Openfind™ Software Engineered for Growth™

Email Threats Analysis Report

Q2 2014

2014 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

2014 年第二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 44.8%、16%與 12.3%。本季冠軍中國比例較上一季上升近 7%，而第二名的美國跟上季相比卻減少近 15%，顯示本季中國地區的垃圾信影響程度大。第二季出現了今年新進榜的新加坡占有 3.5%。台灣名次與上季相同，皆為第四名，但比例也明顯上升了 3.4%。前四名垃圾信來源國的比例加總後高達總量 80.5%，顯示中國、美國、日本、及台灣本地對於台灣地區的郵件安全影響程度相當重大。

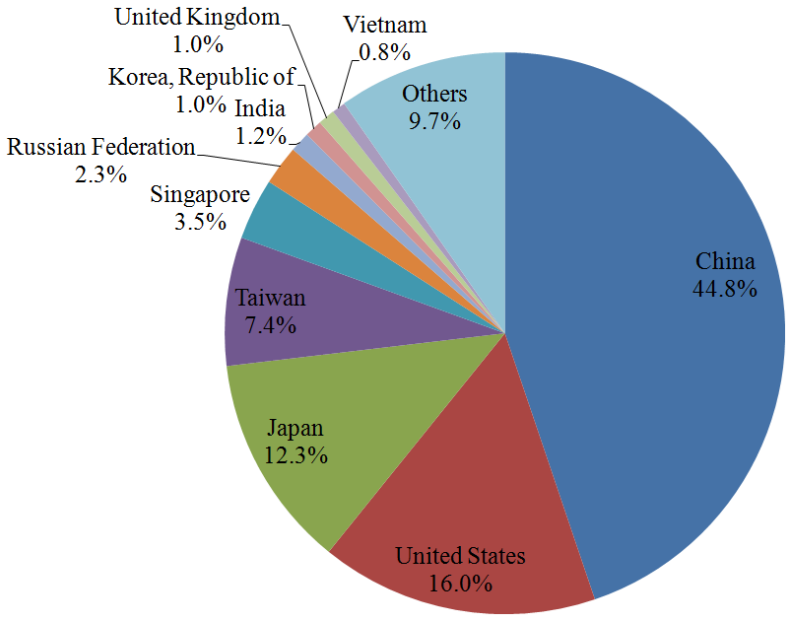
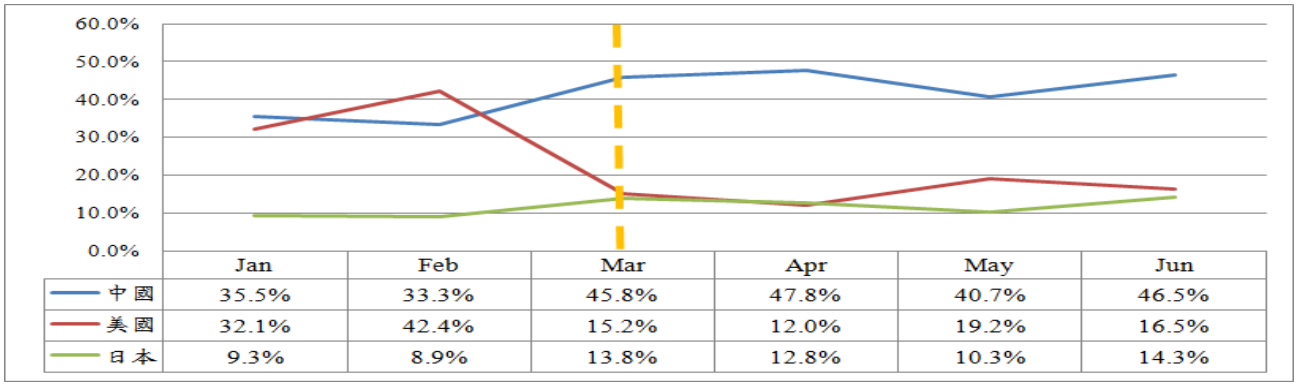


圖 1. 2014 年第二季垃圾信來源國家分布

3 月份似乎是個有趣的分水嶺，本季前三名皆延續 3 月的水準，在本季有穩定的表現。中國的垃圾信件量延續 3 月份的 45.8%的高比例，在本季本月皆占整體比重的 40%以上，行銷攻勢似乎沒有隨著季節改變而趨緩，依然蓬勃發展。季軍日本也有類似的走勢，延續 13.8%的比例，在本季於 10.3%~14.3%間擺盪。而亞軍美國，在 2 月份達到 42.4%的高峰之後，延續 3 月份的 15.2%左右的水準，於本季皆維持在 12%~19%的區間，行銷活動趨緩。接下來可密切觀察第三季時，是否又會出現其他的分水嶺。



	Jan	Feb	Mar	Apr	May	Jun
中國	35.5%	33.3%	45.8%	47.8%	40.7%	46.5%
美國	32.1%	42.4%	15.2%	12.0%	19.2%	16.5%
日本	9.3%	8.9%	13.8%	12.8%	10.3%	14.3%

