Openfind™ Software Engineered for Growth™

Email Threats Analysis Report

Q1 2014

2014 第一季 Openfind 郵件威脅分析報告

目錄

一、全球垃圾信發送來源地區

2014 年第一季垃圾信來源國家的前三名分別為中國、美國與日本，依序佔整體垃圾信的 37.9%、30.8%與 10.6%。在本季中，美國超越了日本成為了第二名，與上季相比，大幅上升 25%。本季來源國家出現了去年不曾進榜的英國(1.0%)與只進榜一次南韓(0.8%)分別位居本季第八名及第九名。值得注意的是，本季前三名即占了垃圾信總量的近 8 成，顯示中國、美國與日本對於台灣地區的郵件安全影響非常重大。

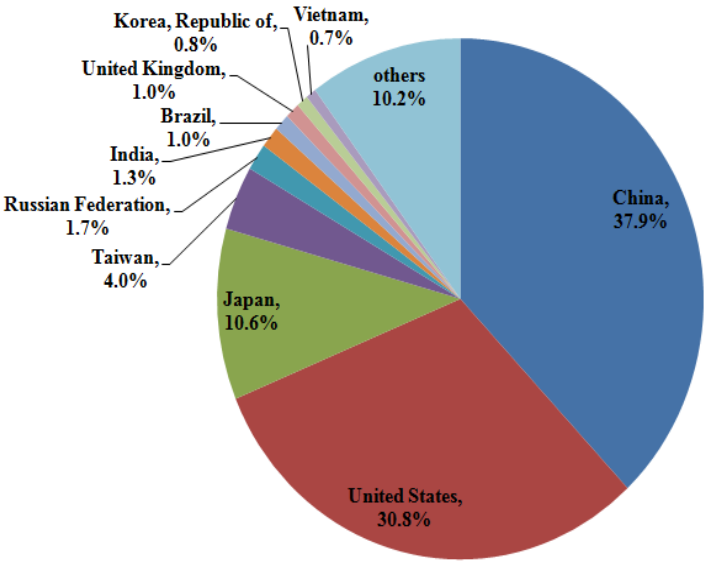

圖 1. 2014 年第一季垃圾信來源國家分布

細部觀察 1 月、2 月及 3 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三分之一左右，但在 3 月份時，比起 2 月份，提升了 12.5%，有大幅上升的趨勢。推測為新的一年度，中國各商城或網購業者欲在第一季投入諸多行銷活動、及廣發 EDM 等新訊，期許為整年營收鞏固良好基礎。新進榜的英國與南韓在 3 月，佔比皆來到了 1.0％以上，可密切觀察是否於第二季仍會有持續成長的現象。

表 1. 2014 年第一季垃圾信來源國家比例

國家	1 月	2 月	3 月	季平均	季排名
中國	35.5%	33.3%	45.8%	37.9%	1
美國	32.1%	42.4%	15.2%	30.8%	2
日本	9.3%	8.9%	13.8%	10.6%	3
台灣	4.9%	3.3%	4.0%	4.0%	4
俄羅斯	1.5%	1.3%	2.3%	1.7%	5
印度	1.1%	0.9%	2.1%	1.3%	6
巴西	1.5%	0.8%	1.0%	1.0%	7
英國	0.8%	0.4%	1.8%	1.0%	8
南韓	0.8%	0.6%	1.0%	0.8%	9
越南	0.6%	0.5%	1.0%	0.7%	10
其他	12.0%	7.6%	12.0%	10.2%	

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，且相較於前一季有下降的趨勢。俄羅斯名次較前季上升一個名次，不過佔比卻下降 1.2%。而印度於前季比重無明顯變化僅下降 0.2%。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。最多的網頁主題為購物相關類別，顯示超過 3 分之 1 的垃圾郵件網址會導引收件人前往購物相關網頁。

