Openfind™ Software Engineered for Growth™

Email Threats Analysis Report

Q3 2013

2013 第三季 Openfind 郵件威脅分析報告

目 錄

一、全球垃圾信發送來源地區

本季垃圾信來源國家的第一、二名分別為中國及日本，而美國與台灣則並列第三，依序佔整體垃圾信的 34.4% 、32.2% 與 3.9%。 與上一季相比，冠亞軍對調，形成拉鋸型態。此外，前兩名國家即占了66.6%垃圾郵件量，可見本季垃圾信來源非常集中。美國睽違兩季後，又再次躍入前三名寶座，與台灣並列本季第三，各占 3.9%。俄羅斯、及巴西則是本年度新進榜的來源國家各占 2.5% 及 1.5% 。

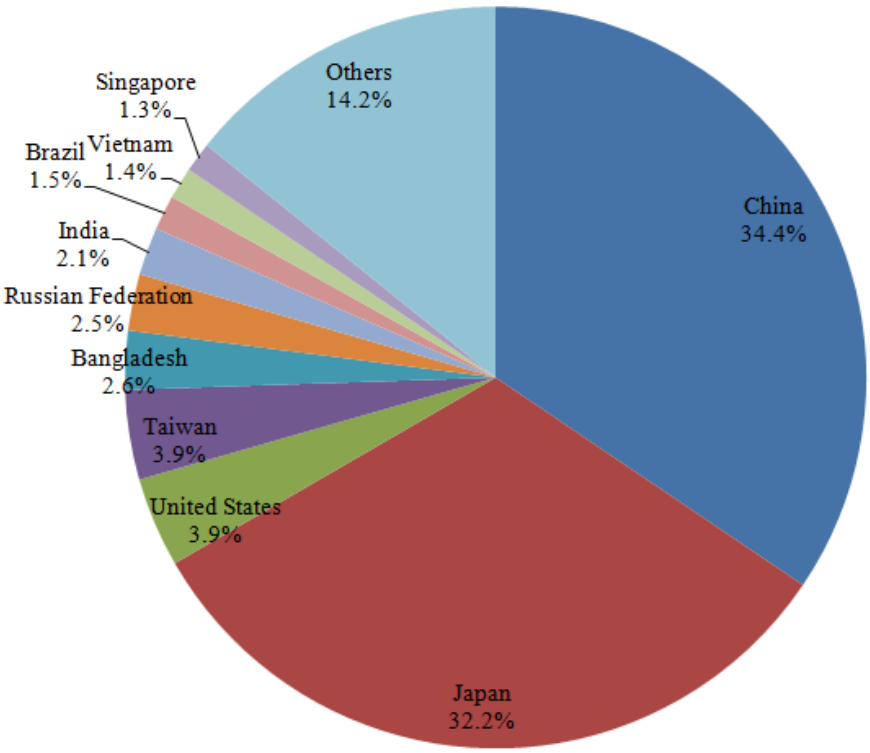


圖 1. 2013 年第三季垃圾信來源國家分布

細部觀察 7 月、8 月及 9 月來源比例，可發現中國在 8 月時，出現高於日本兩倍以上的垃圾信件量，在 9 月時雖然略微下降。日本於七月出現高峰，8、9 月在 21~23% 的位置徘徊。美國從 7 月~9 月成長兩倍左右，從 2.8% 上升至 5.7% ，整體季平均表現與台灣相似。

表 1. 2013 年第三季垃圾信來源國家比例

國家	7 月	8 月	9 月	季平均	季排名
中國	27.4%	46.2%	39.0%	34.4%	**1**
日本	41.5%	21.2%	23.0%	32.2%	**2**
美國	2.8%	4.2%	5.7%	3.9%	**3**
台灣	3.0%	5.6%	4.4%	3.9%	**3**
孟加拉	4.0%	0.9%	1.2%	2.6%	**5**
俄羅斯	2.3%	1.7%	3.3%	2.5%	**6**
印度	2.0%	1.6%	2.5%	2.1%	**7**
巴西	1.3%	1.8%	1.8%	1.5%	**8**

越南	1.4%	0.9%	1.6%	1.4%	**9**
新加坡	0.9%	3.3%	0.6%	1.3%	**10**
其他	13.4%	12.6%	16.9%	14.2%	

台灣目前在季排名位居第三，在 8、9 月的比例也有明顯提高。承襲上一季現象，美國與台灣的垃圾郵件來源比例總相差在 1 個百分比之內，且於本季同時擠入前三名的位置。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類別，顯示約有 27.2%的垃圾郵件網址會導引收件人前往商業之網頁。