圖 2. 2014 年中國、美國及日本上半年佔比趨勢

表 1. 2014 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
中國	47.8%	40.7%	46.5%	44.8%	1
美國	12.0%	19.2%	16.5%	16.0%	2
日本	12.8%	10.3%	14.3%	12.3%	3
台灣	8.3%	8.8%	4.8%	7.4%	4
新加坡	0.9%	5.4%	4.1%	3.5%	5
俄羅斯	2.9%	2.0%	2.0%	2.3%	6
印度	1.3%	1.0%	1.2%	1.2%	7
南韓	1.1%	0.9%	1.0%	1.0%	8
英國	1.8%	0.5%	0.6%	1.0%	9
越南	0.9%	0.8%	0.6%	0.8%	10
其他	10.3%	10.4%	8.3%	9.7%	

台灣目前在本季排名位居第四，4、5 月時，一度衝高至 8.3%~8.8%，其後又恢復於 4% 左右的水平。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。

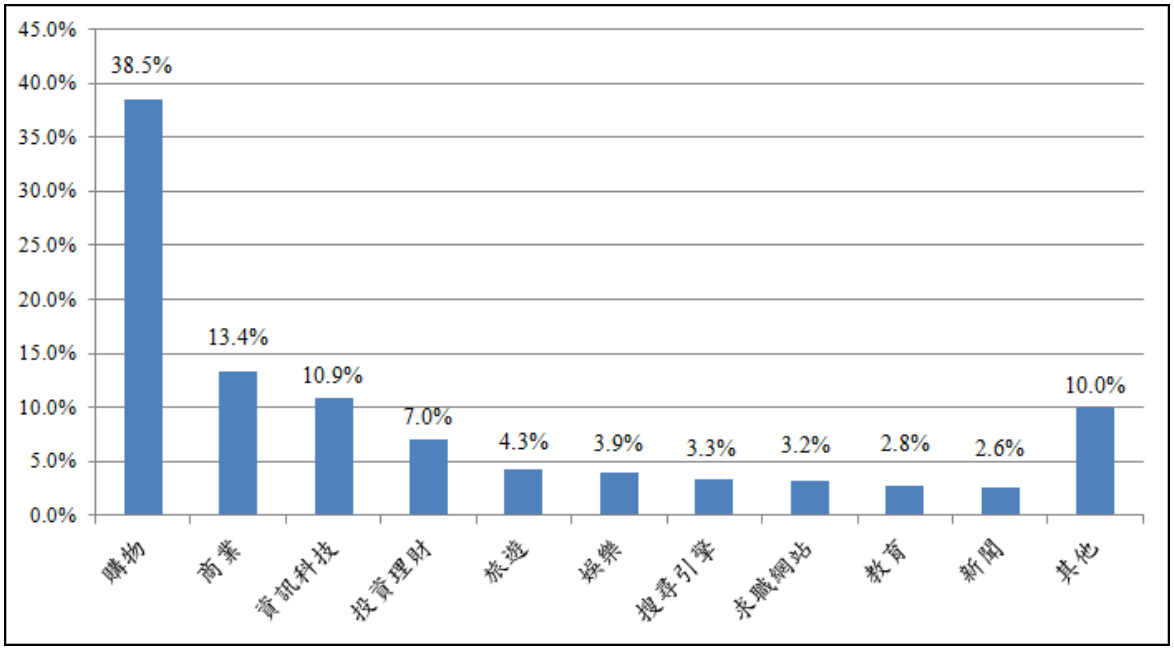


圖 3. 2014 年第二季垃圾信 URL 網頁內容分類

本季購物類別遙遙領先其他類別佔比 38.5%，與第二名商業差距為 25.1%，狀況與第一季相去不遠。本季旅遊類別上升至第 5 名與新進榜第 8 名求職網站，顯示臨近暑假與畢業季，有大量的潛在旅遊需求，也有許多就職活動在此時熱絡發生。Q1 也有進榜的新聞類別本季持續出現，反應垃圾郵件緊扣時事以便增加點擊率的手法趨勢，推測第二季末世足賽議題也成為新聞垃圾郵件佔比提高的主因之一，Openfind 提醒各用戶加裝可防範帶有新聞特徵的郵件 DNA 鑑識分析機制，以達最佳過濾效果。

表 2. 2014 第二季與 2014 年第一季 URL 網頁內容分類比較

	2014 第一季		2014 第二季	
排名	類別	比例	類別	比例
1	購物	38.4%	購物	38.5%
2	商業	12.6%	商業	13.4%
3	資訊科技	9.8%	資訊科技	10.9%
4	投資理財	5.8%	投資理財	7.0%
5	線上財務管理	4.9%	旅遊	4.3%
6	旅遊	3.9%	娛樂	3.9%
7	娛樂	3.2%	搜尋引擎	3.3%
8	教育	2.9%	求職網站	3.2%
9	新聞	2.9%	教育	2.8%
10	搜尋引擎	2.8%	新聞	2.6%

觀察 2014 第二季與第一季 URL 網頁內容，可發現兩季前十大排名主題幾乎完全相同，線上財務管理類別與求職網站類別一退一進，而線上社群服務類別延續前 2 季退燒現象於前季退出榜外後，本季仍未進榜。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. APT 攻擊第一步：騙取目標系統的使用者帳密