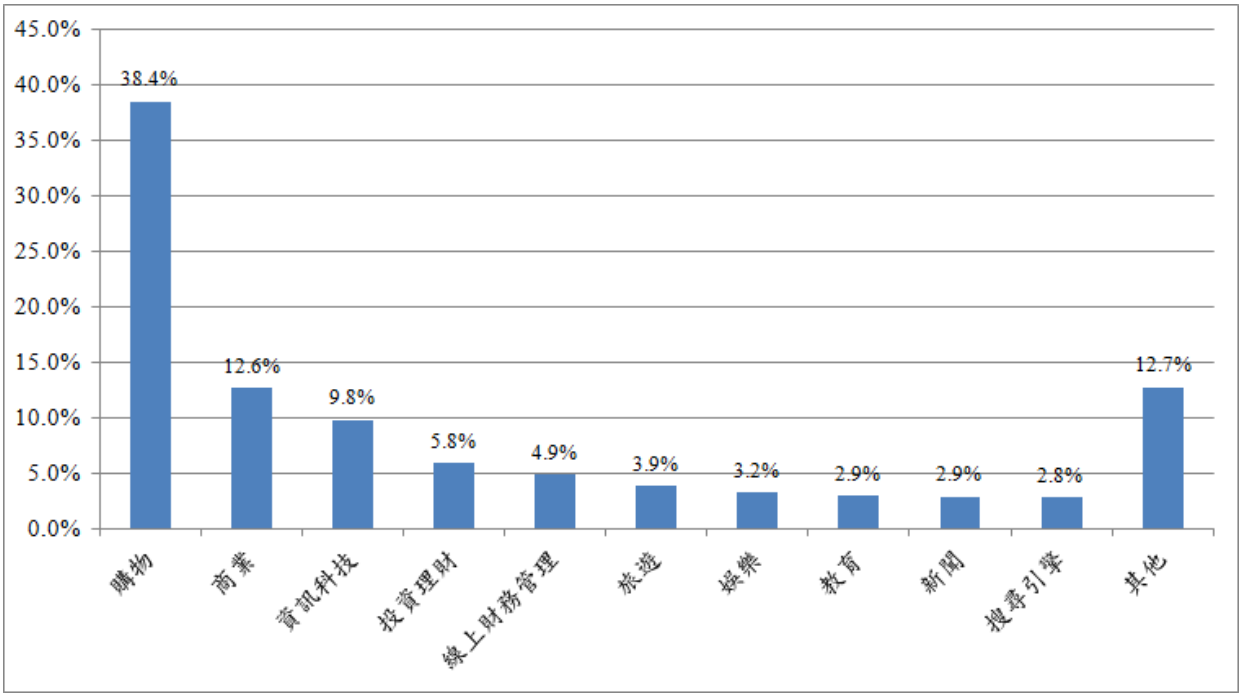

圖 2. 2014 年第一季垃圾信 URL 網頁內容分類

本季購物類別遙遙領先其他類別佔比 38.4%，與第二名商業差距為 25.8%。本季前三名垃圾信 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，2013 年排名第 5 的教育類別，於本季退居第八名。此外，出現新進榜的新聞類別，反應垃圾郵件緊扣時事以便增加點擊率的手法趨勢，推測三月時的服貿與學運議題也成為新聞垃圾郵件佔比提高的主因之一。

表 2. 2014 第一季與 2013 年第四季 URL 網頁內容分類比較

	2014 第一季		2013 年第四季	
排名	類別	比例	類別	比例
1	購物	38.4%	商業	26.9%
2	商業	12.6%	購物	23.7%
3	資訊科技	9.8%	資訊科技	12.6%
4	投資理財	5.8%	教育	4.8%
5	線上財務管理	4.9%	投資理財	4.0%
6	旅遊	3.9%	搜尋引擎	3.8%
7	娛樂	3.2%	線上社群服務	3.7%
8	教育	2.9%	娛樂	3.4%
9	新聞	2.9%	旅遊	3.1%
10	搜尋引擎	2.8%	線上財務管理	2.4%

觀察 2014 第一季與 2013 年第四季 URL 網頁內容，可發現兩季前十大排名主題幾乎完全相同，新進榜新聞類別，而線上社群服務類別延續前季退燒現象於本季退出榜外。近期若要著手處理垃圾郵件防護過濾困擾時，仍建議先從購物、商業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、本季垃圾郵件趨勢觀察

1. 假造與真實網址極為相似的釣魚網址

垃圾信發送時，垃圾信發布者可能會偽造擬真名號，引誘收件者上當。上當的收件人因此進而點擊其中超連結，或甚至於引導至釣魚網頁中填入帳號密碼。在此手法中，垃圾信發布者除了假造一個釣魚網站之外，更會精心設計該網站之網址，保留可辨識名稱的英數字，更改不易被人發現有異狀的符號字元，例：將 www.abcxyz.com.tw 修改為 abc-xyz-com.webs.com 等。

