Openfind™ Software Engineered for Growth™

Email Threats Analysis Report

Q4 2014

2014 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

2014 年第四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 55.6%、15.7%與 8.7%。在本季中，日本超越了台灣成為了第三名。與上季相比，前 4 名佔比有上升的趨勢。本季來源國家出現了上季未進榜的德國(0.7%)與印尼(0.6%)，分別位居本季第七名與第十名。值得注意的是，本季前三名即佔了垃圾信總量的 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。

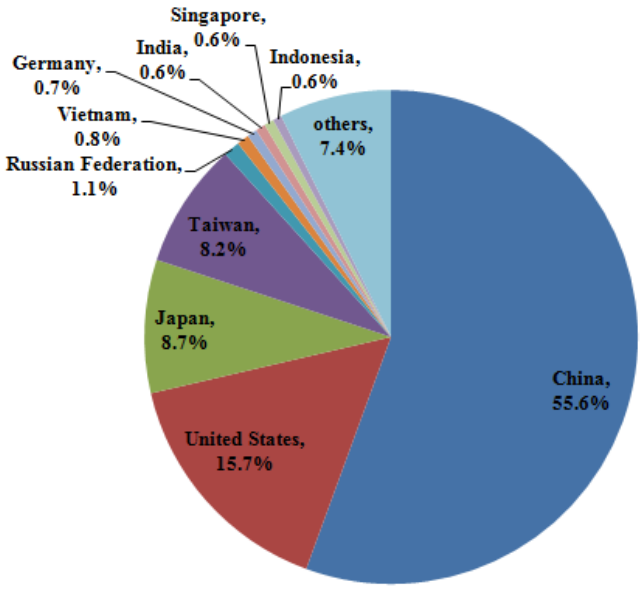
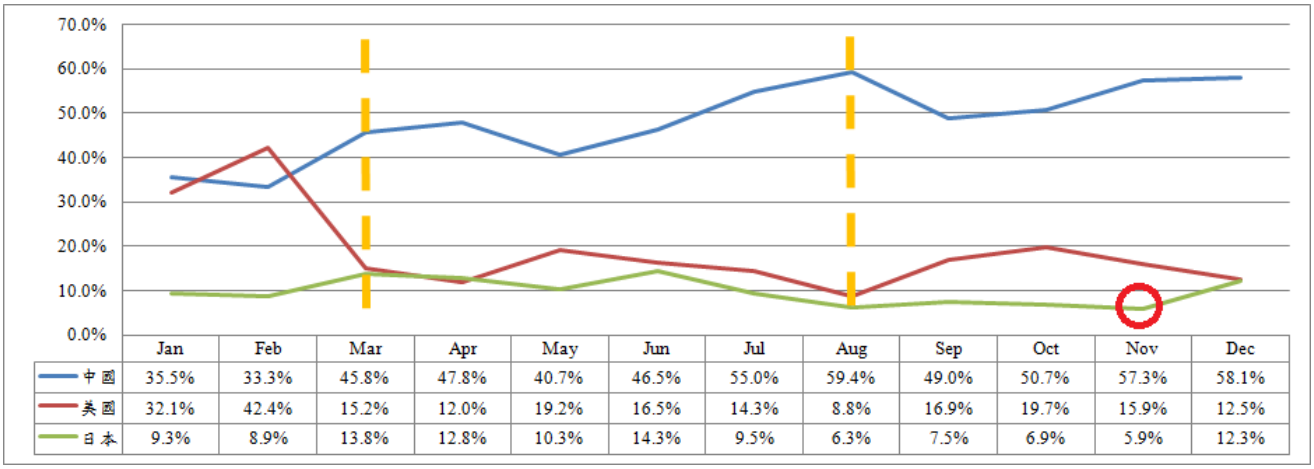


圖 1. 2014 年第四季垃圾信來源國家分布

延續第一季發現三月是屬於中國、美國、及日本地區持續走勢的分水嶺，第三季觀察到八月是個反彈月份。本季觀察下來，日本的反彈月份在十一月，在達到今年度新低的 5.9% 後，於十二月成長 1 倍以上之多。