APT 攻擊的常見手法就是在郵件內容的編寫上利用社交工程攻擊或是應用收件人關心的議題，激發收件人的點擊好奇心。而在郵件格式的呈現則會利用附檔、超連結、及含有表格的外部網頁等元素製作惡意郵件。當收件人跟隨郵件內容指示下意識在陌生網頁中填入自己的帳號、密碼、或是 Email Address 時，也代表駭客已經完成 APT 攻擊侵蝕的第一步。

2. 知名品牌常成為被偽冒的標題

從國人常使用的社群網站、分享連結方便的影音網站、即時通訊服務，到非常普遍的 APP 下載商店等，當龐大的使用者們逐漸習慣了這些系統不定期所發出的通知信模式後，上述知名品牌的名號，開始被有心人士偽冒，進而完成了唯妙唯肖的釣魚郵件。收件人可先確認自己是否曾以此帳號在該類網站註冊，且通知信的語句是否通順，如果企業管理單位擔心人為疏失點選的話，建議可導入郵件過濾服務與外部網頁風險提示等資安防護，強化郵件溝通安全。

3. 多數廣告信件具有相似文本特徵

長期觀察一地區的廣告信件，除了發現有類別集中的現象之外，也觀察到不同時間發送的廣告郵件也常具有類似語句或詞藻的文本特徵，由於無法確實掌握每一封信會出現的詞彙，這樣的特徵難以用傳統的關鍵字偵測，而是應該把目光放遠，將整封信的文本特徵取出，利用特殊的全文雜湊函數進行完整比對，相似度高者，極有可能為會造成收件人困擾的廣告郵件。

四、垃圾信樣本詳細說明

以下我們將介紹並說明在本季中收集到的釣魚信件案例，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

本季中收集到的釣魚信件中，仍有許多例子是內文語法不順的，如下這一例偽冒成 Mail2000 通知信的釣魚信：

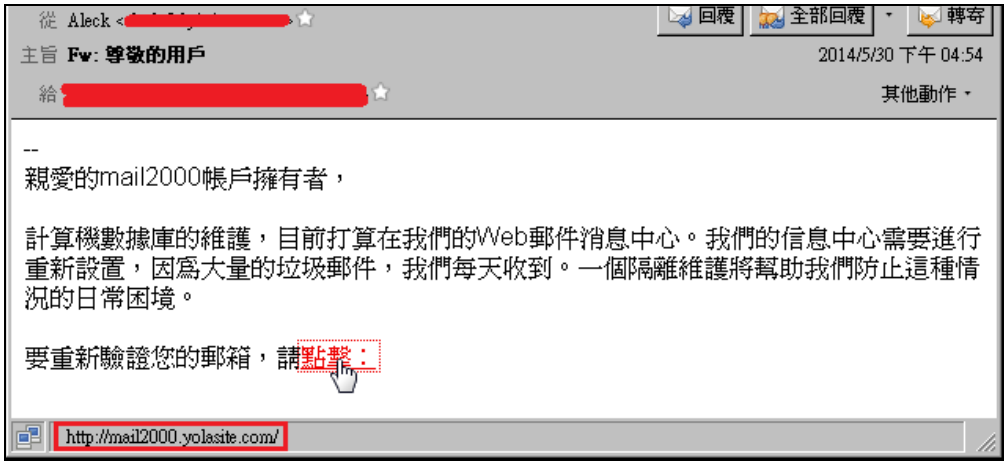


圖 4. 偽冒 Mail2000 名義的釣魚信範例

除了語法不順外，可注意到信中超連結的網域看起來也有問題，雖然其中有 mail2000 字樣，但是實際上 domain 是 yolasite.com，若是直接連到 yolasite.com 則會被轉址到 yola.com，它是一個提供使用者免費/付費放置網頁服務的網站，和 Mail2000 基本上沒有關係。接著嘗試打開超連結：