2. 利用第三方網站新聞為廣告商品提升形象分數

廣告信內文除了敘述廣告商品的特色與優勢外，多半也會附加外部網頁連結。比較常見到的是連結到廣告業者自建的商品網頁。本季觀察到，有廣告信是附加一個知名入口網站的商品新聞稿頁面連結，進行商品行銷曝光，利用該入口網站知名度，同時提升此商品的可信度與形象分數。

3. **廣告業者接用其他單位舊網域，過期白名單可能成為濫發廣告信幫兇**

一旦有單位更新網址或是不續用原先的網址，則該網址即可被其他單位所註冊或利用。廣告業者有時會利用其他單位不再使用的網域作為自己商品的行銷網站。若前一使用單位已被加入寄件來源白名單，一旦該組織更換網域，在白名單未更新的情況下，接用此網域的廣告信業者可就此漏洞，準確將廣告信件送至使用者的正常信匣之中。為避免過期的白名單成為系統缺口，敬請定期更新白名單，並確保每一筆資料的正確性與有效性。

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

和以往一樣，本季中也收集到不少釣魚信件，如下這一例電子郵件通知信：

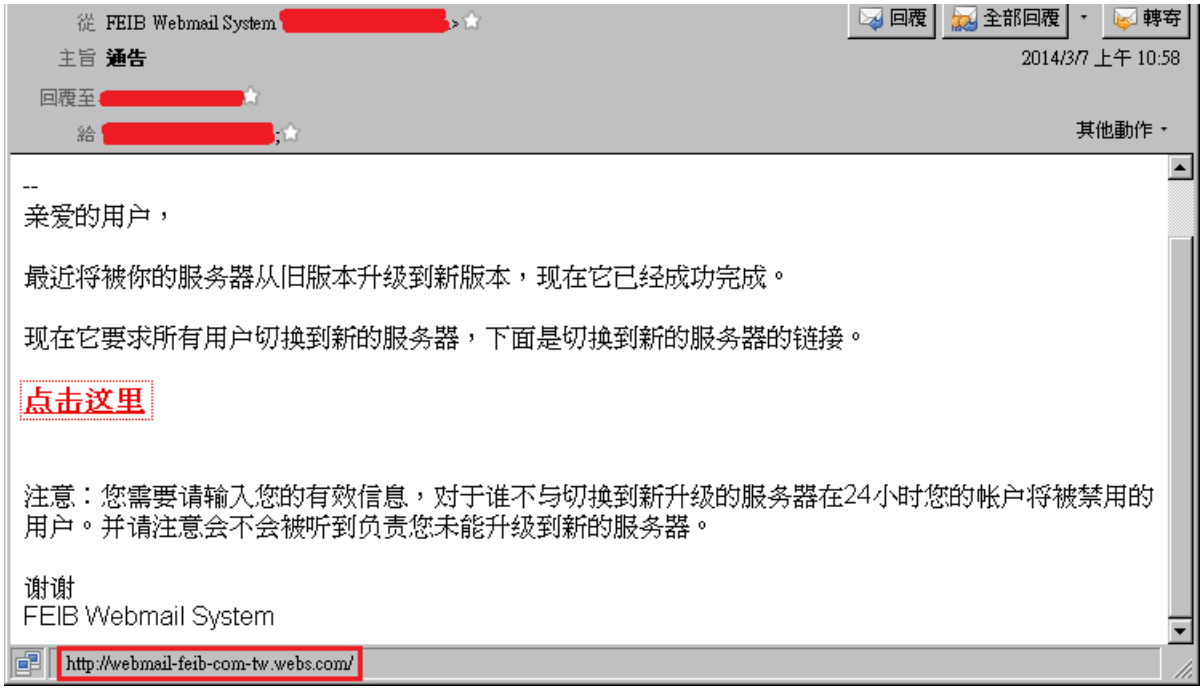

圖 3. 語法不順且偽冒銀行名義的釣魚信範例

由寄件者及內文的"FEIB webmail system"字樣觀察，本封釣魚信應是假造國內某知名銀行名義所發，不過另外也發現信中語句語法不順，這點和前一季的例子一樣，可推測應是不諳中文的發信者發出的，或是利用線上翻譯軟體將原本為其他國家語言的釣魚郵件內容，翻為簡體中文。

接著檢查郵件內含之超連結，信中網址是 http://webmail-feib-com-tw.webs.com/，眼尖的人可發現，該網址模仿攻擊目標網站 url，利用符號取代的方式改寫網址，例如：用破折號取代部分的句號等方式，意圖混淆使用者；而此 url 的網域則是一個提供免費網頁空間的網站，駭客直接引用做為假網站空間。