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
中國	35.5%	33.3%	45.8%	47.8%	40.7%	46.5%	55.0%	59.4%	49.0%	50.7%	57.3%	58.1%
美國	32.1%	42.4%	15.2%	12.0%	19.2%	16.5%	14.3%	8.8%	16.9%	19.7%	15.9%	12.5%
日本	9.3%	8.9%	13.8%	12.8%	10.3%	14.3%	9.5%	6.3%	7.5%	6.9%	5.9%	12.3%

圖 2. 2014 年中國、美國及日本 2014 年佔比趨勢

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 5~6 成左右，但在 11 月份時，比起 10 月份，提升了 6.6%，有小幅上升的趨勢。日本則是在 12 月份時，比起 11 月

份成長了一倍以上，推測是 12 月份為日本節慶集中的月份，廣為宣傳活動及節慶消息而製造了不少垃圾信。

表 1. 2014 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	50.7%	57.3%	58.1%	55.6%	1
美國	19.7%	15.9%	12.5%	15.7%	2
日本	6.9%	5.9%	12.3%	8.7%	3
台灣	8.8%	9.6%	6.7%	8.2%	4
俄羅斯	1.3%	1.2%	0.8%	1.1%	5
越南	1.0%	0.8%	0.6%	0.8%	6
德國	0.7%	0.7%	0.6%	0.7%	7
印度	0.8%	0.6%	0.5%	0.6%	8
新加坡	0.9%	0.1%	0.8%	0.6%	9
印尼	0.7%	0.6%	0.4%	0.6%	10
其他	8.5%	7.3%	6.6%	7.4%	

台灣目前在本季排名位居第四，垃圾郵件來源比例與上季差不多，且相較於 11 月份，比例有下降的趨勢。日本在本季超過台灣成為第三名，佔比小幅提升 1%。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、本季垃圾郵件趨勢觀察

1. 以熱門議題為名，夾帶有病毒風險的檔案

此手法已盛行多時，但至今仍常被使用，顯示電子郵件用戶對於郵件安全意識尚未被完全建立。郵件內容可能是針對收件人設計的特定議題，也有可能是非針對性但於同時期相當熱門的議題，目的皆在於誘使收件人點擊。上當的收件者如果下載或執行了附檔，電腦可能會被植入木馬程式而被進一步利用。在此手法中，附檔的類型不僅限於 .exe 檔，一般常見的 .docx 及 .pptx 等文件檔案格式都有可能有病毒夾帶在其中。Openfind 在此建議收件者遇到夾帶有附檔的信件，不要進行點擊或下載，直接移除至垃圾桶即可。

2. 利用短網址服務一再轉址，避免被過濾

垃圾信發布者為了躲避被當成垃圾信而被過濾，會利用短網址服務，將垃圾信中轉址用的網站的 hostname 一再變換，當一個用久了，就換下一個，以期規避垃圾信件的過濾。

3. 垃圾信件的網址導引至具有表格的網站畫面

此類釣魚信件，大部分的目的為取得收信者的重要資訊，例如收信者的個人帳密、重要機敏資料等，但實際到了頁面，會發現整個介面非常簡陋，具警覺性的收信者就會察覺有異常而停止操作，因此威脅性較低。Openfind 在此建議收件者遇到有可以輸入資料的表格，不要填寫任何個人資料，直接關掉頁面即可。

三、垃圾信樣本收集介紹

以下我們將介紹並說明在本季中收集到的資安相關信件案例，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。

● 資安相關信件樣本

在本季中有收集到一件釣魚信件案例，是相當典型的電子郵件帳戶釣魚信：

圖 3. 電子郵件帳戶釣魚信

只要是釣魚信，基本上都是意欲取得收信者的某些重要資訊的，如上圖的這個例子便是用個人帳戶使用空間已達上限當幌子，要騙取收信者的個人帳密，不過在信中所提及的關於收信者或是服務提供者的資訊相當少，甚至沒有，因此可以進一步推測這封釣魚信應該是用於廣發給收信者名單的，相較於針對性較強的釣魚信(比如針對 Gmail、Yahoo mail 使用者)而言，攻擊性要少的多。