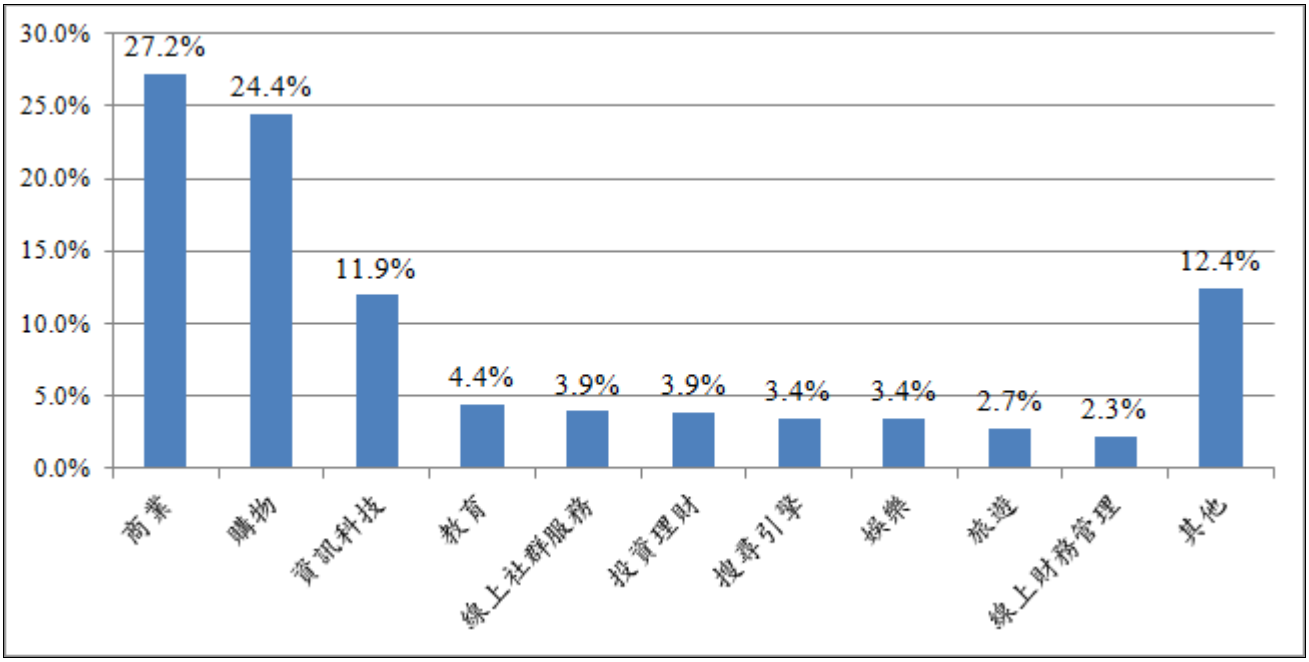


圖 2. 2013 年第三季垃圾信 URL 網頁內容分類

這一季來看與金流最直接相關的 URL 類別相當多，包含：商業、購物、投資理財、以及線上財務管理。畢業潮的影響力退去後，進入前十名的類別與前兩期相當類似。旅遊、投資與搜尋引擎皆再度進榜。教育的議題一直以來皆在榜上，本期更進入第 4 名，推測可能原因有二：業界人士一直不放棄重返校園的學習心態、以及適逢 9 月開學準備階段，故以教育相關的資訊，較易引起使用者關注。

表 2. 2013 年第二季與第三季 URL 網頁內容分類比較

	第二季		第三季	
排名	類別	比例	類別	比例
1	資訊科技	21.8%	商業	27.2%
2	線上社群服務	19.1%	購物	24.4%
3	購物	17.0%	資訊科技	11.9%
4	商業	9.2%	教育	4.4%
5	聯誼交友	5.5%	線上社群服務	3.9%
6	教育	5.5%	投資理財	3.9%
7	線上財務管理	5.3%	搜尋引擎	3.4%
8	線上音樂平台	2.2%	娛樂	3.4%
9	電子信箱服務	2.2%	旅遊	2.7%
10	求職網站	1.9%	線上財務管理	2.3%

觀察第二季與第三季 URL 網頁內容，可發現兩季前十大排名主題有些許不同，不僅商業排名躍升第一，購物的排名也提升了一個名次來到了第二。此外，本季也是首次前兩名即佔 50% 以上比例，顯示網路購物與各類金流活動正於網路世界蓬勃發展。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 IT 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，使用超連結及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. **貌似無害的郵件釣魚與轉址**
   在同樣以超連結為主要郵件攻擊手法的各式垃圾信中，以釣魚信件對使用者威脅最大，因為看似無害的超連結往往隱藏惡意危機與不知名威脅，若再加上駭客刻意的轉址或縮短 URL，使用者更是難以查覺。若使用者不慎點入超連結，便得面臨各種資安風險，包含資訊外流、或是成為傀儡電腦等，影響層面重大。

2. **小心沒有動作的提交按鈕**
   具有威脅性的偽造頁面，通常都會模仿得唯妙唯肖。近期發現許多專門騙取郵件或是銀行帳號密碼的偽冒網頁，外觀跟真實網頁幾乎毫無差異，使用者請小心，當您在帳號密碼欄位任意輸入後按下提交按鈕，若您發現網頁並沒有任何變化，可能就要提高警覺。尤其是當您發現該按鈕引導的超連結位置與目標網站不相關時，此時潛藏的風險程度越高。

3. **以熱門時事或社會新聞做為廣告郵件主題**
   垃圾信的發布，主要是為了吸引收件人點選，而在這一季當中，我們發現有越來越多的垃圾信會利用熱門時事或社會新聞做為噱頭，以「行銷加值服務」、「你有困難我幫你」或是「告知大眾事情真相」的教導方式，誘人點閱該廣告郵件。

