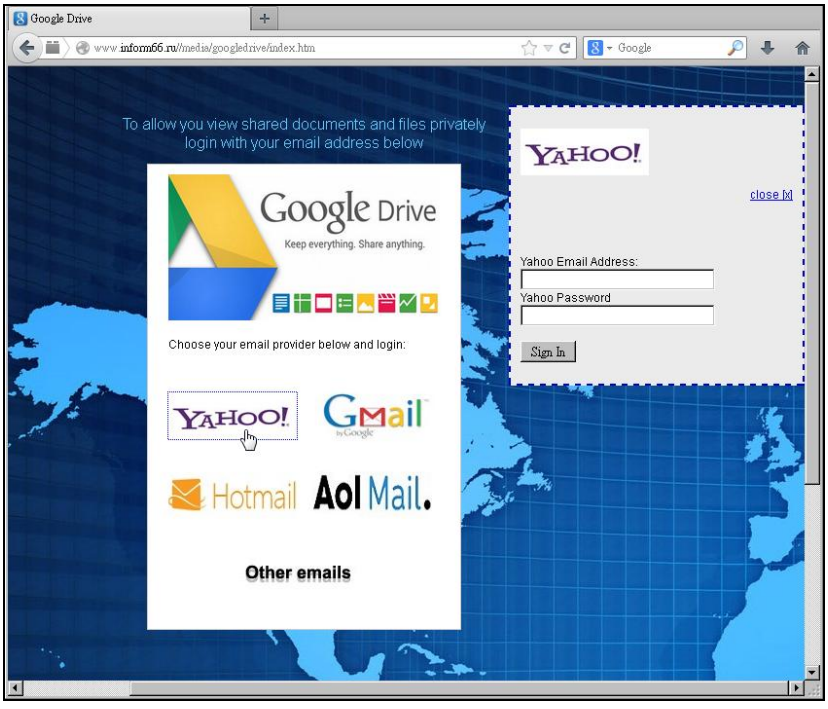

圖 8.選用其他釣魚網路服務

在此例中，釣魚信發送者駭入一網站，並在網站下新增自己的資料夾及釣魚網頁，基本上若是網站管理員沒發現的話，這個釣魚頁面便可一直放下去。

進入頁面後，如圖所示，在上方標明是某知名網路公司 Drive，也就是某知名網路公司的網路硬碟，但是下方卻有多種網頁郵件服務可選，可能是為了多吸引被害者而設。接著用另一知名網路公司的帳號密碼測試看看：