圖 5. 釣魚信連結所引導至的偽造網頁

點開其超連結後，發現頁面非常陽春，只有 Mail2000 字樣和簡單的輸入欄，其它幾乎什麼都沒有。

接著嘗試作登入動作試試看：

圖 6. 嘗試於釣魚網頁輸入任意帳密

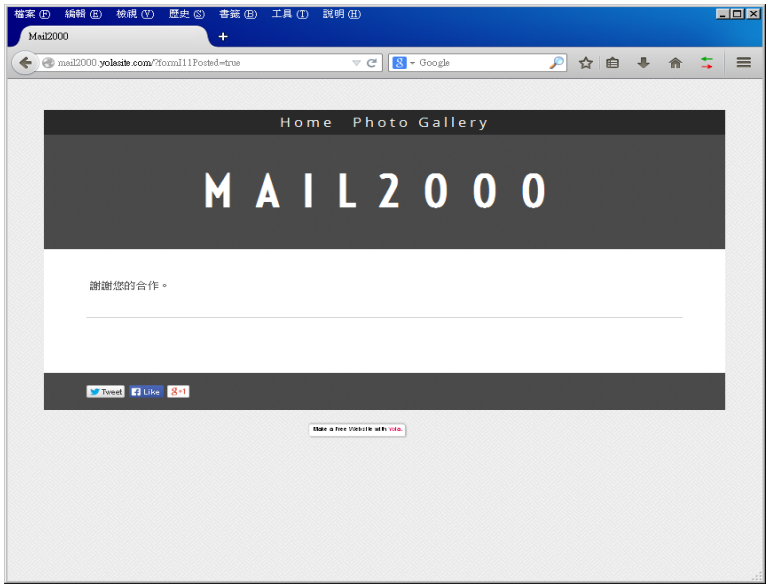


圖 7. 在釣魚網頁鍵入帳密後的情況

發現登入完後，只秀出了一個簡單的訊息，沒有導到正常的 Mail2000 頁面。接著檢查原始碼，看到其中 form 的 action 所指定的位址：

<form method='post' accept-charset="UTF-8" action='//forms.yola.com/formservice/en/c6ee1...(略)...f/I11/'>

應是 yola.com 本身接收 form submit 資訊的 cgi，也就是說，該釣魚信發送者利用第三方網站提供的免費建置網頁功能，建立騙取帳密用的網頁，以及其本身的 cgi 用來收集被害者的資訊，且因其未指向其它 host 的 cgi 做處理，減少了能被外界沿線追查與分析的資訊，藉此了解這樣的免費網頁網站，對一般人來說是能方便建置網頁的工具，對釣魚信業者來說更是迴避被資安業者分析的好幫手。

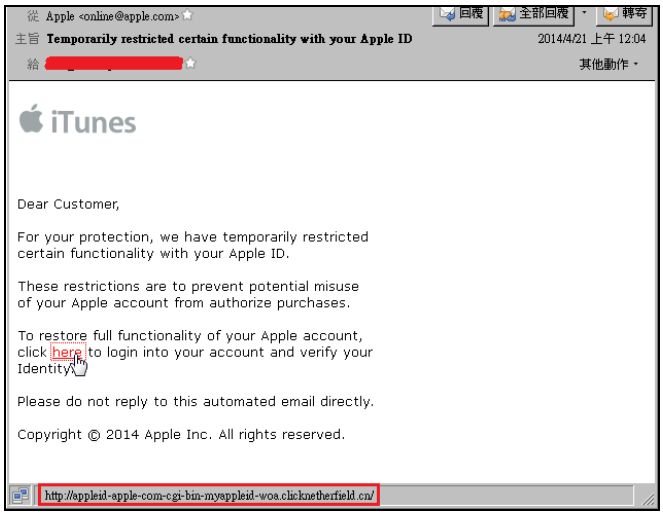


圖 8. 偽造成 Apple 通知信的釣魚信

如圖，本季中也收集到偽造成 Apple 通知信的釣魚信，此封信件乍看之下似乎是真正的通知信，但仔細觀察信中的超連結：

http://appleid-apple-com-cgi-bin-myappleid-woa.clicknetherfield.cn/

可發現前面不是 appleid.apple.com 而是 appleid-apple-com，把部分符號代換掉了，且真正的網域是 clicknetherfield.cn，這是許多釣魚信件慣用的手法，他們會將網址編造得和正牌網址很像，用以魚目混珠，騙過使用者的眼睛，讓使用者進入詐騙網頁。

為了防範假網址，建議使用者在點開超連結時，最好能先仔細查看該網址，若覺得有問題就避免點開，以免受騙上當。

● 台灣常見垃圾信

上一季中發現的使用社交工程的商業廣告信，其超連結是利用 Yahoo 新聞作為廣告站點，基本上沒有透露出其廣告信業者的資訊，而本季中也收集到了幾乎一樣手法的廣告信：

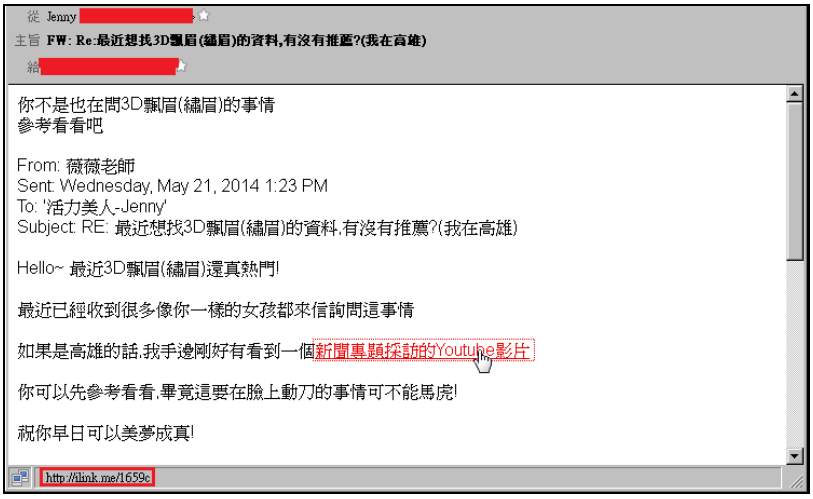


圖 9. 保養品廣告信

乍看之下，似乎是正常的往來書信，經由某收信者再轉寄給使用者，基本上不太會讓人起疑。接著觀察該信中的超連結，點選之後發現有多重轉址：

http://ilink.me/1659c 轉址到

http://cemad.cigi.tw/click.html?loneg1 轉址到

https://www.youtube.com/watch?v=RQEMd5SSULI&feature=player_embedded

圖 10. 保養品廣告信超連結點開後的影片

垃圾信發送者利用縮址隱藏網址，中間應是垃圾信發送者為了分析及計數用的中繼站點，最後再導到 youtube.com，而當使用者看到此影音網站上分享的影片時，雖然看似是普通的電視節目影片，但其實已經算是看到廣告了。