四、垃圾信樣本詳細說明

延續上一章提過的「小心沒有動作的提交按鈕」垃圾信發布模式，本季中觀察到的釣魚信件，就有類似的情況，以下為駭客偽造的 mail2000 登入介面：

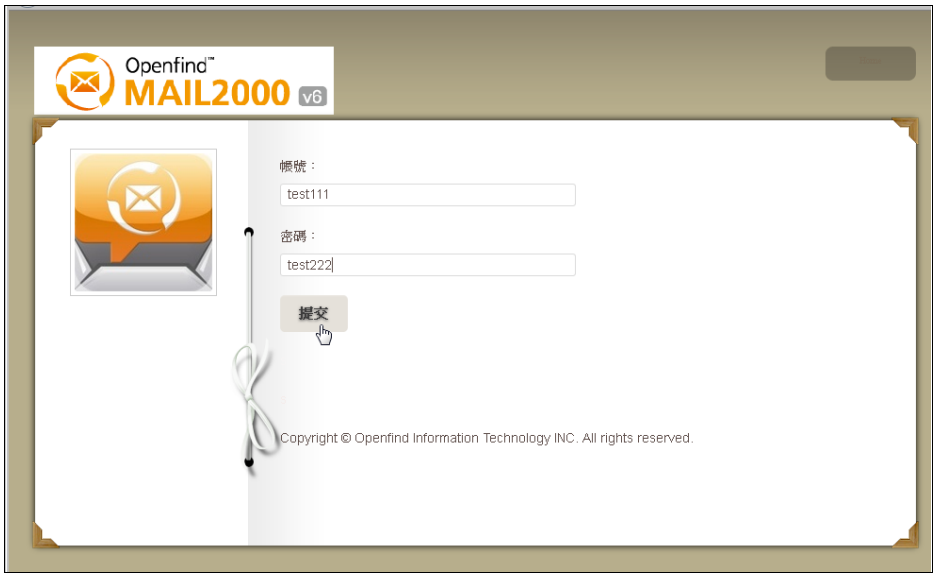


圖 3. 偽冒的 Mail2000 登入頁面 – 填入帳密頁面

當我們試著填入帳號及密碼時，發現密碼竟然是以明文的方式，而非以常見的「*****」代表使用者填入的密碼。

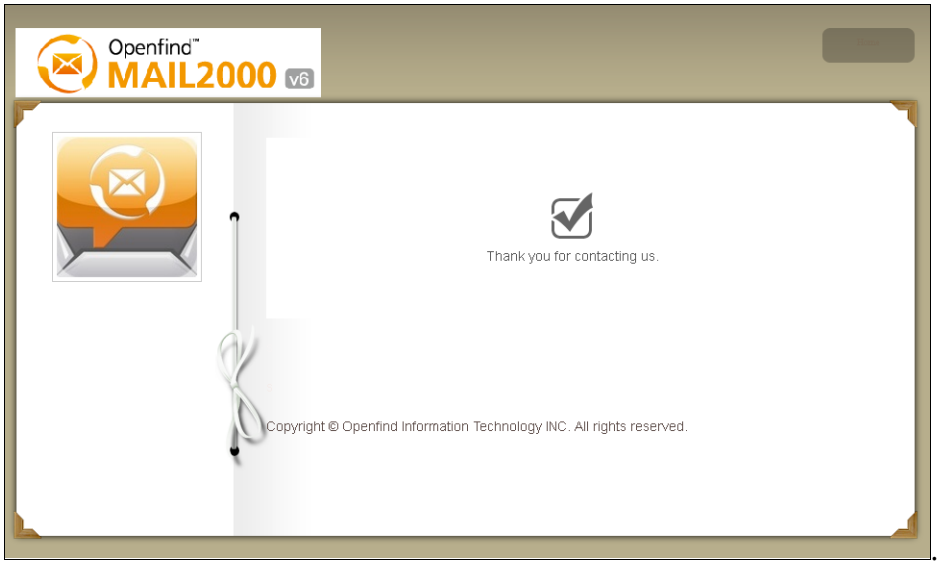


圖 4. 偽冒的 Mail2000 登入頁面 – 提交帳密後

最重要的是，當我們按下提交鈕後，可能是製作者不想在伺服器上留下連線記錄或其它原因，該頁面沒有轉址到真正的某政府單位網路信箱登入頁面，而是留在原址，使用者請特別小心此類按下按鈕後，毫無回應的網頁。

一樣的情形不只發生在台灣，在其他地區也可看到類似的手法，如下圖為某郵件服務的帳號申請畫面，一樣是密碼欄位以明文顯示，且點選提交後，畫面並未導入到其他畫面，而是留在原址：

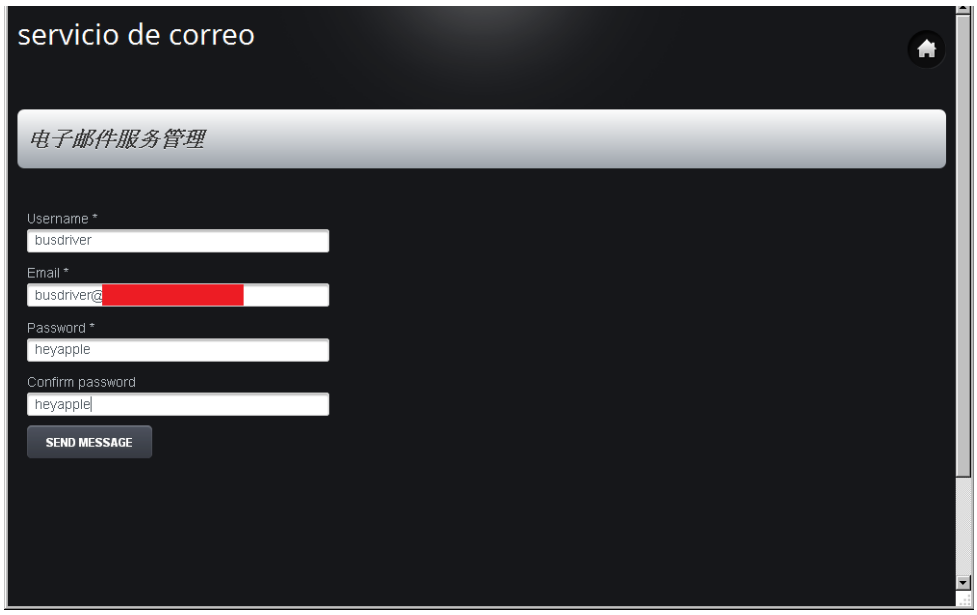


圖 5. 偽冒的郵件服務註冊頁面 – 填入帳密頁面

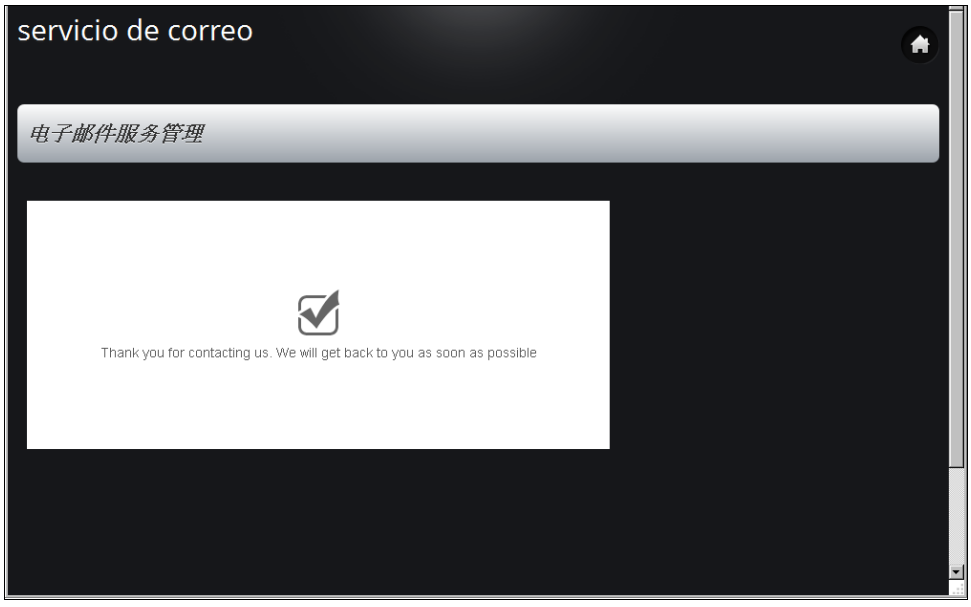


圖 6. 偽冒的郵件服務註冊頁面 – 提交帳密後

初步看過釣魚網頁可能會引導我們前往的陷阱頁面、並了解到使用者可以簡單測試頁面風險的幾個小秘訣後，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