點選超連結後，進入如下頁面：

圖 4. 釣魚信連結所引導至的偽造網頁

接著再嘗試輸入任意帳密：

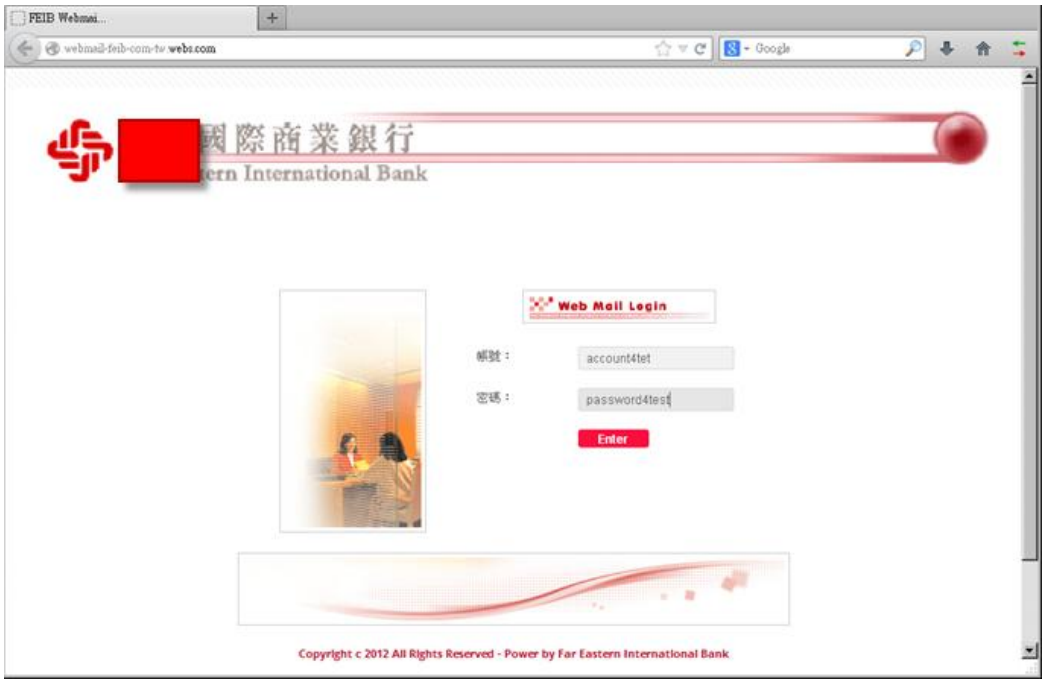

圖 5. 嘗試於釣魚網頁輸入任意帳密

點選 Enter 後，發現以下情形：

圖 6. 在釣魚網頁鍵入帳密後的情況

由上圖的操作可知，此釣魚郵件的建置成本相當低廉，且有諸多疑點存在：密碼以明文方式處理，鍵入完帳密後也沒有將釣魚頁面導到其它正常網站的頁面，且跟偽冒目標的真實網站相比並不神似，算是有相當多的破綻。建議使用者在收到疑似釣魚信件時，小心確認其真偽，以免帳號被盜。

