Openfind™ Software Engineered for Growth™

Email Threats Analysis Report

Q2 2013

2013 第二季 Openfind 郵件威脅分析報告

目 錄

一、全球垃圾信發送來源地區 3
二、 URL 內容分類解析 4
三、垃圾信發布模式觀察 5
四、垃圾信樣本詳細說明 6
- 台灣常見垃圾信發送模式 6
- 中國常見垃圾信發送模式 12
- 日本常見垃圾信發送模式 15

一、全球垃圾信發送來源地區

垃圾信來源國家的前三名分別為日本、中國與澳洲，依序佔整體垃圾信的 29.5 % 、27.2% 與 8.2%。由此可見，不同於上一季的前三名(中國、澳洲、日本)，日本超越中國，成為全球主要垃圾郵件來源。第二名中國也僅差第一名日本 2.3%，光這兩個國家就占了 56.7%，是全球垃圾信主要來源。其後 8 個國家的垃圾信件量加起來剛好約跟中國一樣，可見垃圾信有集中的趨勢。

台灣地區占 3.4%，本季排名第 6。

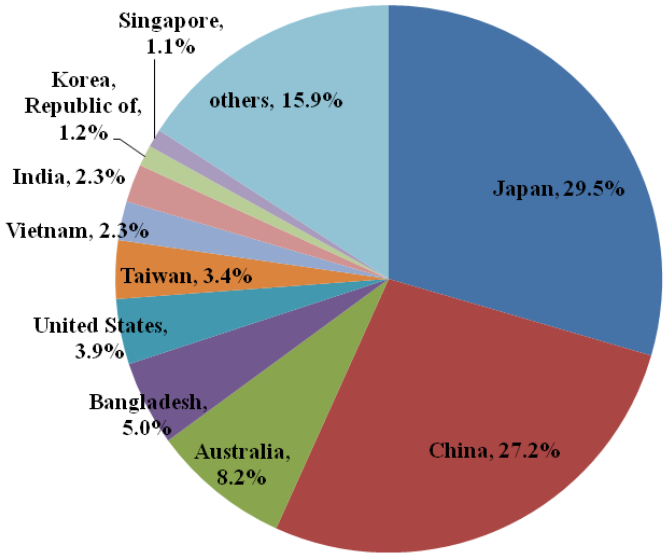

圖 1. 2013 年第二季垃圾信來源國家分布

細部觀察 4 月、5 月及 6 月來源比例，可發現中國在 4 月時，出現高於日本三倍以上的垃圾信件量，在 5 月時又降至約為一半的 21.7 %，而孟加拉在 5 月時，突然冒出排名第 4 的 10.5%垃圾信件量。呼應日本製造業、交通及觀光景氣轉好，商業活動更顯蓬勃，日本相關的垃圾信來源於 6 月明顯升高。

表 1. 2013 年第二季垃圾信來源國家比例

國家	4 月	5 月	6 月	季平均	季排名
日本	12.1%	23.8%	48.6%	29.5%	1
中國	42.1%	21.7%	19.1%	27.2%	2
澳洲	14.3%	10.6%	1.1%	8.2%	3
孟加拉	0.2%	10.5%	4.8%	5.0%	4
美國	4.1%	4.2%	3.5%	3.9%	5
台灣	3.4%	3.2%	3.7%	3.4%	6
越南	2.8%	2.4%	1.8%	2.3%	7
印度	2.6%	1.7%	2.4%	2.3%	8
南韓	2.1%	0.6%	1.0%	1.2%	9
新加坡	0.7%	1.3%	1.1%	1.0%	10
其他	15.6%	19.9%	12.9%	15.9%	

台灣目前在季排名位居第六，垃圾郵件來源比例不低且相較於第一季，有提高的趨勢，值得重視。美國與台灣的垃圾郵件來源高低曲線具有相似趨勢，一直維持在中高比例區間。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。最多的網頁主題為資訊科技相關類別，顯示約有 5 分之 1 的垃圾郵件網址會導引收件人前往資訊科技之網頁。

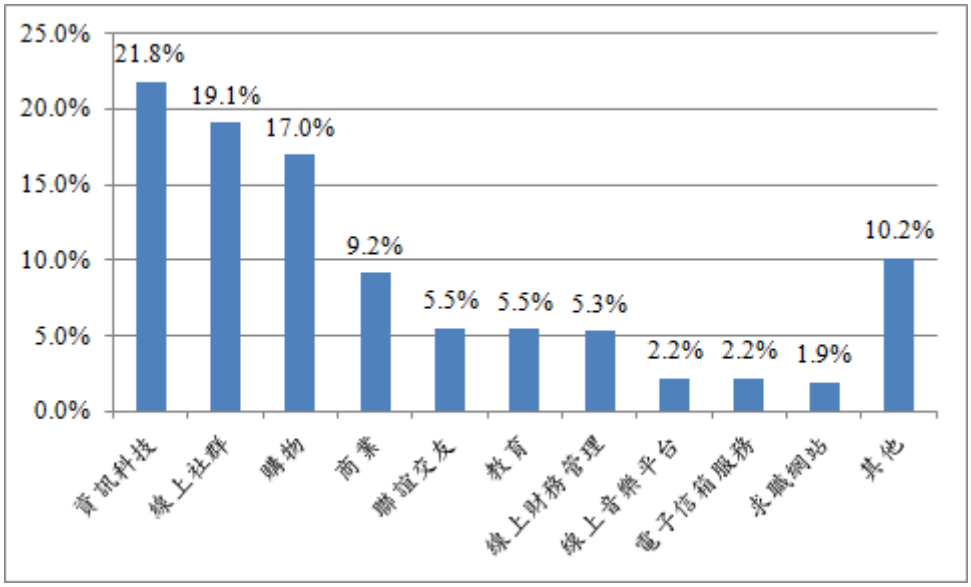

圖 2. 2013 年第二季垃圾信 URL 網頁內容分類

除了滿足使用者對於快速發展的資訊科技新知需求外，網路使用者在休閒議題上面，對於社群網路服務、購物需求也常有眾多接觸，值得重視的是這一季發現「求職網站」的相關網頁逐漸有增多的趨勢，除了呼應求職、轉職及失業率等相關社會議題外，推測適逢畢業潮，企業開始大量招募新進員工也是可能原因之一。