搭著最近幾個月在台灣相當熱門的黃色小鴨流行風潮，有的廣告信網站也搭配小鴨商品進行推銷，如下面這個例子：

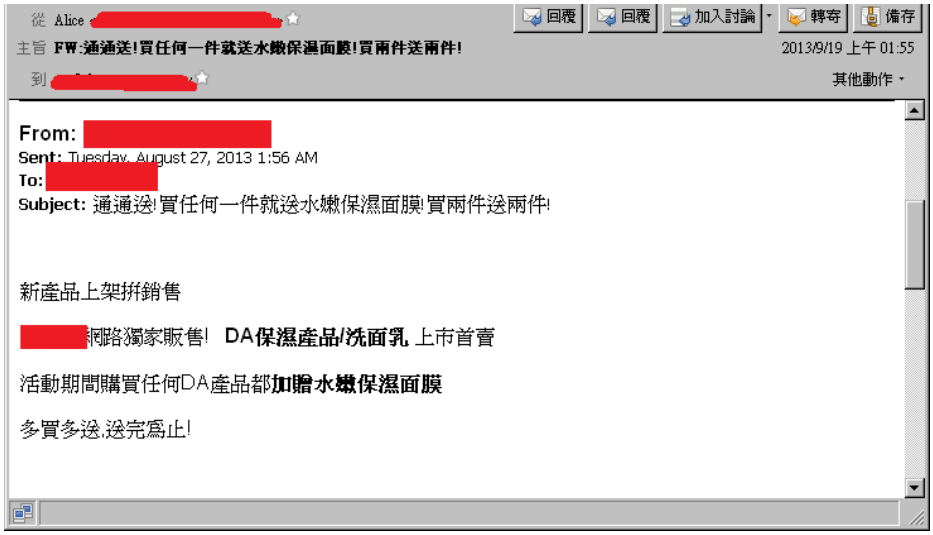


圖 7. 保養品推銷廣告信

圖 8. 保養品推銷廣告信目標網站

信件內容是普通的推銷廣告信，但在目標網站中有搭配小鴨商品作贈品當作促銷手法，增加銷售機會。另外，除了販賣一般商品的廣告信，像是非法藥品、盜版光碟或一般日常用具之外，具有服務性質的商業廣告信種類也越來越多，比如下面這一例子：