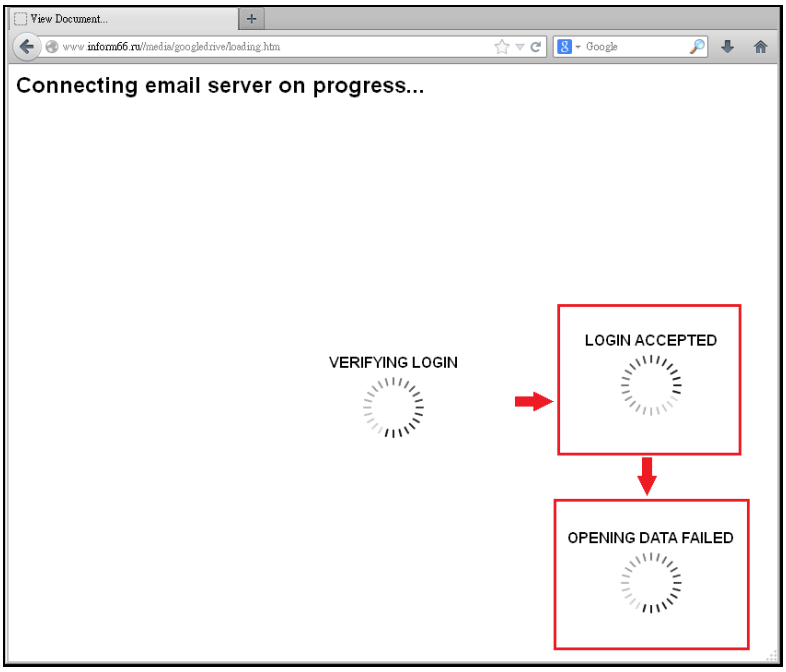

圖 9.利用知名網路公司帳號密碼登入畫面

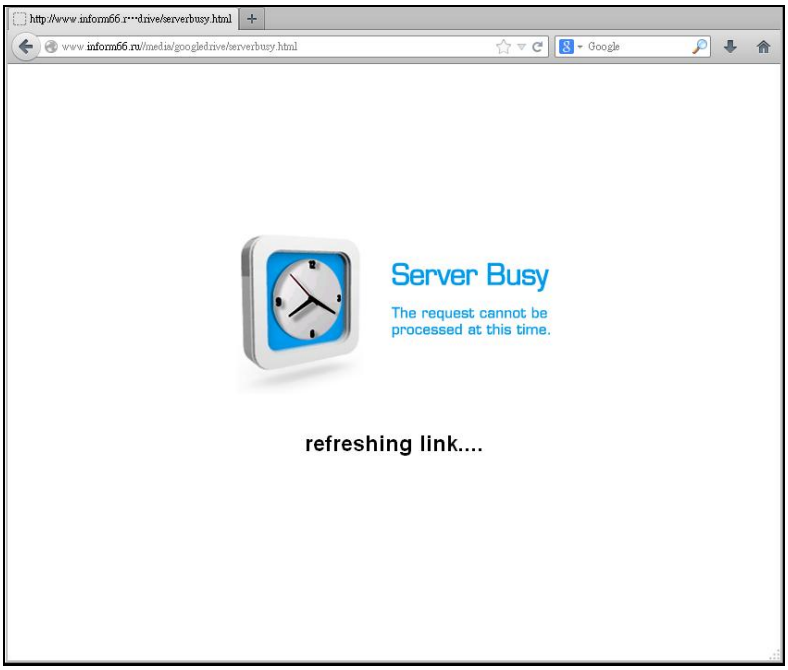

圖 10.登入後的最後產生畫面–網頁無法正常顯示

鍵入帳號密碼並登入後，先是顯示登入訊息，接著是讀取資料的訊息，但卻是讀取資料錯誤，最後秀出伺服器忙錄的資訊，並再轉址到另外一個和原先不同的登入頁面，此時才是真正的某知名網路公司雲端硬碟登入頁面。

圖 11.真正的某知名網路公司登入畫面

從一開始的假造登入頁面，到讀取錯誤訊息，最後再到真正的登入頁面，這一連串的動作正好是其中一種典型的釣魚頁面會有的動作，檢查其中的流程，大略是：

http://www.inform66.ru//media/googledrive/index.htm(假造登入頁面)轉址到

http://www.inform66.ru//media/googledrive/loading.htm(錯誤訊息頁面)轉址到

http://www.inform66.ru//media/googledrive/serverbusy.html(伺服器忙碌頁面)轉址到

http://drive.google.com/(某知名網路公司雲端硬碟頁面)轉址到

https://accounts.google.com/ServiceLogin?service=wise&passive=1209600&continue=https%3A%2F%2Fdrive.google.com%2F%23&followup=https%3A%2F%2Fdrive.google.com%2F&ltmpl=drive

在其中的錯誤訊息頁面的網頁原始碼，發現了像是台詞似的幾個訊息：

```
...
splashmessage[2]='PROCESSINGDOC'
splashmessage[3]='...FINALIZINGDOCUMENTVIEW...'
splashmessage[4]='SERVERTOOBUSY!!!'
splashmessage[5]='ERRORPROCESSINGFILES!!!'
...
```

而伺服器忙錄頁面的網頁原始碼，也只有短短的幾行：

```
<br><br><br><br><br><br><br><br>
<center><imgsrc="index_files/sb.jpg"><br>
<h2>refreshinglink....
<metaHTTP-EQUIV="REFRESH"content="3;url=http://drive.google.com
">
```

僅僅秀出圖片，以及轉址到其他網址的作用。

這類的釣魚信件雖然多，但是破綻也不少，建議使用者當收到類似的可疑信件時，馬上刪除比較好，若還是想試著登入看看，也可先用假的帳號密碼來測試是否有問題，以免自己的真實的帳密被盜取走而不知。

● 台灣常見垃圾信

基本上通常各地區常見的垃圾信，信中廣告的商品、店家等都和本地較相關，但台灣由於和香港、中國地理位置相近，語言、文字也通，所以在台灣也時常會收集到香港、中國等地的垃圾信，下圖例是其中是較有趣的例子：