除了商業廣告信之外，本季收集到較特殊的廣告信，如圖：

圖 11. 某宗教學院廣告信

此為普通的仿 EDM 而成的廣告信，應是為了增加知名度以及報考人數而發的廣告信，這種在信中直接夾帶圖片的廣告信，相較其它廣告信沒有點開超連結後的資安疑慮，只要對信件本身作掃毒過濾即可，是相對較安全一點的信件，但也因為夾帶檔案，本身體積就大，若是數量一多，也是會佔據使用者的信箱空間，造成不小的麻煩，儘早清理為上。

● 中國常見垃圾信

到目前為止，簡體中文廣告信中各式廣告信的比例仍然沒有多大的改變，像是商城廣告信、商務課程廣告信、代開發票廣告信等，這類廣告信往往內容都差不多，但發散的數量卻不少，如圖：

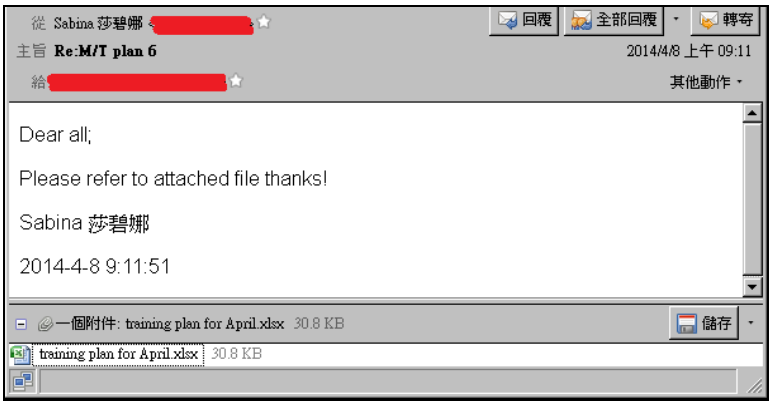


圖 12. 簡體中文課程廣告信之一

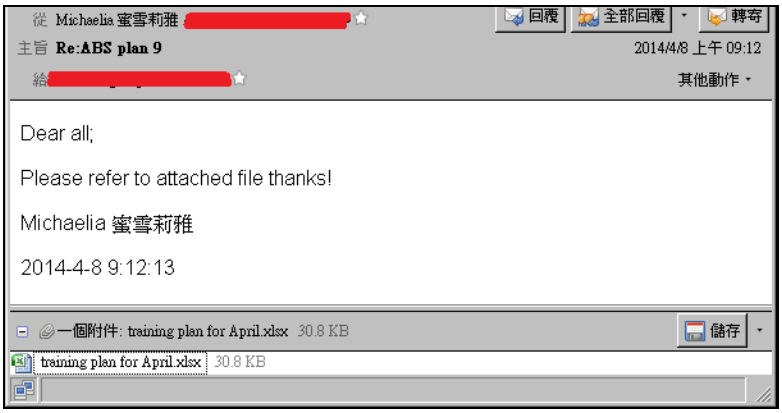


圖 13. 簡體中文課程廣告信之二