圖 7. 偽造目標的真實網站設計

● 台灣常見垃圾信

普通垃圾信在散布廣告資訊時，基本上會搭配廣告信業者準備的網域，來當作廣告頁面的存放處，而本季中則發現到不同於此的例子，如以下這封類社交工程的廣告信：

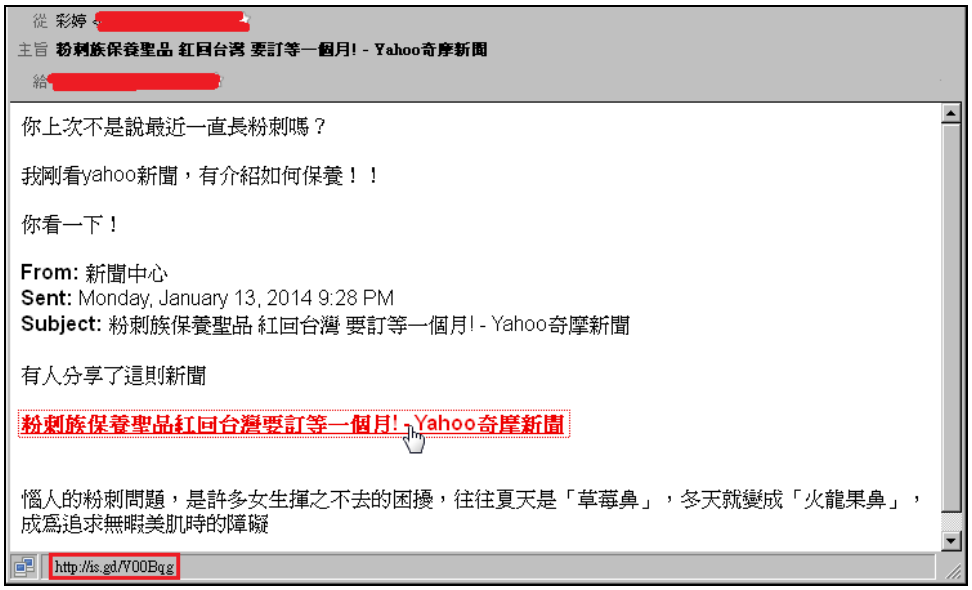

圖 8. 保養品廣告信

圖 9. 保養品廣告信點擊後畫面

點了廣告信內含之連結後，發現會經由縮址連結進入入口網站 Yahoo 的新聞頁面，而不是垃圾信發送者自己建的網域。利用一個公開的新聞稿頁面進行商品行銷曝光，對廣告信發送者來說相當方便，是相當值得追蹤觀察的手法。

另外，以下封廣告信做範例介紹，仍然是一篇應用現有網域之便利性，達成行銷之手法。此郵件內容為常見的貸款廣告信，根據以往的經驗，大多會用短網址或轉址等手法來掩飾，於是接著嘗試點擊郵件內之超連結來確認是否有轉址情形：

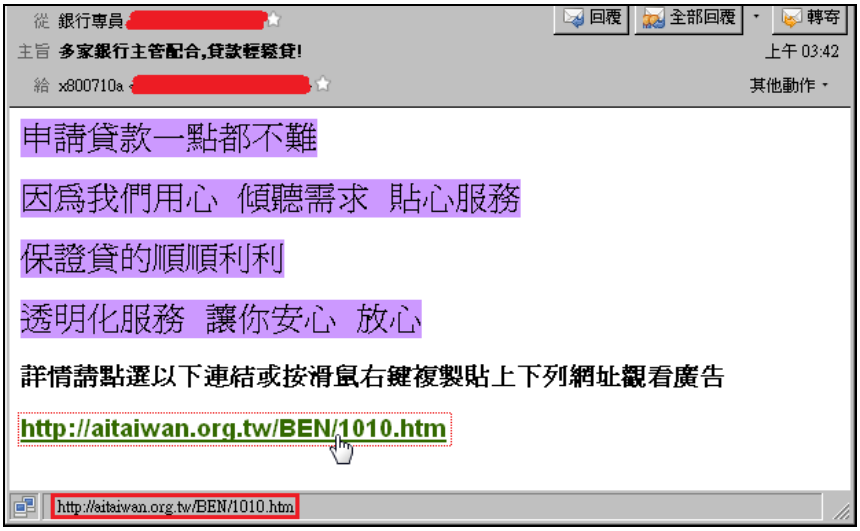

圖 10. 銀行貸款廣告信

圖 11. 銀行貸款廣告信超連結點擊後畫面

點了超連結，發現該網址沒有作轉址的動作，而是直接依照所示之 URL 秀出貸款廣告頁面，這在一般廣告信中是非常少見的，於是繼續檢查該網址的網域 aitaiwan.org.tw：