圖 12.網址結尾為.tw 的枕頭廣告信

圖 13.枕頭廣告信點擊後畫面

打開此信以及打開該網站超連結後觀察了一下，發現網址雖然是.tw，但公司所在地址及電話是香港的，而連絡人電子郵件則是中國的網域，兩岸三地的資訊都有，可見雖然只是普通廣告信，但由於語言、相通，又有網路之便，廣告信的流通也是擴展得相當迅速。

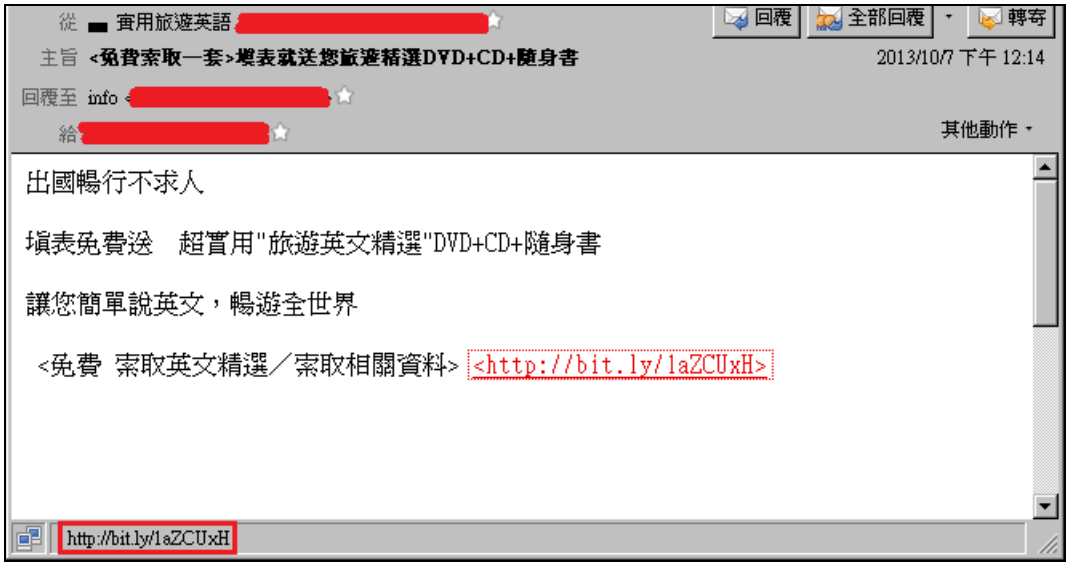

圖 14.英文課程廣告信

如上圖，在五花八門的廣告信中，除了一般物品廣告信、商務課程廣告信之外，也出現了英文課程廣告信：

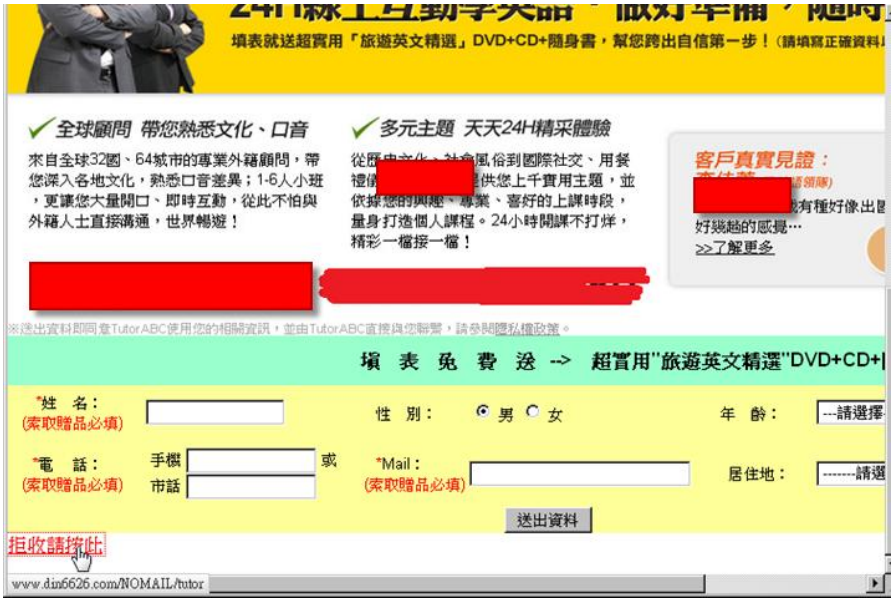

圖 15.英文課程廣告信點擊後畫面

觀察一下廣告信本身，發現和大部分廣告信一樣，完全沒有和廣告主本身有關的資訊，另外也使用第三方的短網址服務來隱藏目標廣告頁面的網址；而連到廣告頁面後，除了有個「填表免費送」的表格，吸引收信者填個人資料之外，還附有「拒收請按此」的超連結，可供收信者填電子郵件位址：