圖 9. 房屋修繕廣告信

開頭就附有聯絡方式，沒有其它華麗的廣告詞，且用條列式的說明特點，非常直接的廣告信，若是有需要該服務的收件者，可能真的會跟該工程行聯絡。

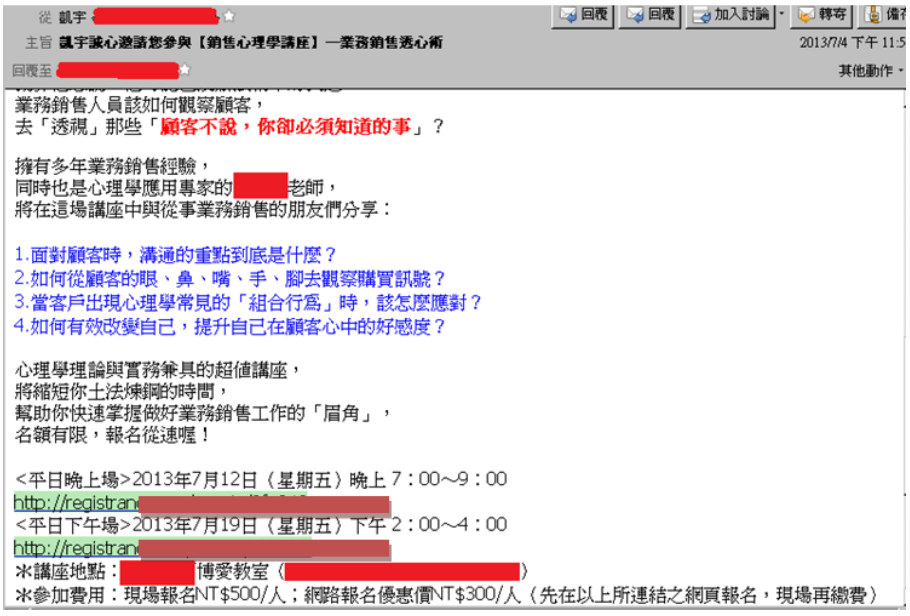


圖 10. 商務講座廣告信

上圖為針對從事銷售服務的商業人士的課程廣告信，但以往可能只是普通的銷售技巧研習班，現在則變化到多了講座型式的課程，而且講師還可能小有知名度。

除了以上較特別的廣告信例子，以往常見的一般廣告信也仍是不停的發送，如下這一封借貸廣告信：

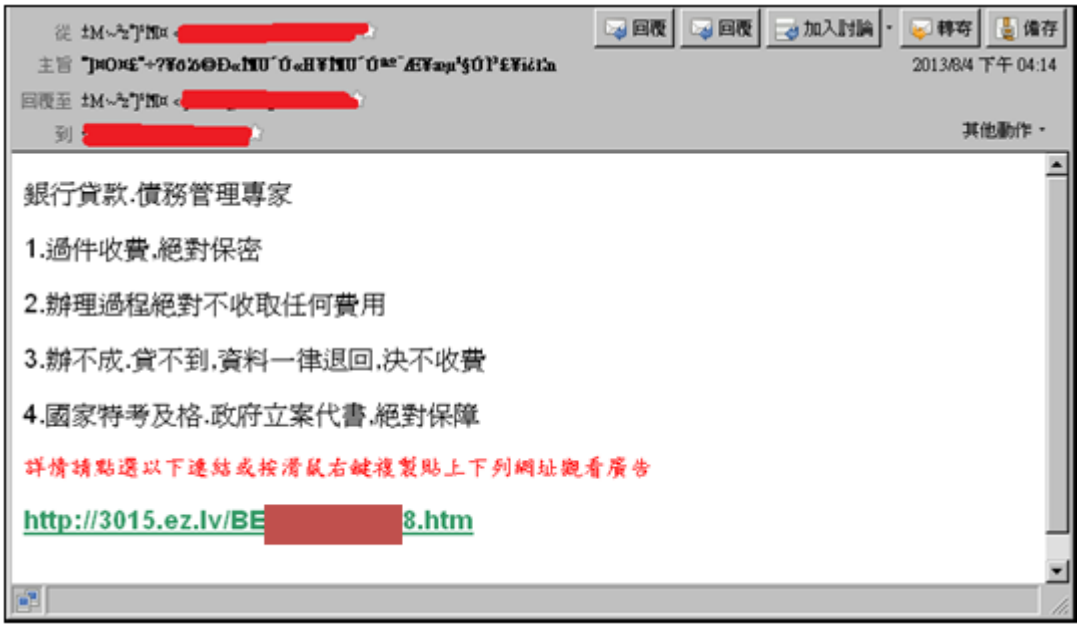


圖 11. 金融借貸廣告信

圖 12. 金融借貸廣告信網站頁面

雖然業者在信中和網站上皆提出保證，說無論如何就不收費用，或是政府立案絕對保障之類的，但這類廣告信和網站往往最是危險，若是收件者輕易提供個資，很有可能面臨資訊安全等相關為協。

● 中國常見垃圾信發送模式

在簡體中文廣告信方面，和以往一樣，廣告信內容仍多是網路商店廣告、代開發票廣告、商務課程廣告等等，如下這一封商務課程廣告信：

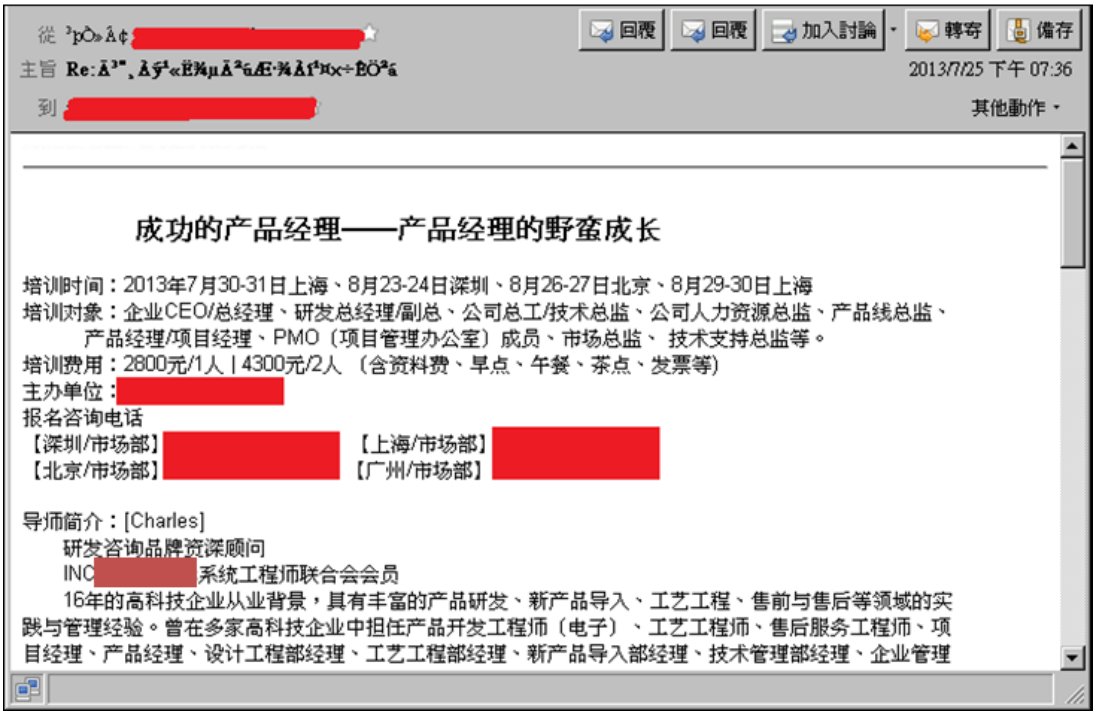


圖 13. 常見的簡體中文商務課程廣告信

和以往的商務課程廣告信一起比較起來，發現廣告信本身大多只在內文、附檔或圖片等處做變化。而其他商品的廣告信變化就稍微多了點，像是以往出現的類 EDM 廣告信，或是利用第三方網站的通知信作為廣告詞的媒介等等，廣告目標變化也多，如下這一例：