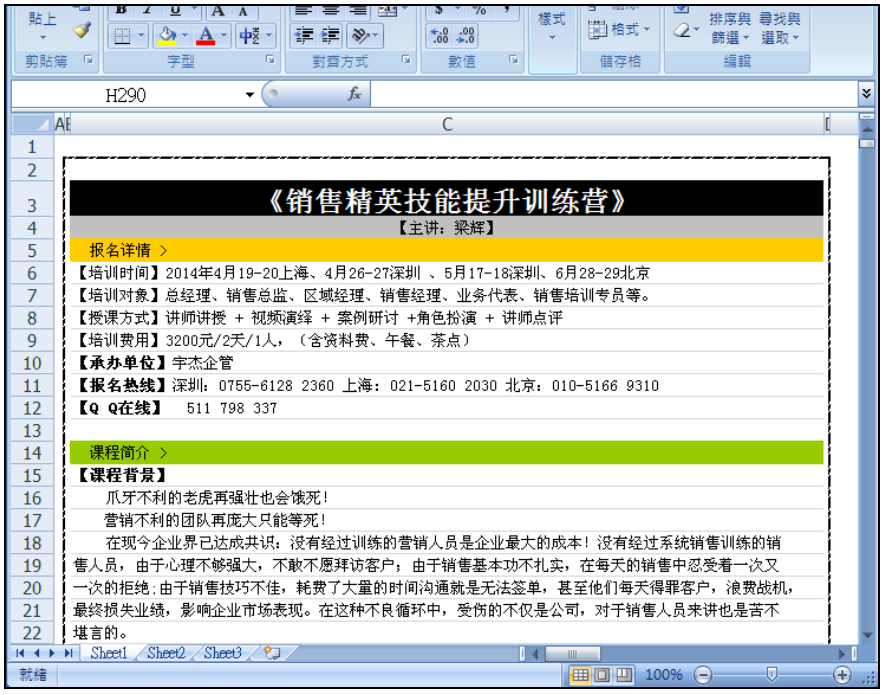


圖 14. 簡體中文課程廣告信附檔

上兩封信結構上有使用一些社交工程的手法，而內容只有些許不同，附檔更是一模一樣， 乍看之下似乎沒有什麼特徵能夠幫助攔截，但針對整封信來看，由於兩封信大幅度的相似，只要針對此點再配合垃圾信判斷機制，便應能順利為使用者攔截下來了。

圖 15. 香港網路商店廣告信

如圖，除了以往常見的廣告信外，本季中收集到一個廣告商品較特殊的仿 EDM 的廣告信，看來是隨著電影熱潮同時推出的周邊商品，觀察內容後，發現此廣告信內沒有對超連結作轉址的處理，可能是發送者沒有注意而未處理。

接著點選超連結查看：

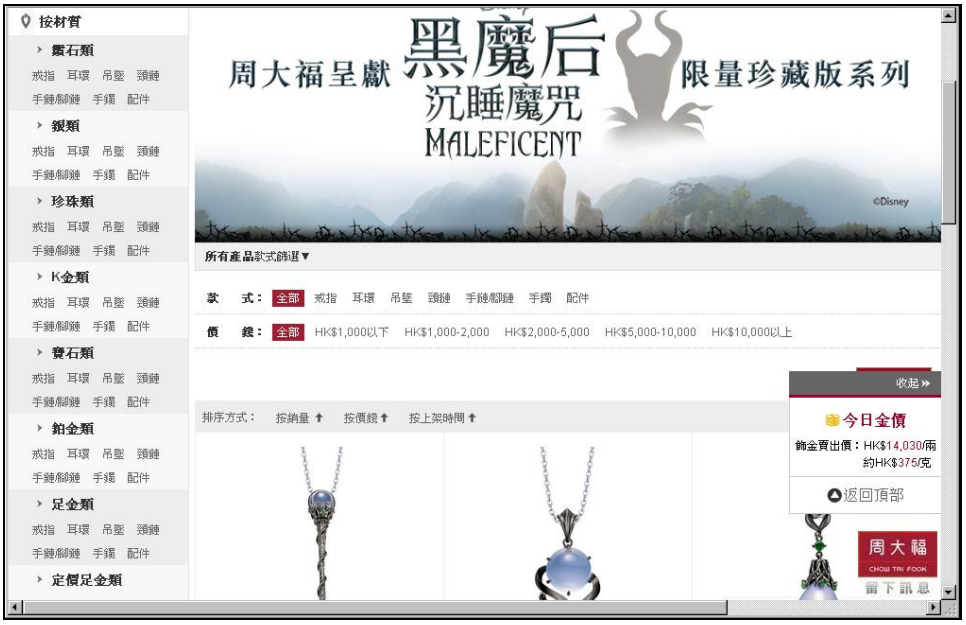


圖 16. 香港網路商店廣告信超連結頁面

看起來是不同於淘寶、天貓等網路商城的一般網路商店，且商品則都是較貴重的首飾類，而廣告信應是為配合促銷活動而發，此外看來沒有其它問題，只是普通廣告信件，加以攔截即可。