圖 12. 疑似使用原網域的網站

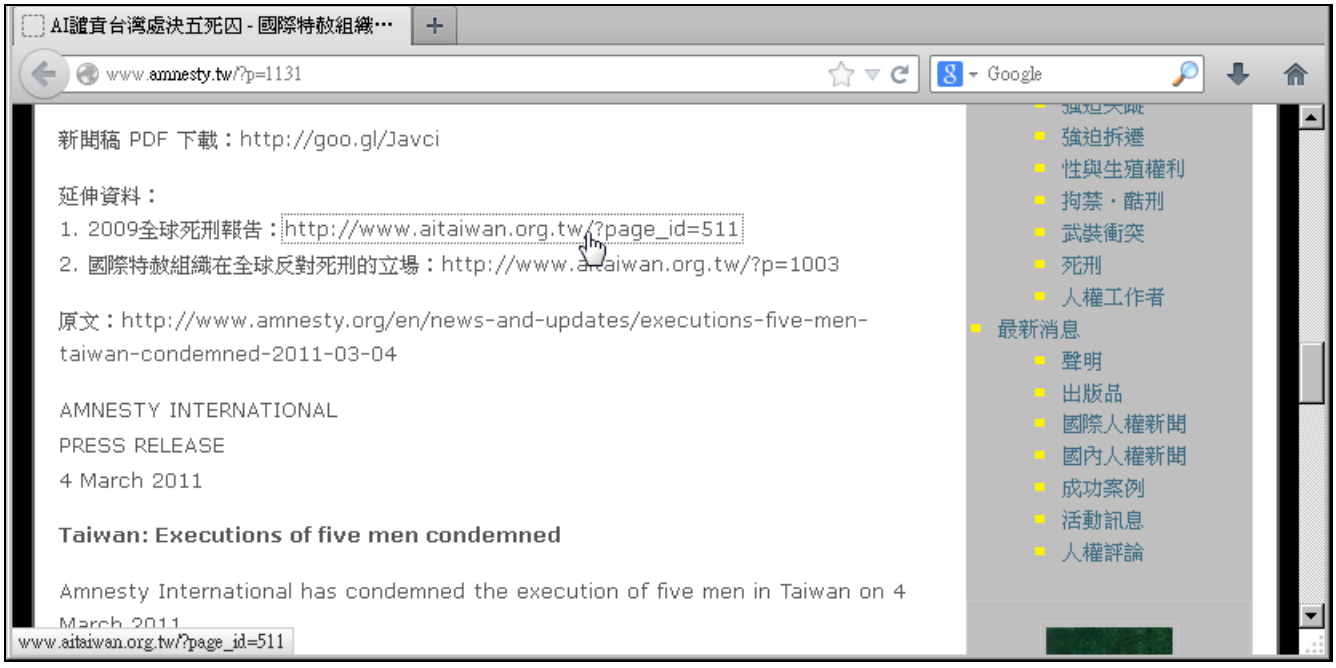

圖 13. 疑似使用原網域的網站的其中一頁

經研究後發現，「aitaiwan.org.tw」此網域之前應該是由某非營利組織使用。在該網站中，也可觀察到其一文章的超連結是連到 aitaiwan.org.tw 的網域。爾後該組織轉用 amnesty.tw 網域，aitaiwan.org.tw 則捨棄不用，於是這個舊網域便被廣告信發送者藉機利用。雖然在此例中的超連結沒有作轉址的動作以