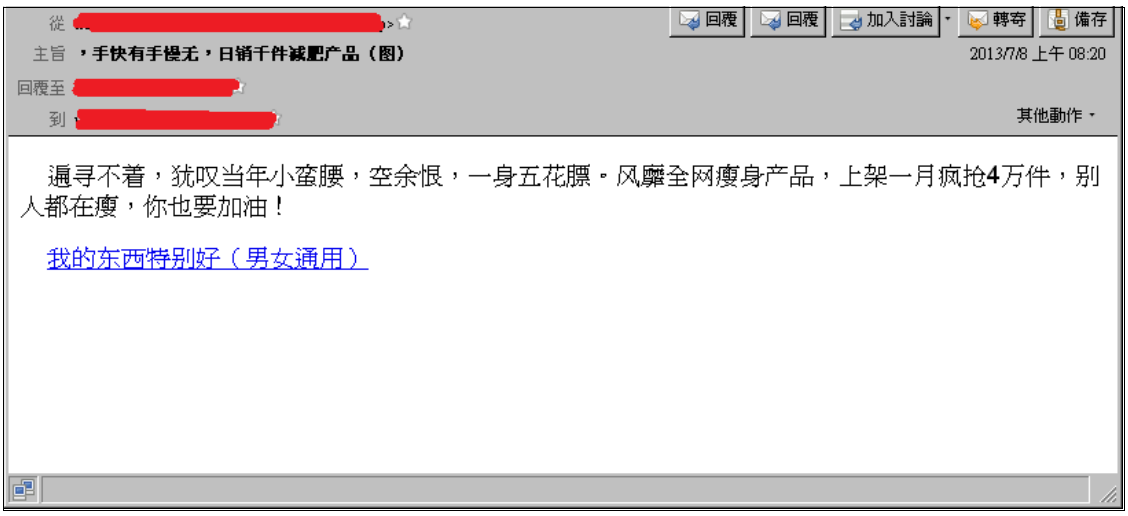


圖 14. 某簡體中文減肥藥廣告信

圖 15. 某簡體中文減肥藥廣告信網站頁面

以往大多是廣告日常用品和食物，但現在藥品廣告信的種類和數量也有變多的趨勢。

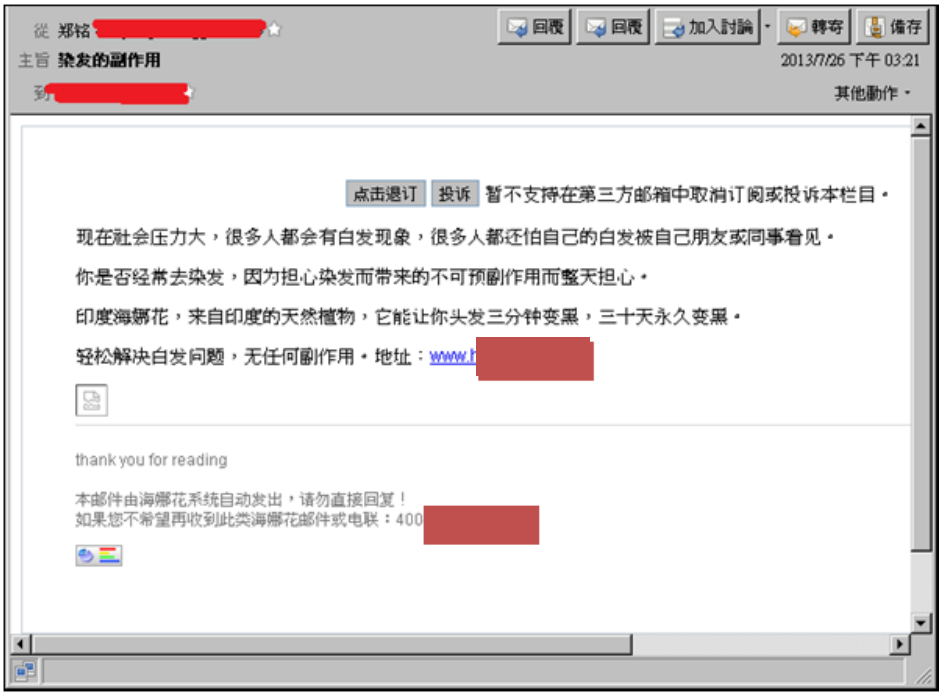


圖 16. 某簡體中文洗髮精廣告信

圖 17. 某簡體中文洗髮精廣告信網站頁面

如上圖例，這封廣告信作法雖然類似 EDM，在信中有含退訂或投訴的超連結，但是其實本質還是垃圾信，且信中的退訂或投訴的超連結不一定有用，搞不好還提醒垃圾信發送者，這個收件者帳號不但有人在使用，而且還會看信，反而以後收到更多的垃圾信。

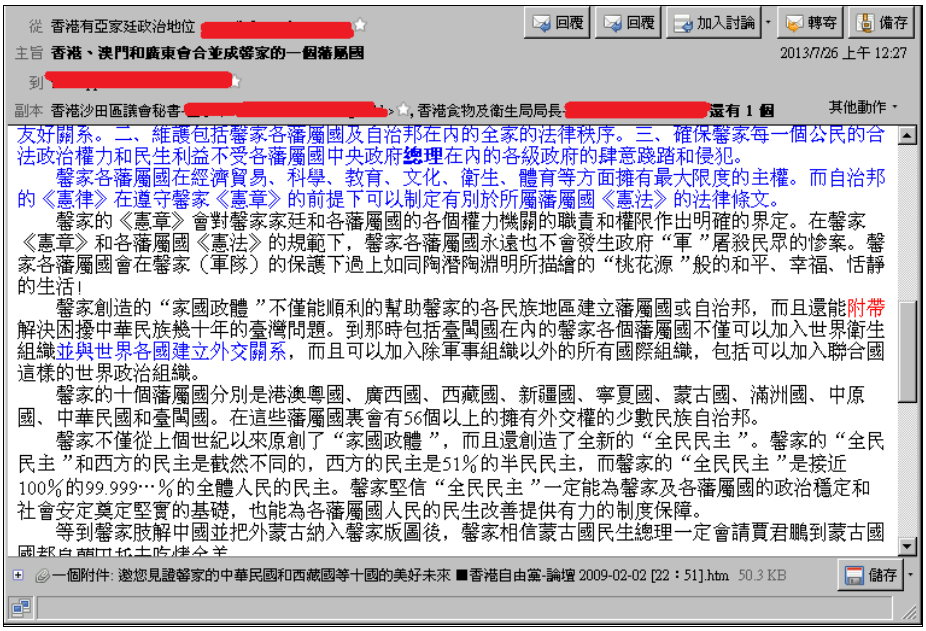


圖 18. 某政治廣告信

此外，最近的政治廣告信出現得也比之前稍微的頻繁，如上圖，可能為香港某團體所發的廣告信，雖內容可能較無資安危險，但常收到這類信件有可能因為敏感議題導致歧見。

● 日本常見垃圾信發送模式

在日文廣告信方面，延續常見日文電子郵件的特色，不管是 EDM 或垃圾信，其內容呈現大多都是純文字搭配文字圖案裝飾，少部分加上圖片，而在垃圾信數量上，仍以成人約會或色情服務業為大宗，接著是優惠詐騙信、博弈類廣告信等等，在中文廣告信常見的網路商店廣告信則是相對少見，如下這一案例：