表 2. 2013 年第一季與第二季 URL 網頁內容分類比較

第一季			第二季	
排名	類別	比例	類別	比例
1	購物	22.4%	資訊科技	21.8%
2	商業	20.8%	線上社群服務	19.1%
3	資訊科技	11.1%	購物	17.0%
4	娛樂	7.8%	商業	9.2%
5	教育	4.8%	聯誼交友	5.5%
6	搜尋引擎	4.6%	教育	5.5%
7	投資	4.4%	線上財務管理	5.3%
8	旅遊	3.7%	線上音樂平台	2.2%
9	線上社群服務	3.6%	電子信箱服務	2.2%
10	新聞	3.0%	求職網站	1.9%

觀察第一季與第二季 URL 網頁內容，可發現兩季前十大排名主題相差甚遠，不僅資訊科技排名躍升第一，線上社群服務的排名也提升了七名來到了第二，此外聯誼交友、線上財務管理、線上音樂平台、電子信箱服務以及求職網站等五大議題也首度擠入榜內，值得後續關注。近期若要著手處理垃圾郵件防護過濾困擾時，仍建議先從 IT 相關議題、線上社群服務及購物相關議題進行處理，設定特殊關鍵字或進行樣本訓練，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

延續以往垃圾信的趨勢，轉址服務仍為垃圾信利用的主要手法，相關模式說明如下：

1. **透過轉址服務網站或其它手法間接轉址（Redirect）**
   具有威脅或不正當目的的垃圾郵件多會夾帶危險性無法預期的網頁連結，常見的手法即是巧妙營造信件中超連結存在的合法性；為了隱藏帶有威脅的真實網址位置，除了轉址服務或短網址服務網站，攻擊者也申請網路上暫用的主機名稱或短期利用的網域名，轉址以隱藏目標網站網址。

2. **透過第三方網站提供的服務或機制寄送廣告信**
   以往垃圾信發送者常利用被駭的電腦主機，做為廣告信發送跳板；現在則有越來越多的垃圾訊息透過各式社群網站之通知信寄送給收信者，由於是正當網站所寄送的信件，自然較容易被收信者打開閱讀，進而達成行銷效果。

3. **類社交工程廣告信**
   社交工程攻擊信件通常假冒收信者親友寄信，再於信中夾帶如 word 文件檔或 winrar 壓縮檔等附檔，被降低警覺性之收件者往往不經確認便開啟附檔而中毒；最近有許多廣告信模仿此種手法，提高收信者開信機率，惟信中並非夾帶病毒或木馬，而是較為單純而無攻擊性的廣告內容。

四、垃圾信樣本詳細說明

在郵件安全的議題中，釣魚信件一直以來都是企業或各級單位感到相當頭疼的問題，包括仿造銀行通知信、電子郵件通知信及社群網站訊息等各式通知信，甚至是企業間合作提案或是往來聯絡等，釣魚事件皆層出不窮；以下我們將會逐步介紹台灣地區、中國地區以及日本地區等常見的垃圾信樣本，其中不乏釣魚郵件案例。