● 日本常見垃圾信

以往在日文廣告信方面，常見的都是博弈類廣告信、優惠詐騙信及色情廣告信等，如以下這封就是典型的賽馬廣告信：

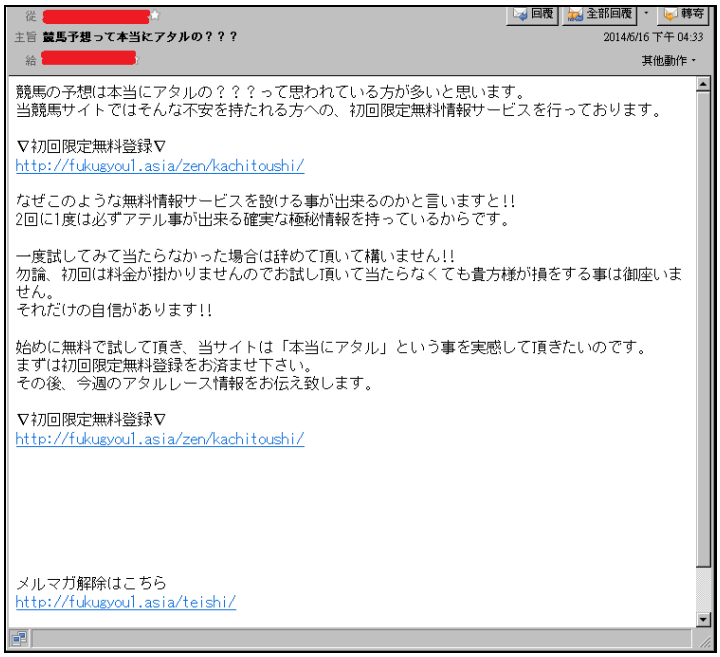


圖 17. 日文賽馬廣告信

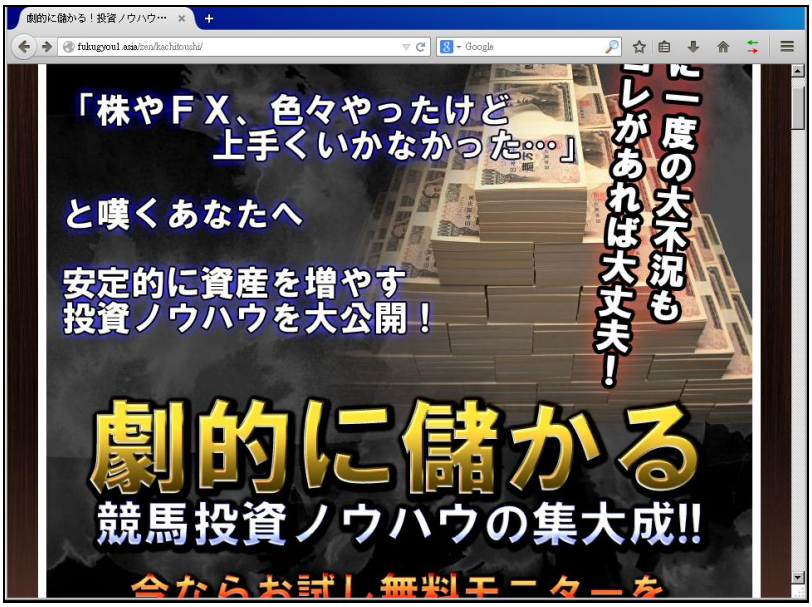


圖 18. 日文賽馬廣告信超連結點擊後畫面

就像大多數的廣告信，少不了用免費登錄來吸引使用者加入會員，但使用者登錄成為會員後，除了接踵而來的各種付費活動，麻煩的是加入會員時所填的資料，可能會被垃圾信發送者用來發送其他管道的廣告信，甚至是被用來假冒身分之類的， 可算是得不償失。

接著在信中除了免費登入的超連結外，還有退訂廣告信的超連結：

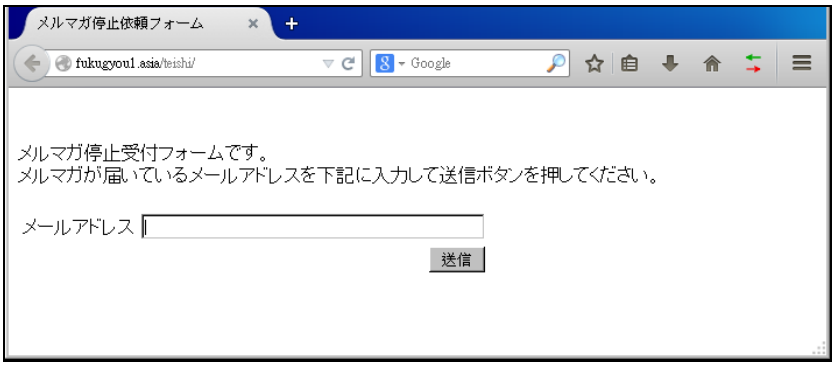


圖 19. 日文賽馬廣告信的退訂廣告信頁面

嘗試點開超連結後，看起來是確認要停止送信用的表格，不過這類不正當的廣告信的退訂功能可能非但沒有作用，反而還讓垃圾信發信者確定這個電子郵件位址的使用者會看信件的內容，進而發送更多廣告信件，造成使用者困擾。