圖 16.提供收信者填入電子郵件位址畫面

雖然有拒收廣告的連結，但須注意的是它不一定有用，反而可能告知了廣告信發送者這個電子郵件位址的確有人在使用，而且也會看廣告，因此若使用者收到類似的廣告信件，建議使用者可直接刪除，避免透露更多自己的資訊給廣告信業者收集。

隨著最近中國小米機的熱潮，台灣也出現了小米機的廣告信件：

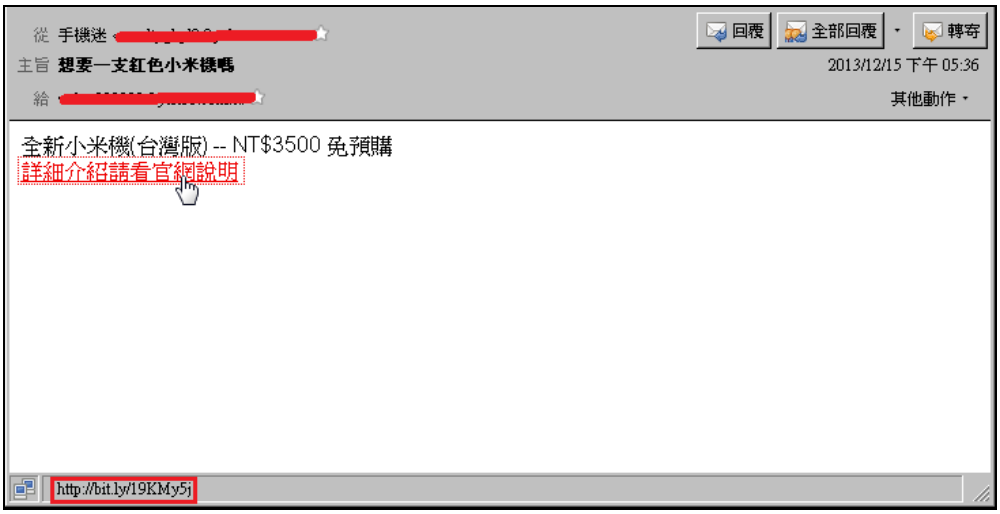

圖 17.小米機廣告信

圖 18.小米機廣告信點擊後畫面

觀察廣告信本身，同樣是常見的廣告信形式，內文簡陋，使用第三方短網址服務等，較不同的是，短網址直接連到了廣告主的購物網站頁面，不像前例是連到廣告信業者的單一廣告頁面，而收信者連到購物網站頁面後，可能較易受到吸引，不只瀏覽該商品，也會逛該購物網站其它商品頁面，此種手法對廣告信業者和廣告主效益較高，也很常見於各種廣告信。

● **中國常見垃圾信**

在中國的簡體中文廣告信方面，本季中收集到了某銀行小額借貸的廣告信：

圖 19.簡體中文金融借貸廣告信

圖 20.主網域為 360doo.com 的簡體中文金融借貸廣告頁面

此廣告信的內容作的和一般 EDM 一樣，連到超連結後看起來則是申請表格的頁面，但值得注意的是，該廣告頁面的網址和這家廣告主主要的網域不同：

圖 21.主網域為 pingan.com 的簡體中文金融借貸廣告頁面

一個主網域是 360doo.com，一個則是 pingan.com，基本上沒有關連，因此猜想此廣告信可能是該銀行的廣告信，但也有可能是釣魚信，為保安全，建議使用者若有需要，最好仍是從該銀行的主網站連網頁最保險。