● 台灣常見垃圾信發送模式

如下是最近收集到的一個網頁郵件服務釣魚信案例：

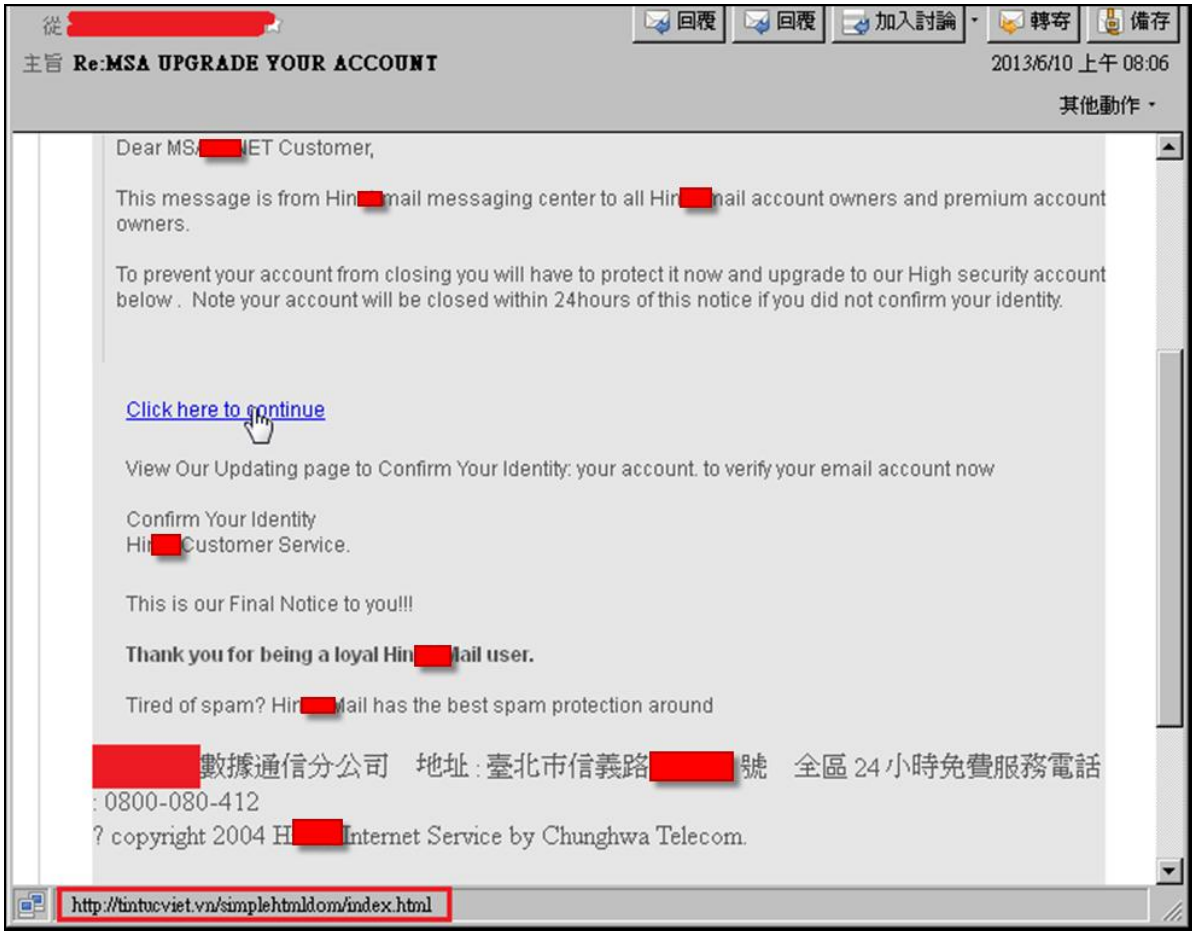

圖 3. 國內某知名電信商網頁郵件服務釣魚信

開啟信件觀察後可發現，和一般通知信不同，信中的「敬啟者」處只有「Dear … Customer」，而不是收信者的姓名或暱稱，可猜測應是同一信件大量發送；另外信中內文還警告會在 24 小時內關閉帳號，為了避免關閉帳號以及帳號升級，而要使用者登入來確認身份，但事實上為了尊重客戶，現在絕大多數的網頁郵件服務業者也不會有如此強迫性的動作。

網頁下方看到他的超連結，發現是 http://tintucviet.vn/simplehtmldom/index.html，網域是 tintucviet.vn，是越南的網站，基本上也和該電信商無關，推測應該是被駭客駭入後，再被加裝釣魚頁面而成。

進一步比較真實郵件信箱登入頁面與偽造的登入頁面，發現頁面相似度相當高，參考如下：

圖 4. 釣魚信引導的偽造登入頁面

圖 5. 國內知名電信商網頁郵件服務真實登入頁面

兩相比較下，頁面上差別不大，但正牌的登入頁面有使用 https 來加密，而釣魚頁面則沒有。接著檢查頁面程式碼看看：

```
<FORM name=personal onSubmit="return checkInput(document.personal)"
action=login.php method=post>
 <INPUT type=hidden name=usertype>
       <input type=hidden name=https value=1>
       <input type=hidden name=lang value=zh>
<TABLE id=puser cellSpacing=0 cellPadding=0 width=215
background=https://webmail.hinet.net/images/login-bg1.gif border=0 name="puser">
```

圖 6. 釣魚頁面的部分程式碼

```
<FORM name=personal onSubmit="return checkInput(document.personal)"
action=login.do method=post>
 <INPUT type=hidden name=usertype>
       <input type=hidden name=https value=1>
       <input type=hidden name=lang value=zh>
<TABLE id=puser cellSpacing=0 cellPadding=0 width=215
background=images/login-bg1.gif border=0 name="puser">
```

圖 7. 正牌登入頁面的部分程式碼

抽出其登入頁面中輸入帳號密碼的部分來檢查比較後發現，釣魚頁面中接收帳密資料後再處理的程式是 login.php，而正牌登入頁面中則是 login.do；另外也發現釣魚頁面在載入時是使用絕對路徑，和正牌登入頁面只使用相對路徑 images/login-bg1.gif 不同。

使用測試帳密登入偽造頁面之後，發現實際上只是被轉址到該電信商的首頁，但此時帳密應已被駭客得知！

根據過往觀察，這類的釣魚信件及釣魚頁面跟正牌的相似度越來越高，但由於其大量發信以及急欲求得使用者帳密的特質，還是可以在收信時發現到蛛絲馬跡，如對收信者稱呼或內文的急迫性等，此外最重要的就是信中的超連結，只要在打開超連結時，多注意其網址有無特殊之處，或和正牌業者的超連結內容有無不同，相信便可避掉此類的攻擊，針對這類網路威脅進行防禦，建議使用 MailGates 郵件防護系統內含之郵件內容防護模組，可即時提醒使用者網頁風險等級並可在使用者點選網頁之前即可一眼看出 URL 是否有暗藏玄機！

除了對資安方面有不少影響的釣魚信件攻擊外，社交工程也是網路資安上的一大威脅，而最近也發現有不少垃圾信利用社交工程的手法來打廣告，比如前一季觀察到的寬頻業者寬頻廣告信，這季也觀察到出現類似假裝與收件人熟識的手法所撰寫出的廣告信件：

圖 8. 刻意假冒與收件人熟識的廣告信 (上半)

圖 9. 刻意假冒與收件人熟識的廣告信 (下半)