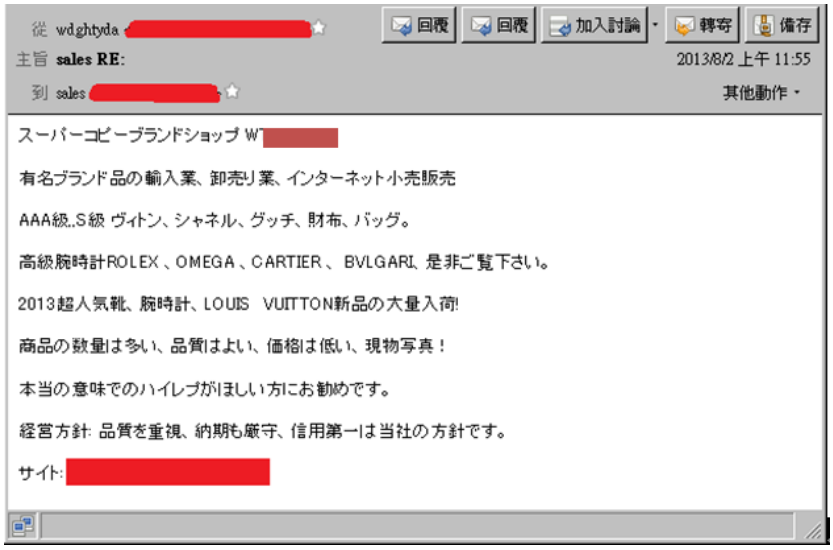
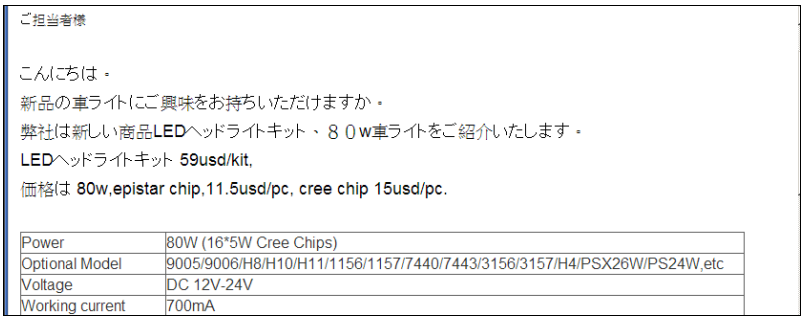


圖 19. 日文網路商店廣告信

圖 20. 日文網路商店廣告信網站頁面

此一例子中，信中的風格仍是同樣只有文字，但是其超連結則是利用第三方網站的短網址服務多作了一次轉址，由 http://126.am/wtobrand 轉址到 http://www.wtobrand.com/，也就是廣告目標網站。

另外還收集到少見的商業廣告信，也就是它廣告的對象可能是公司行號而不是一般使用者，如下圖所示：



ご担当者様

こんにちは。
新品の車ライトにご興味をお持ちいただけますか。
弊社は新しい商品LEDヘッドライトキット、８０w車ライトをご紹介いたします。
LEDヘッドライトキット 59usd/kit,
価格は 80w,epistar chip,11.5usd/pc, cree chip 15usd/pc.

Power	80W (16*5W Cree Chips)
Optional Model	9005/9006/H8/H10/H11/1156/1157/7440/7443/3156/3157/H4/PSX26W/PS24W,etc
Voltage	DC 12V-24V
Working current	700mA