隱藏目標廣告頁面，但是使用這種別的網站使用過的網域名，可能有個好處是它已被列入 url 白名單之中，因而會被垃圾信過濾機制略過，準確送入收件人信件匣。

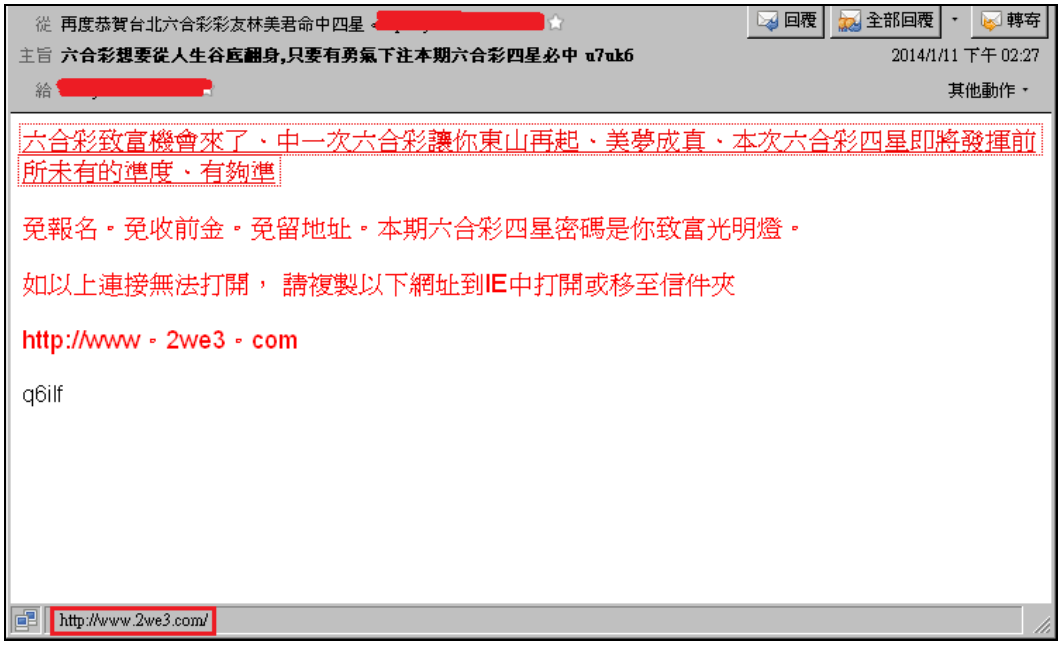

圖 14. 香港六合彩廣告信

在此例六合彩廣告信中，和前例一樣直接連接目標廣告頁面，較值得注意的是，網站本身可能只是騙取個資、或是騙取金錢用，隔了一段時間網站的頁面便已下架 (目前觀察網站已無頁面)，若是有收件者一時興起，跟著該網站進行下注，除了錢財損失無法追回，更危險的是個資可能被收集或盜用，因而得不償失。

圖 15. 香港六合彩廣告信點擊後畫面

● 中國常見垃圾信

在中國的簡體中文廣告信方面，本季中觀察到的垃圾信樣本類型大都和往常一樣，除了課程廣告信、代開發票信等，最常見的即是網路商店廣告信，如下這一例商城 EDM 廣告範例：

圖 16. 簡體網路商店廣告信

圖 17. 簡體網路商店廣告信點擊後畫面

這一類的廣告信，基本上已有很固定的形式，除了信中排版做的像一般 EDM 以外，也附有「按此退訂」的超連結，不過這邊仍要提醒使用者，若您不曾訂閱過該網站之 EDM，建議使用者避免點選超連結，避免連至惡意網頁，造成資安漏洞。

● 日本常見垃圾信

日文廣告信方面，以往常見的都是具有商業性質的廣告信，如色情廣告信、優惠詐騙信及博弈類廣告信等，不過本季收集到一則有關於環保的垃圾信，算是其中較有趣的例子：

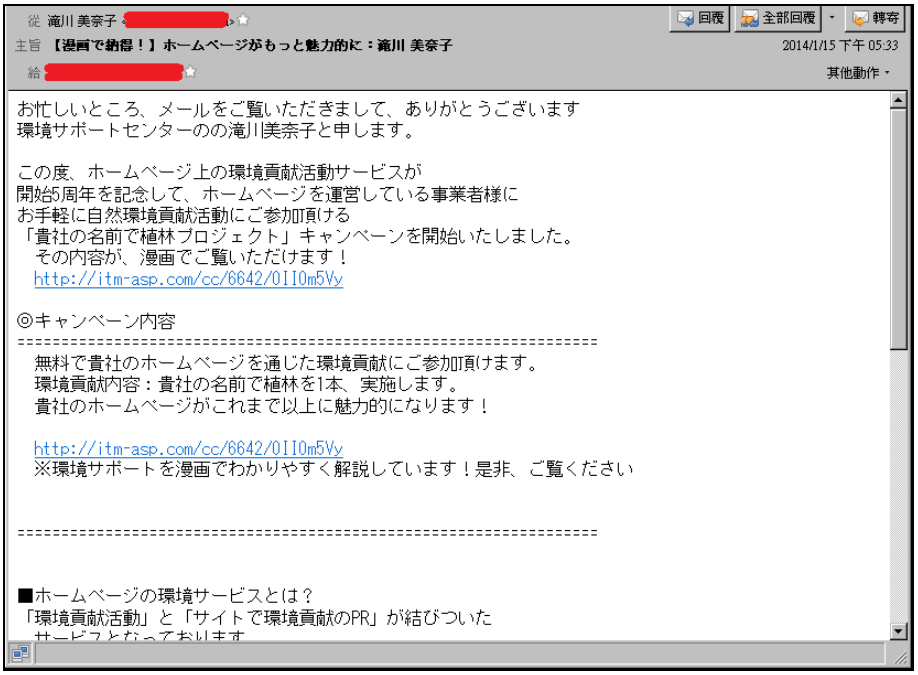

圖 18. 日文環保相關廣告信

圖 19. 日文環保相關廣告信點擊後畫面

此廣告信主要目的為讓參與企業可以公司名義進行植樹活動，並且可於該企業網站中貼上 Green Site License，展現公司環保意識，和往常常見的商業廣告信相當不同。另外，此封廣告信發信來源則是日本某專門製做 EDM 以及代發 EDM 的公司，信中網址的網域便屬於該 EDM 公司，同樣的也使用轉址來導到目標廣告網站，如圖中的頁面，是由

http://itm-asp.com/cc/6642/0II0m5Vy (屬於 EDM 公司之網域)