近來觀察到的這類信件，推測由於垃圾信業者為方便大量發信，各個信件的發信者署名都一樣，如上例中都是小琪，收信者也都一樣，在此例中都是小 B，且此類郵件皆以開頭為假冒熟識的方式進行分享資訊，最後再將廣告的商家聯絡資訊附於文後。

而除了上類裝作熟人的手法，也有利用分享文章再偷渡廣告的情況。以下圖為例，該廣告信首先分享一篇帶有哲理的短文：

圖 10. 先分享文章後行銷公益活動之廣告信 (上半)

圖 11. 先分享文章後行銷公益活動之廣告信 (下半)

在此例中，先引用富含哲理的文章引導收件人閱讀，讓收信者看完文章後，會順暢的接著看廣告，如此一來即達成網路行銷業者行銷之目的。

除了一般店家的廣告外，本季持續觀察到網路行銷業者自行發送的廣告信，下為較特殊的範例分享：

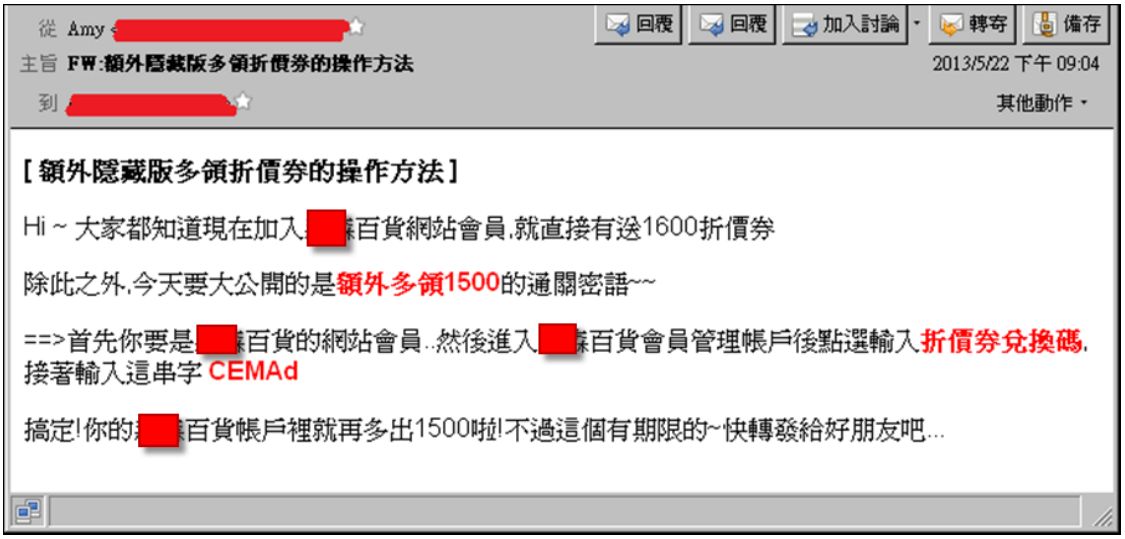

圖 12. 網路行銷廣告信

圖 13. 網路行銷網站頁面

如圖，此垃圾信發送者利用社交工程的手法發送廣告信，細看內容後，發現和一般商城店家為自己的商品打廣告不同，是直接以購物網站的名義進行廣告，算是網路行銷業者利用和購物網站結合行銷，藉以提升網路行銷業者自己的知名度。根據觀察目前有越來越多類似不同產業業者結合發送廣告信的趨勢，相信此舉為相當有力的廣告行為。

除了一般廣告信，金融借貸廣告信也有越來越多的趨勢，且以往大多只有廣告主的聯絡電話，但在這例子中除了有聯絡專線外，還有網站網址，不只加強了廣告本身的可信度，也幫網站打了廣告。

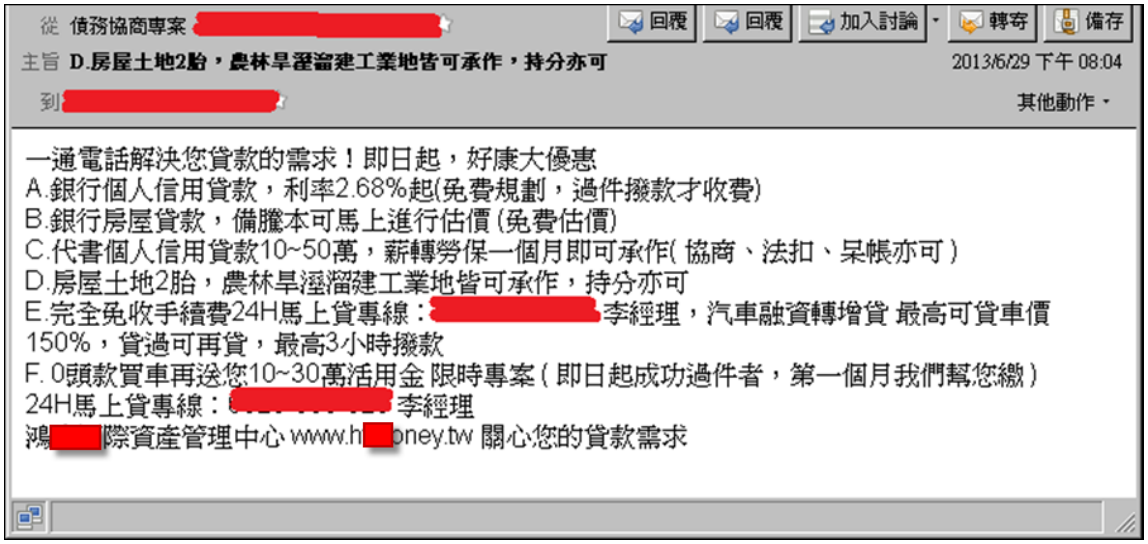

圖 14. 金融借貸廣告信

● 中國常見垃圾信發送模式

而在簡體中文廣告信方面，廣告目標沒有多大改變，多是網路商店廣告、代開發票廣告、商務課程廣告等等，但雖然廣告目標不變，但廣告手法卻是不斷翻新，如常見的代開發票廣告：