圖 21. 日文商業廣告信之一

圖 22. 日文商業廣告信之二

文中記載著詳細的產品規格，雖然看起來是平凡無奇的廣告信，但這類含圖廣告信且以企業用戶為主的廣告信，在日本 SPAM 樣本來說相當少見。

此外，本季中也收集到了販賣日本 B-CAS 卡的廣告信：

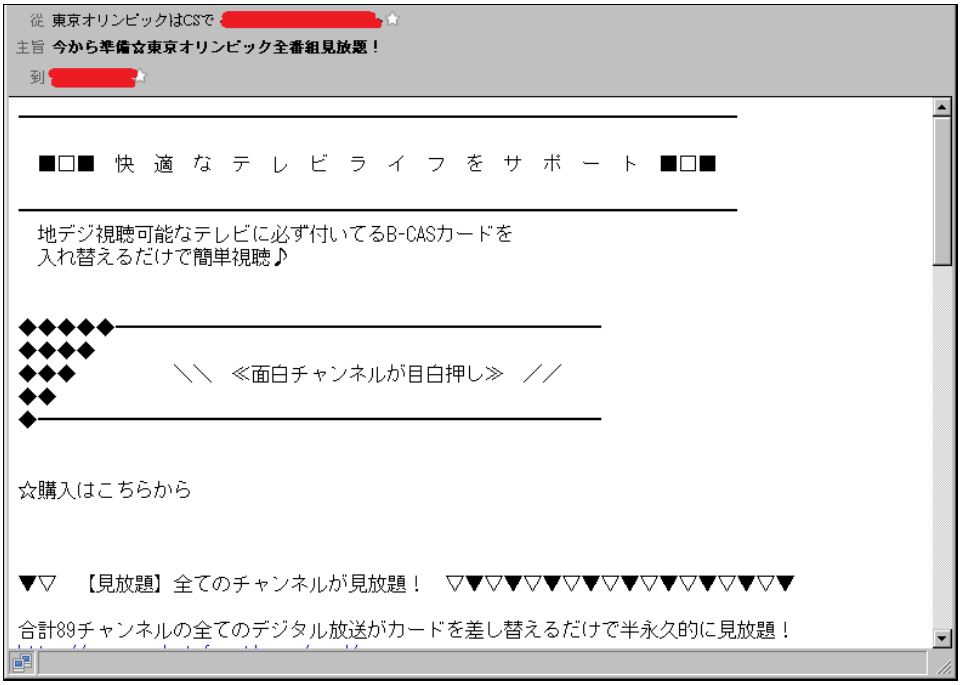


圖 23. 日本以時事為廣告信標題範例郵件

由於日本東京在日前取得 2020 奧運主辦資格，垃圾信發送者也利用此時事加入到廣告標題中，以增加點閱率，信中則就是一般的廣告文，再加上廣告網站的網址。

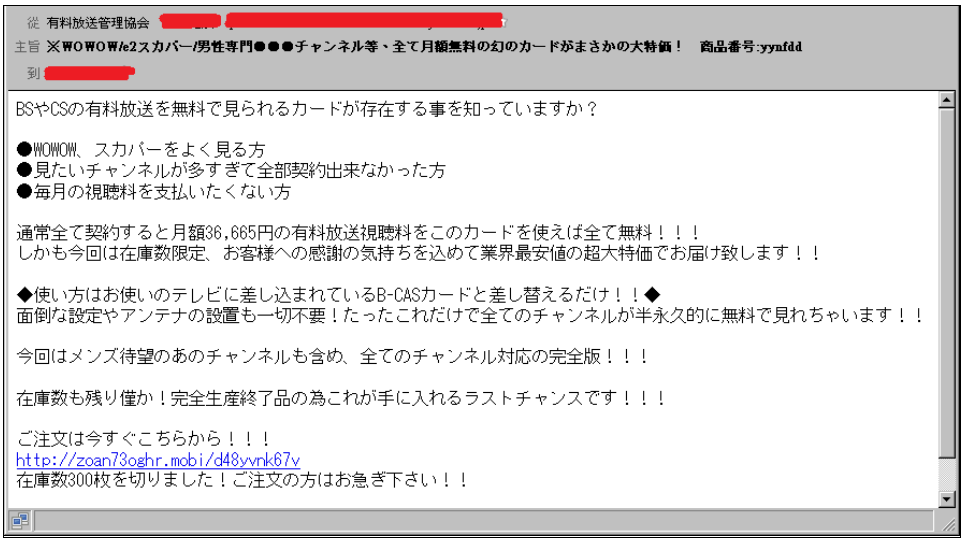


圖 24. 日本 B-CAS 卡廣告信

同樣也是 B-CAS 卡的廣告，但是信中廣告網站的網址則用垃圾信發送者申請的免洗網域，加以隱藏廣告網站本身，這種手法也是垃圾信發送者常用的手法之一。

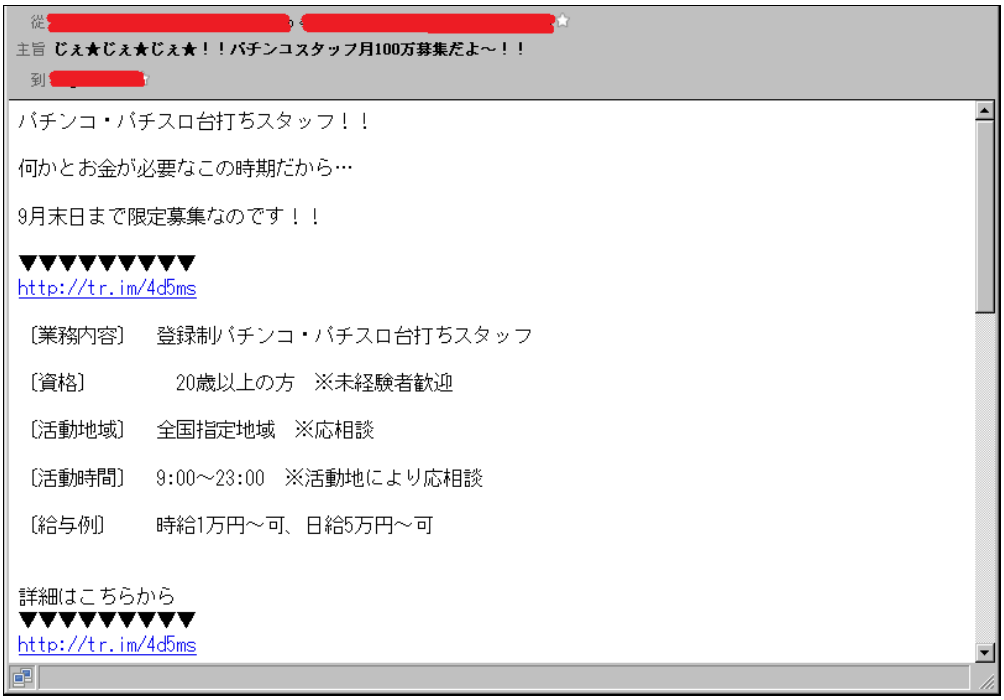


圖 25. 柏青哥詐騙廣告信

而上圖這個例子則本季收集到的柏青哥詐騙信，信中也有使用短網址服務來隱藏廣告網站網址，在實際測試後，發現是由 http://tr.im/4d5ms 轉址到 http://a-i-p.net/?pro_code=004，如下圖：

圖 26. 柏青哥詐騙廣告信網站頁面

連到網站後，發現有許多所謂「成功案例」的圖片，應是作為廣告之用，奇怪的是，其下方的文字也都是由圖片組成，可能是為規避搜尋引擎而作。

圖 27. 柏青哥詐騙廣告信線索之一

如上圖，由於覺得此網站相當可疑，便在搜尋引擎上搜尋，結果卻搜到了專門收集這種詐騙公司資訊的網站，發現果然是家詐騙公司，此外也有如下的清單：

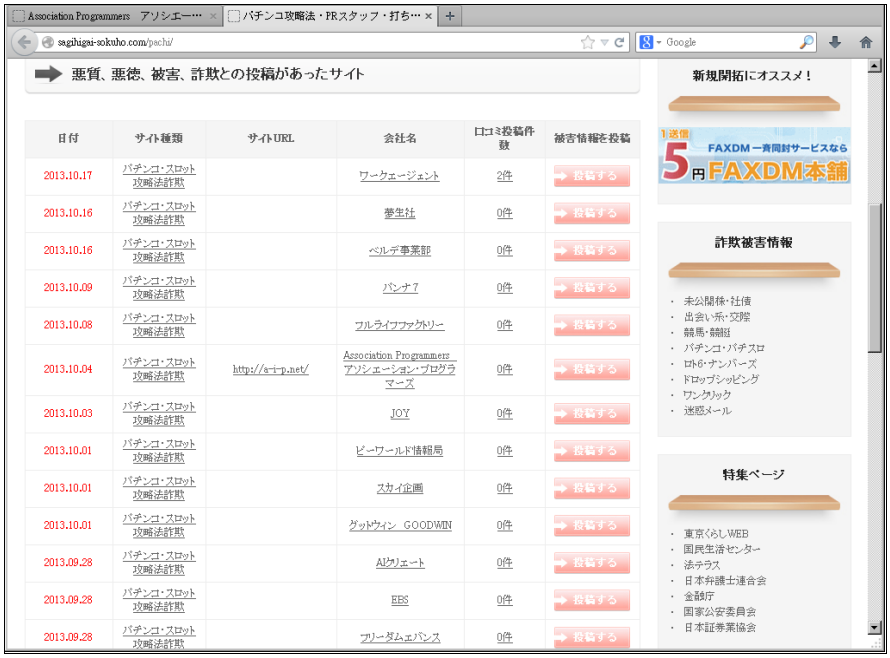


圖 28. 柏青哥詐騙廣告信線索之二

可看到在日本這類的詐騙公司真的是相當的多，每隔幾日便有人回報資訊，實在是多不勝數。建議使用者若是接觸到類似的日本柏青哥或賽馬攻略網站時，也可先在網路上搜尋是否有該公司資訊，以免一時中招，錢卻要不回來了。

Openfind 電子郵件威脅實驗室，特別從 2013 年第三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