● 日本常見垃圾信

日文廣告信方面，廣告主題仍以成人約會為大宗，接著是免費優惠詐騙信、博弈類廣告信或賽馬廣告信等，不過較特殊的是，由於日本人普遍使用手機收發信件，其廣告網頁也常是使用手機的格式來顯示，如下這一封優惠活動廣告信：

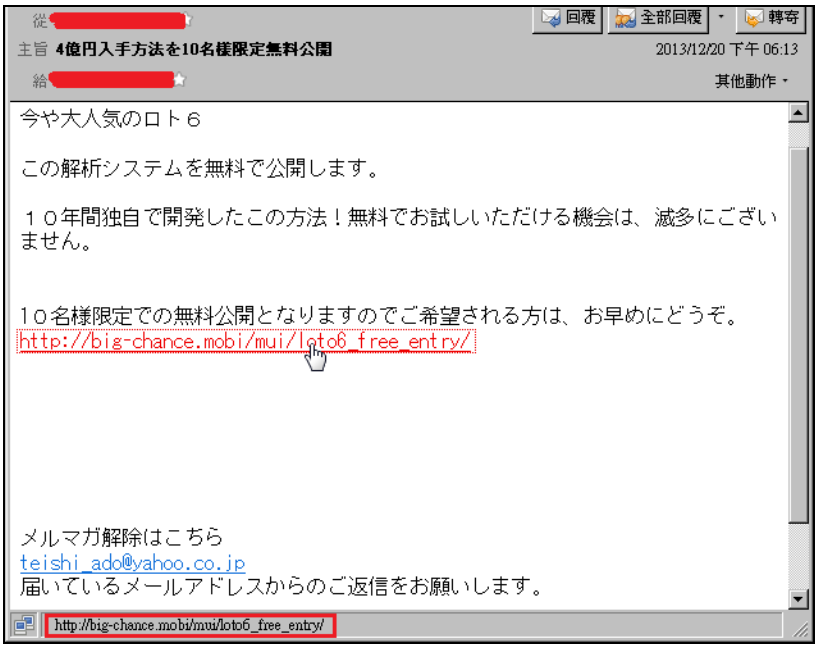

圖 22.日文限定優惠活動廣告信

圖 23.日文限定優惠活動廣告信點擊後畫面

原廣告信內容看起來和一般常見的廣告信無異，但超連結的網址則是使用.mobi 網域，表示是用於手機的網頁，實際連結後發現其網頁格式果然是長條狀的樣式，方便手機顯示。

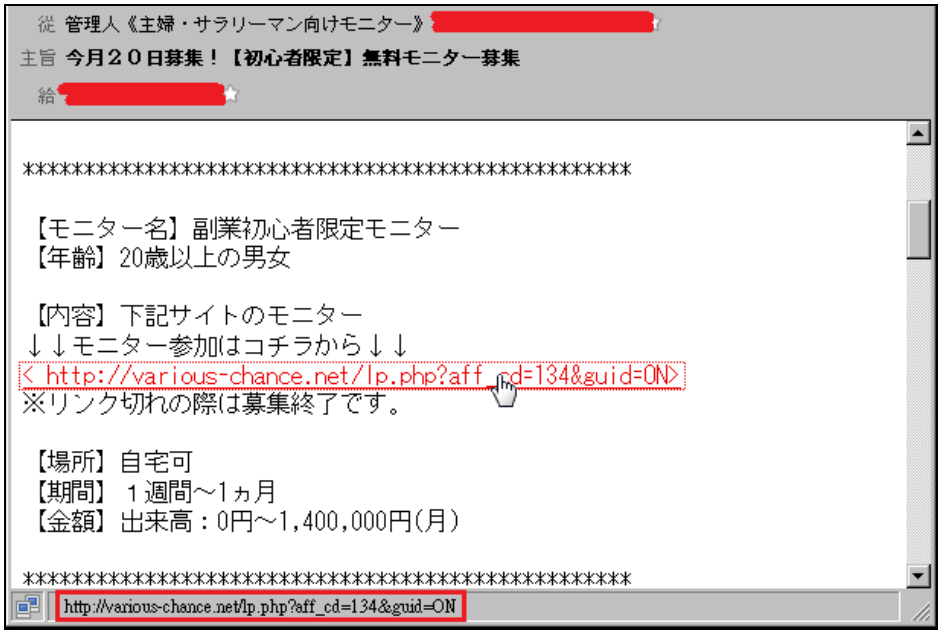

圖 24.日文副業廣告信

圖 25.日文副業廣告頁面點擊後畫面

除了限定活動廣告信之外，本季還收集到了如上圖的副業廣告信，這類的副業廣告信相對於成人、賭博類廣告信上數量較少，較難收集到。在此例中，其超連結並未作轉址處理，可直接連結，連結後觀