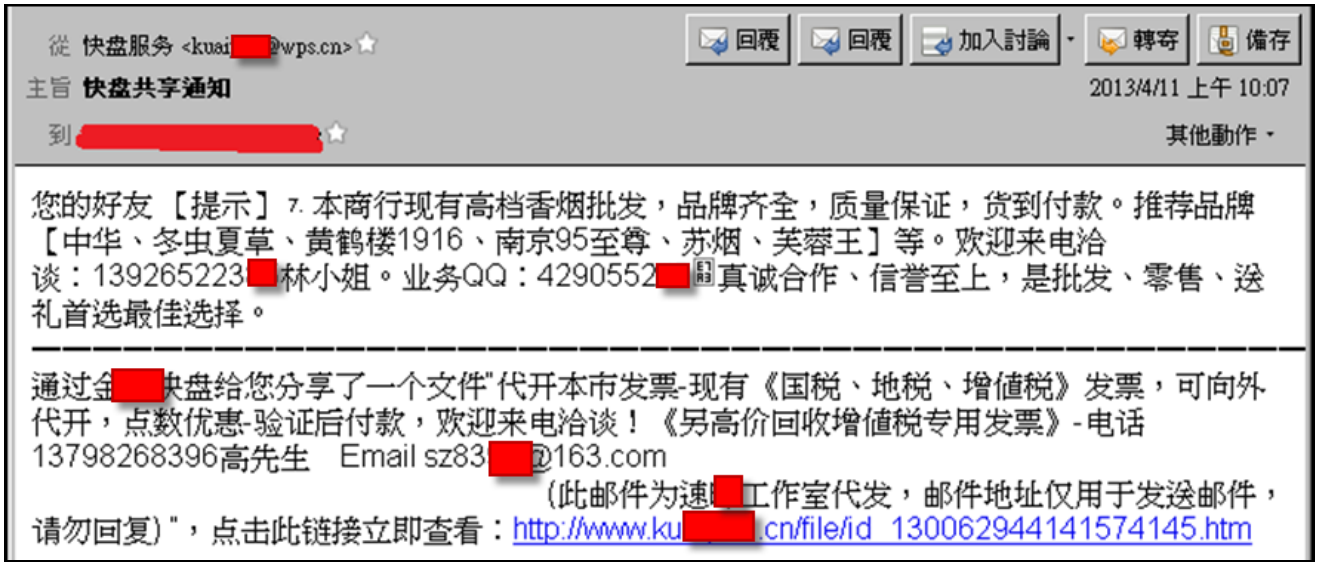

圖 15. 簡體中文代開發票廣告信之一

好比利用社群網站通知信間接發送廣告信一樣，在此例中，廣告信發送者利用了業者提供的服務中會發送通知信的機制或功能，在通知信中塞入廣告的內容，再經由系統寄送給收信者，這種作法雖然有點迂迴，但對廣告信發送者來說，利用該國的知名網站，較不會被起疑心，甚至可能被加入白名單而