轉到

http://www.gsl-co2.com/comic01/ (廣告商品網站)

再轉到

https://gsl-co2.com/comic01/index.html (廣告商品網址)

才是實際的頁面，推測一開始的 EDM 公司網域應有點擊率統計之用，並非純粹轉址而已。

此外，在信的最後有附上「按此退訂」的超連結，如果是一般廣告信，可能是沒用的超連結，或甚至是有害的，不過在此例中寄送此信的公司，看起來是較正常經營的 EDM 派送服務網站，應是有實際退訂作用。

● 其他語言垃圾信

一般商業廣告信為了增加效益，大多會有地域性，也就是會傾向選擇和目標廣告同語系的地區來發送廣告信，不過本季收集到一封在中文地區相當罕見的西班牙文廣告信，如下圖交友網站廣告信：

圖 20. 某西班牙文線上交友廣告信

此封廣告信中，和其他廣告信一樣有使用轉址，可能是發信業者作統計之用，而信件本身，也像封普通的 EDM，雖然如此，建議使用者在收到這類信件時，若是有興趣查看超連結內容，仍要注意有無木馬、後門程式等具威脅性的軟體。

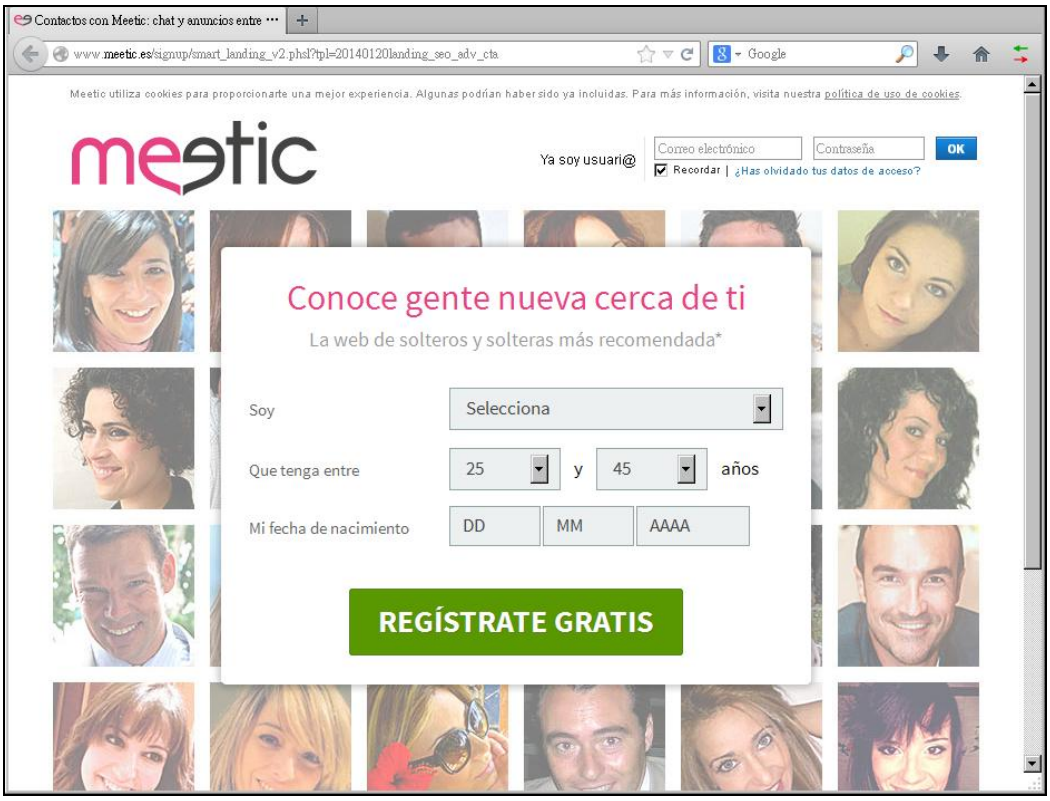

圖 21. 該西班牙文線上交友廣告信點擊後畫面

據查，此交友網站於數年前亦曾進軍台灣，或許有許多台灣會員帳號，推測或許是因此該網站會不定期發送廣告郵件至台灣地區。日前嘗試連至 http://www.meetic.tw/ 會導入 http://www.meetic.com/ ，也請讀者在接收郵件時，小心相關訊息，切勿因一時的好奇心，點選不明郵件的內含超連結，造成意外風險。

Openfind 電子郵件威脅實驗室，特別從 2014 年第一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