察網頁內容，看起來也只是普通網頁，似乎沒有資安上的疑慮；但要注意的是，它雖然是副業廣告，也有可能是詐騙，加入活動前要先交保證金、學費之類的，建議使用者看到同類型的廣告，最好小心為上，以免受騙上當。

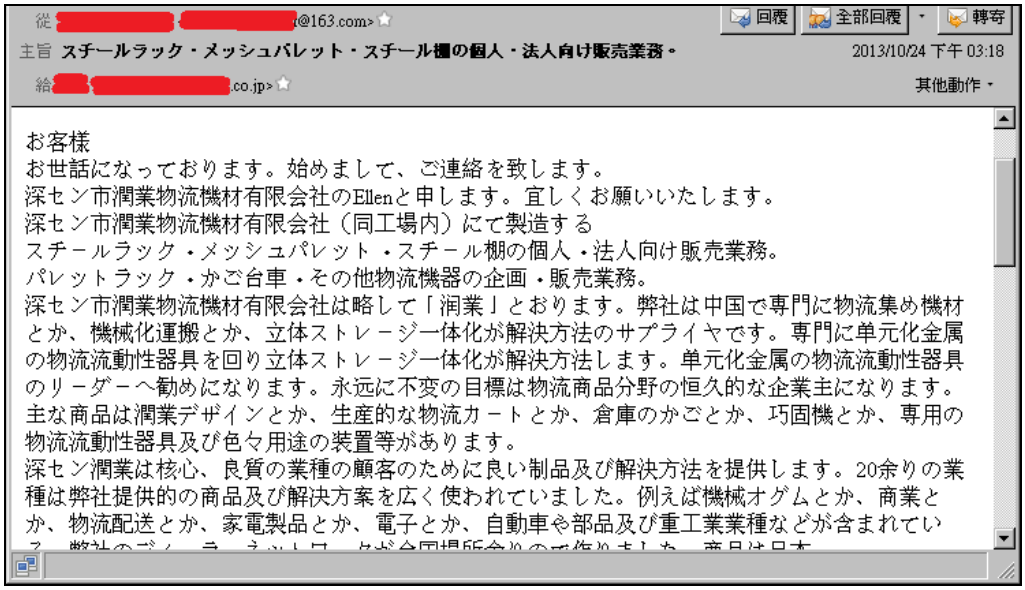

圖 26.中國寄到日本的 B2B 廣告信內容

圖 27.B2B 廣告信來源及其他資訊

如上圖，為 B2B 的商業廣告信，但可注意到它是從中國寄到日本的跨地區的廣告信，是以往相當少見的例子；而除了 B2B 商業廣告信之外，也有一般廣告信，如下圖例的知名網路店家的 EDM 廣告信和商業課程信：