避免過濾，另外這「快盤共享通知」通知信本身，也具有社交工程的特性，信件被開啟機率大，廣告效益也跟著提高。

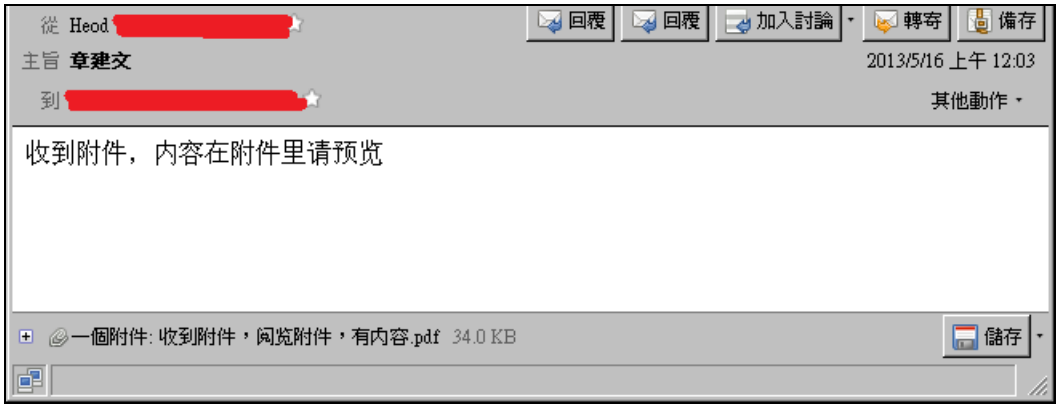

圖 16. 簡體中文代開發票廣告信之二

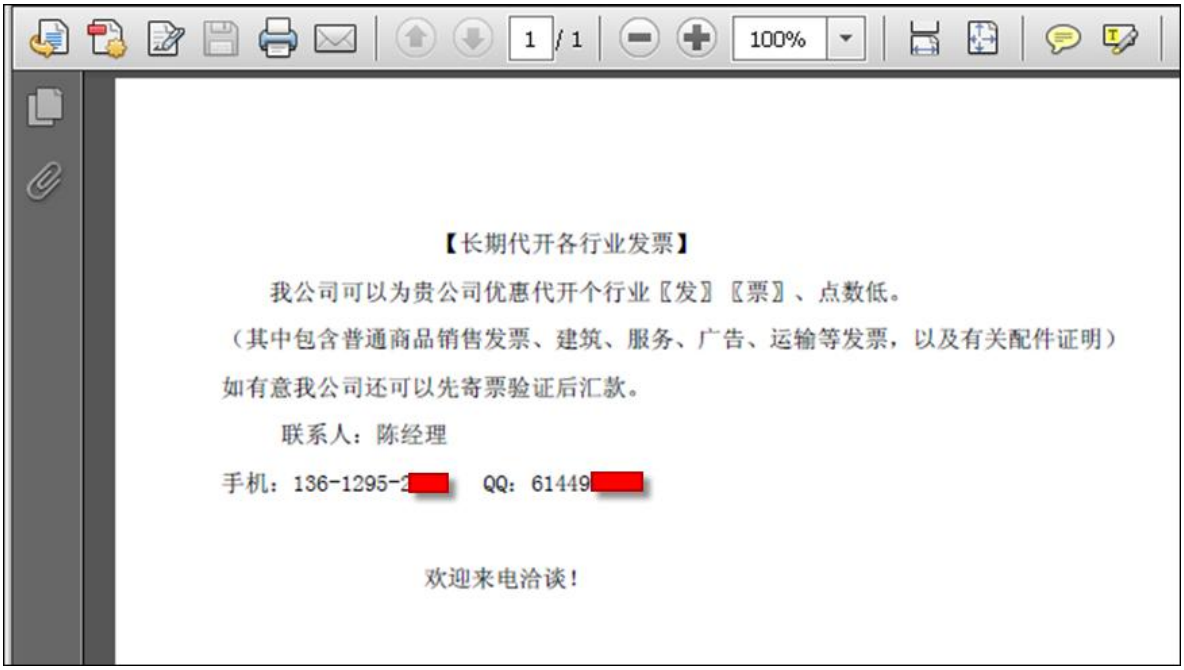

圖 17. 簡體中文代開發票廣告信之二的附檔

只提示收信者打開附檔而沒有其他資訊的廣告信很多，但以往發票廣告幾乎只加圖片類的附檔，而這例子則是將廣告內容全包入 PDF 檔案中，使用者須打開附檔後才可看到內容。