除了常見的商業廣告信外，本季發現了一封較特殊的社會性廣告信：

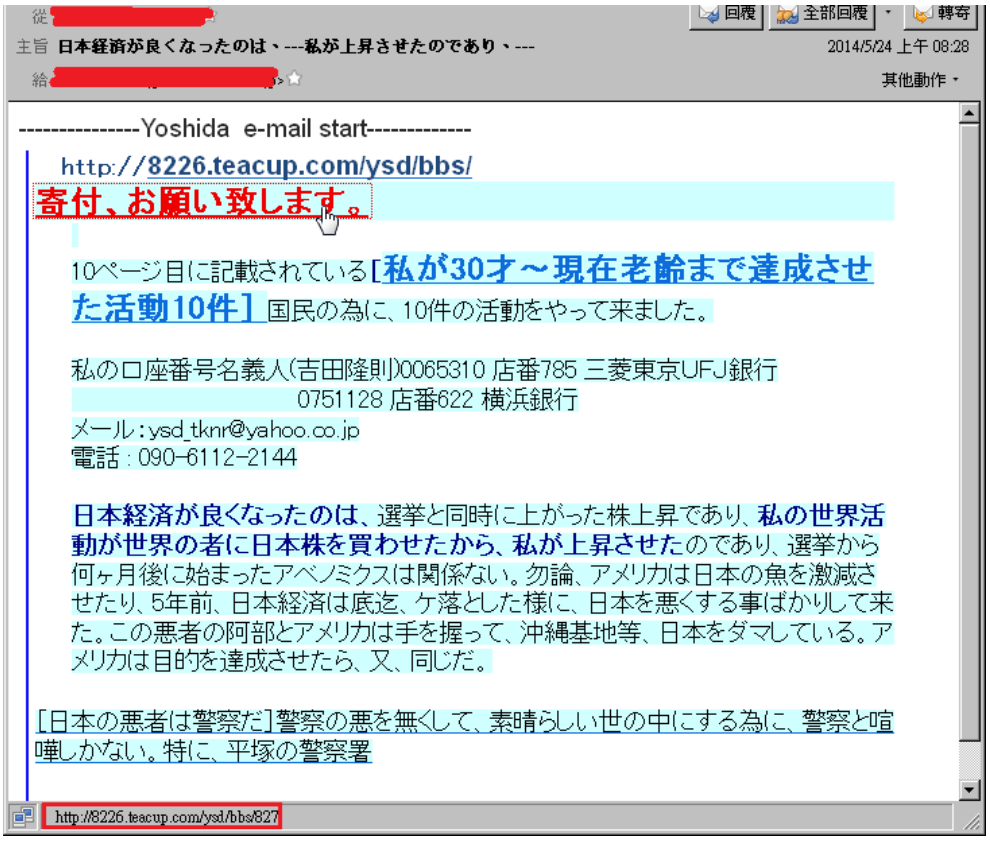


圖 20. 內容特殊的日文廣告信

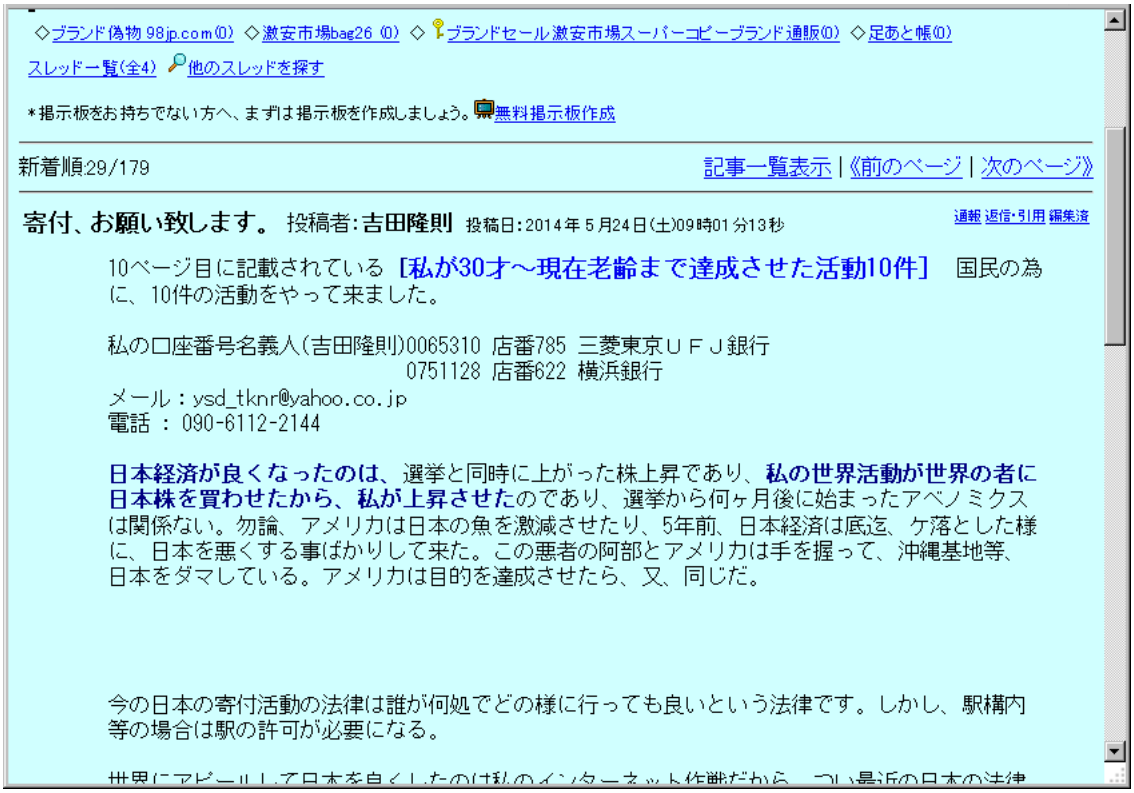


圖 21. 該日文廣告信的超連結頁面

由內容來看，應是想要探討個人和日本社會有關的議題，想藉由此類廣告文宣的發布，引起大眾迴響並募得款項。

Openfind 電子郵件威脅實驗室，特別從 2014 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 的雲端防護及誘餌帳號過濾攔截技術，在發現威脅的同時，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