圖 28.中國寄到日本的 EDM 廣告信

圖 29.知名網路店家的 EDM 廣告信

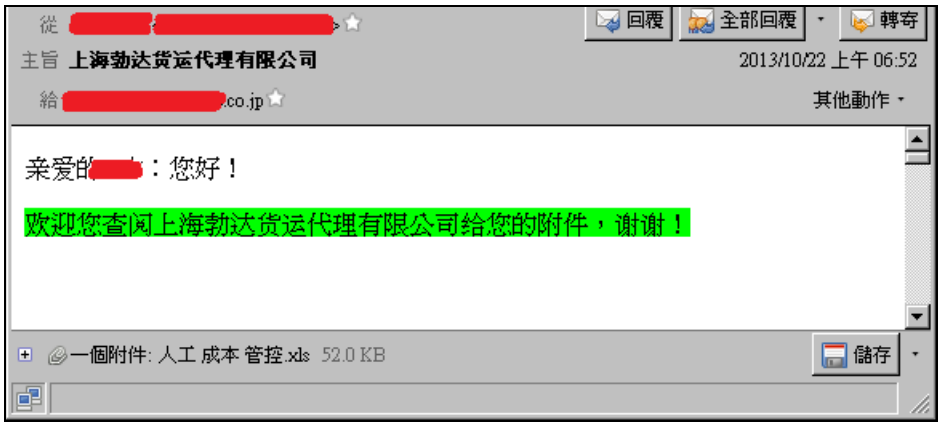

圖 30.中國寄到日本的商業課程廣告信

如圖所示，內容為普通的 EDM 廣告信和商業課程廣告信，特別之處在於收信者不是中文使用者而已，猜想可能是垃圾信發送者用網路爬蟲，在網路上蒐集可用的郵件位址之後，沒有過濾乾淨就直接發送，否則這一類的普通廣告信和 B2B 商業廣告信相比，寄送給非同語言使用者，效益極為有限。另外一種想法是，中國市場實力雄厚且逐漸擴大版圖，看準世界各地皆可能有懂中文的人士，寄送簡體中文編輯而成的廣告信，其實也有機會深入許多日本企業。

Openfind 電子郵件威脅實驗室，特別從 2013 年第四季的電子郵件威脅監控行動中，挑選出這些值得您一覽的電子郵件威脅樣本供您參考，同時這些類型郵件都已經透過 Openfind 的雲端防護攔截技術，在發現威脅的下一秒，即已全面部署至 MailGates 郵件防護系統，以零時差、立即生效的特性，協助全球客戶立即免除以上郵件威脅。

關於 MailGates 郵件防護系統

MailGates 郵件防護系統提供即時完整的郵件安全服務，充分掌握電子郵件相關之各項攻擊與威脅行為，提供內嵌式防毒功能，自動偵測並過濾各式垃圾郵件，有效解惱人的網路攻擊與郵件資安問題，為用戶提供完善郵件防護。具備雙核心雲端防護過濾引擎，以在地化樣本觀察與全球即時探測的零時差防禦技術，全方位掌握垃圾郵件特徵。結合垃圾郵件攔截、企業郵件系統防護、收發紀錄檢視及統計報表發送等多項貼心功能，並率先同業支援 IPv6，全面提升產品相容性。MailGates 郵件防護系統將持續鑽研郵件資安領域，協助企業打造最安全、順暢、可靠的郵件溝通管道。

更多產品訊息，請瀏覽產品網頁 http://www.openfind.com/taiwan/products/mailgates/info.html

Openfind 全產品率先支援 IPv6

隨著全球 43 億個 IPv4 位址即將耗盡，啟用 IPv6 也正式進入倒數計時。為達成網際網路 IPv6 全面化的理想目標，以加速因應雲端科技所帶動的網路成長需求，Openfind 網擎資訊各產品-Mail2000/MailBase/MailGates/MailAudit/OES，已全面完成測試，正式率先支援 IPv6，大幅提升網路環境相容性。

更多訊息，請瀏覽 Openfind 最新消息

http://www.openfind.com/taiwan/newsevents/news_detail.php?news_id=2429

關於 Openfind

Openfind 成立於 1998 年 1 月，長期致力於網際網路相關技術研發，為企業用戶與廣大網友提供高品質、高穩定與高擴充性的軟體與服務。從企業市場搜尋引擎系列產品、電子郵件伺服器或郵件防護、稽核、歸檔系統，到一般使用者的電子郵件信箱與企業郵件代管服務，Openfind 堅守「創新技術與優質服務」的企業文化，以提供使用者最符合成本效益的解決方案。

更多訊息，請瀏覽公司網站 http://www.openfind.com/。

關於鴻璟科技

鴻璟科技成立於 2003 年，為一家創新網路安全方案的全球供應商。鴻璟科技開發資安晶片、資安軟體以及特徵碼資料庫服務，協助客戶如網路服務供應商、網路設備製造商、晶片設計商於新世代防火牆、統一防禦系統(UTM)、電信服務商之家用閘道器、以及行動裝置產品中提供完善並且垂直整合的資安服務。鴻璟科技的技術包含第七層深度網路封包偵測晶片與授權、資安軟體與內容偵測軟體、及包含防病毒、入侵偵測、應用程式與裝置控管、可疑網址與網頁網址分類的特徵碼資料庫系統，所創新研發的技術，可協助客戶抵禦日益嚴重以及巨量暴增的資安威脅和攻擊。

更多訊息，請瀏覽公司網站：http://www.lionic.com