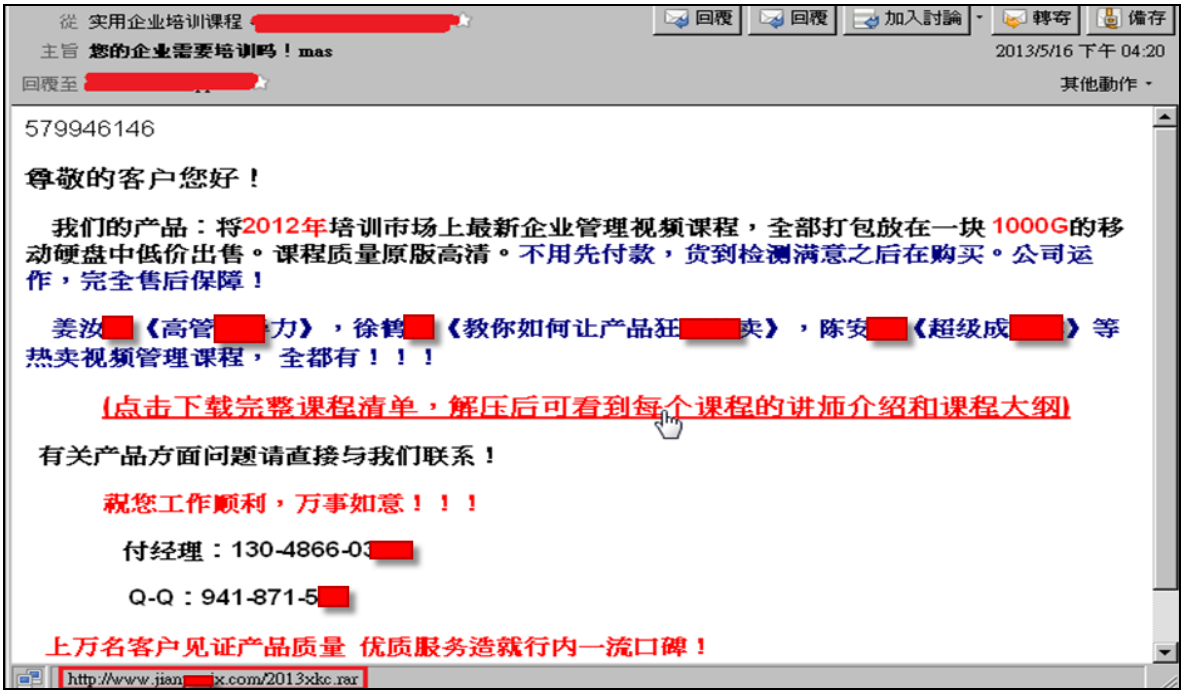

圖 18. 簡體中文商務課程廣告信

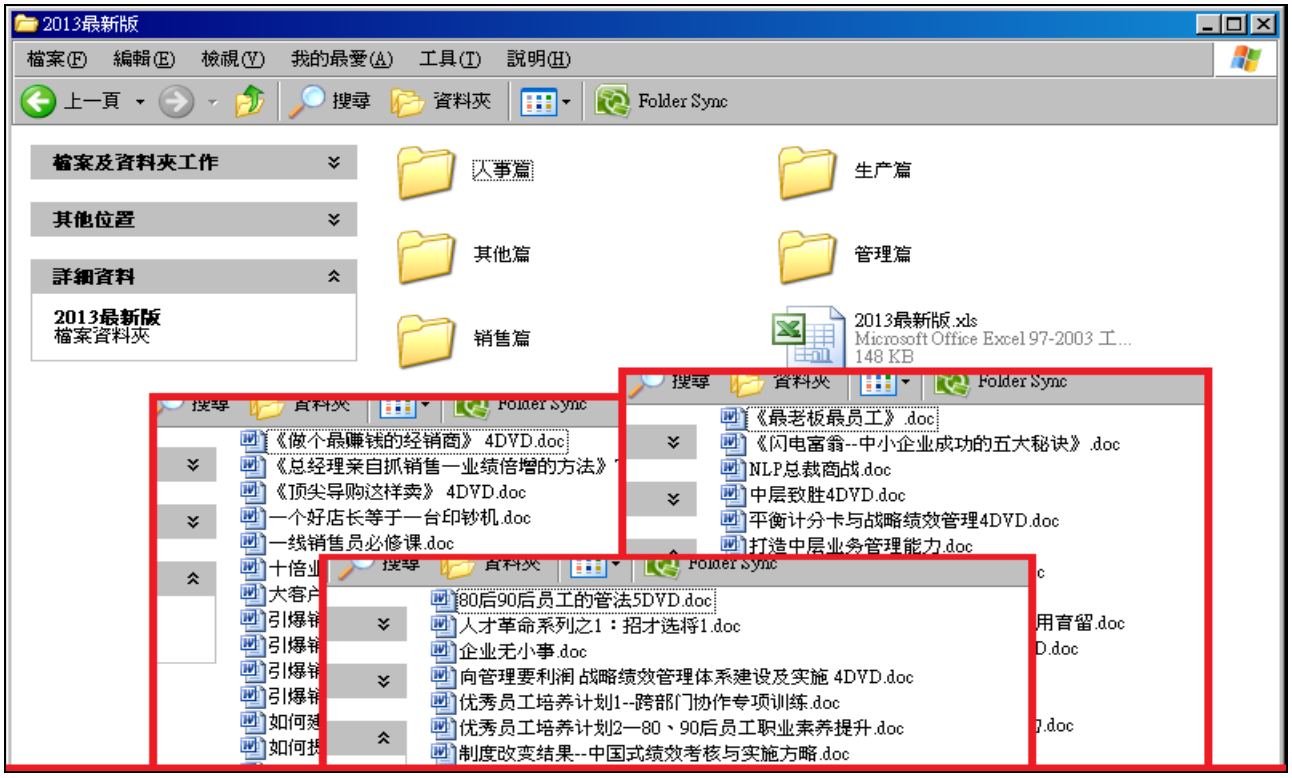

圖 19. 簡體中文商務課程廣告信連結外部檔案部份清單

如上圖，類似檢查附檔內容的例子，較特別的是要求收信者抓清單下來看，而且廣告目標雖然是商務課程，但卻是要收信者買裝有課程內容的外接硬碟，就廣告內容而言，實在是相當特殊的例子。

● 日本常見垃圾信發送模式

日文方面，廣告信主題以成人約會為大宗，常會有許多色情的圖片及敘述，接著常見的則名為 VIP 專屬的免費優惠詐騙信，此外還有博弈類廣告信，像是宣傳高得獎率的賽馬廣告信。

以下為數封名為數量有限的活動廣告信範例：

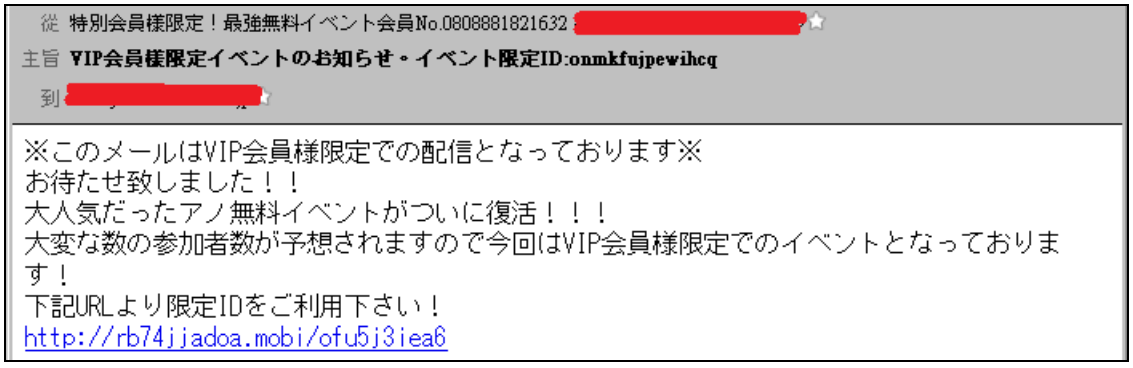

圖 20. 日本常見的 VIP 限定優惠活動廣告信

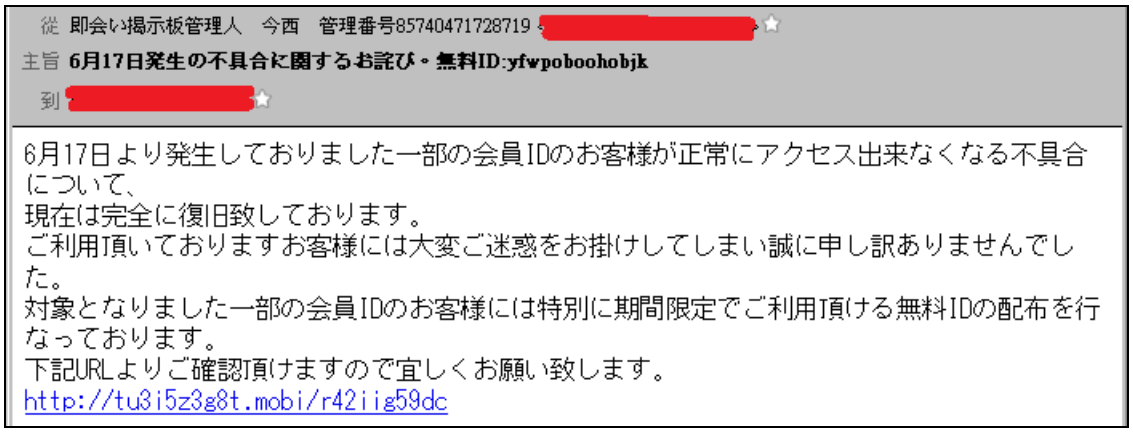

圖 21. 日本常見的期間限定優惠活動廣告信

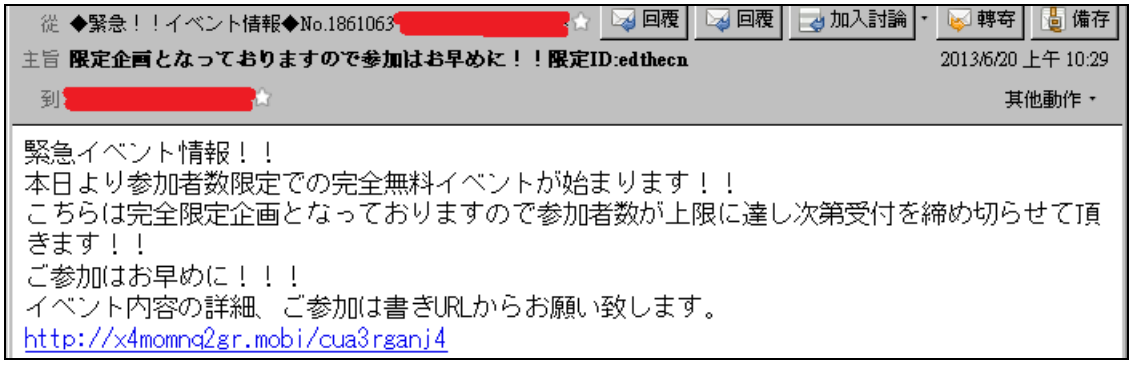

圖 22. 日本常見的人數限定優惠活動廣告信

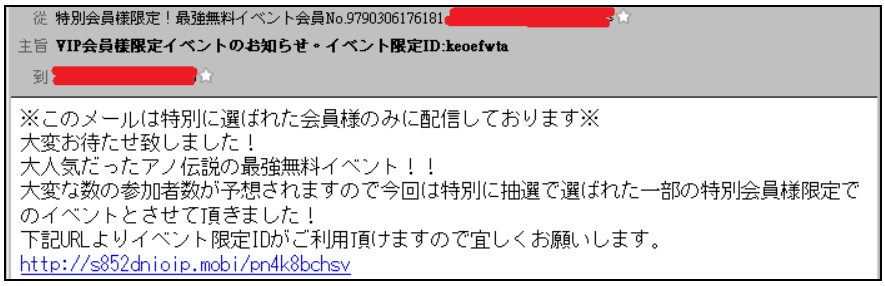

圖 23. 日本常見的 VIP 限定優惠活動廣告信之四

可從上面幾個例子觀察到，帶有限定風格的詐騙信寄件者都是利用暫時性的廣告目標網站，或是利用轉址功能，將瀏覽器轉址到目標網站。

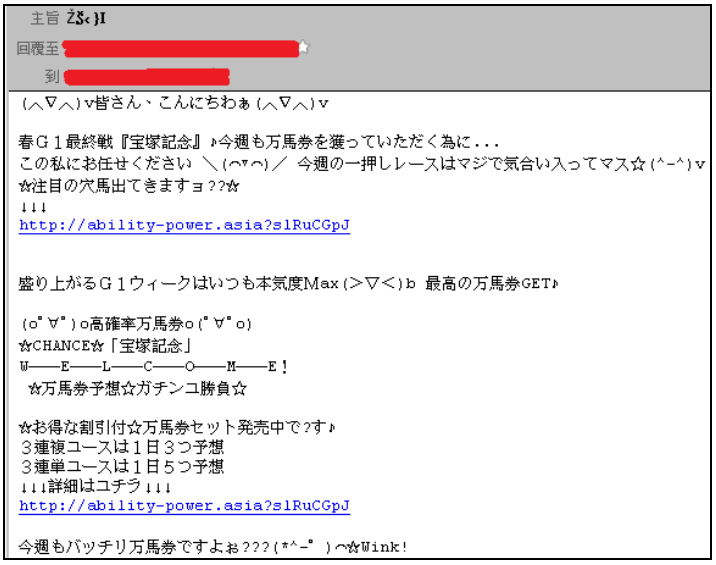

圖 24. 日文賽馬廣告信

這個例子觀察到，賽馬廣告信利用高得獎率的賽馬券為誘餌，進而引誘收件人點選廣告的網址，達成行銷目的。

有趣的是，到目前為止觀察到的此類日本的廣告信，幾乎都是使用自己申請的網域來提供轉址功能或作廣告目標網站，而其它語系的廣告信則是使用現有的短網址或轉址服務居多，雖然在目的上差不多都是為轉址，不過可能是垃圾信發送者本身的使用習慣，才會造成此差異；但不管網址長相為何，面對來路不明或有疑慮的網址，收信者都應小心為上，避免讓自己陷於資安危機之中。

Openfind 電子郵件威脅實驗室，特別從 2013 年第二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