接著進一步觀察、測試：

圖 4. 釣魚信鏈結頁面

打開頁面查看，發現整個 UI 相當的陽春，使用者應有警覺性立刻察覺這是有問題的頁面，而不會繼續操作。

圖 5. 釣魚信鏈結頁面測試之一

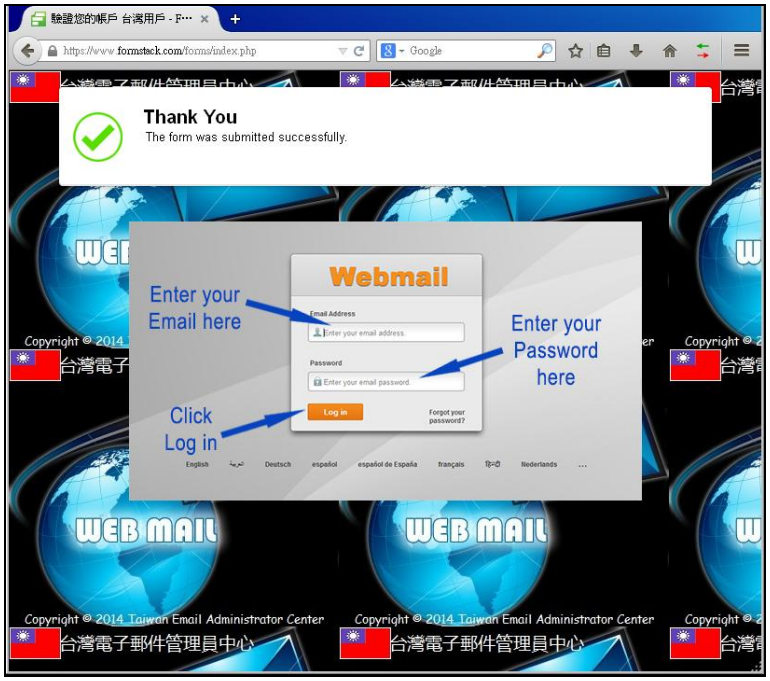


圖 6. 釣魚信鏈結頁面測試之二

如上圖，測試過程除了輸入資料到一個 form 之外，看起來沒有其他問題，但雖然從信件到網頁都很陽春，可是卻沒有什麼破綻可以找到發信者的資訊，在此例中發信者使用一般免費網頁郵件服務來發信外，且網頁本身也是網路上的免費表單服務，可見發信者有做過某種程度的準備，好避免自身資訊外流而被追查。

除了釣魚信件之外，本季也收集到一些病毒信件：

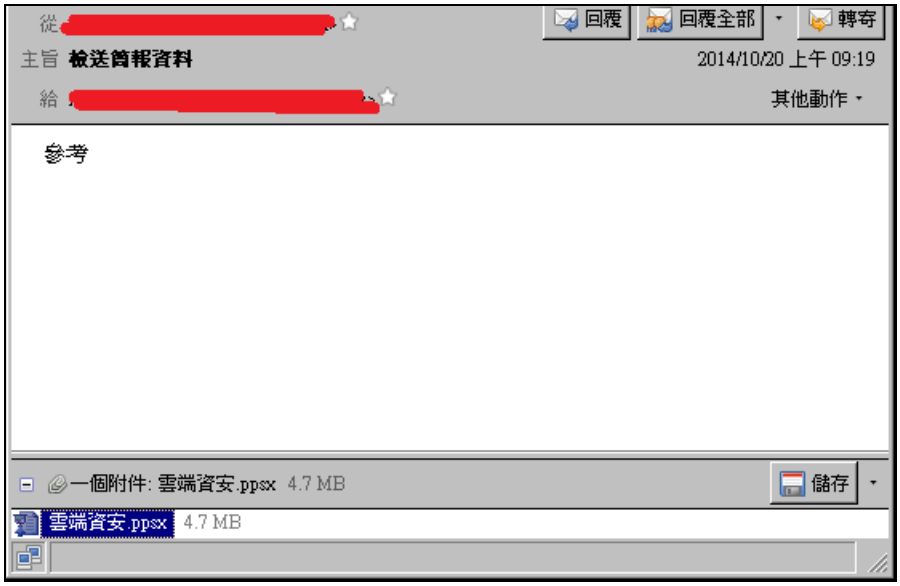


圖 7. 病毒信件之一

如圖，此例看起來只是普通的寄附檔的信件，但經過掃瞄之後，發現的確有木馬夾在附檔之中，若是使用者沒有察覺便開啟附檔瀏覽，那麼在瀏覽的過程中，電腦便已遭木馬感染了。

另外提醒使用者，現在有多種線上掃毒服務可利用來做掃描，比如使用本例中的附檔：

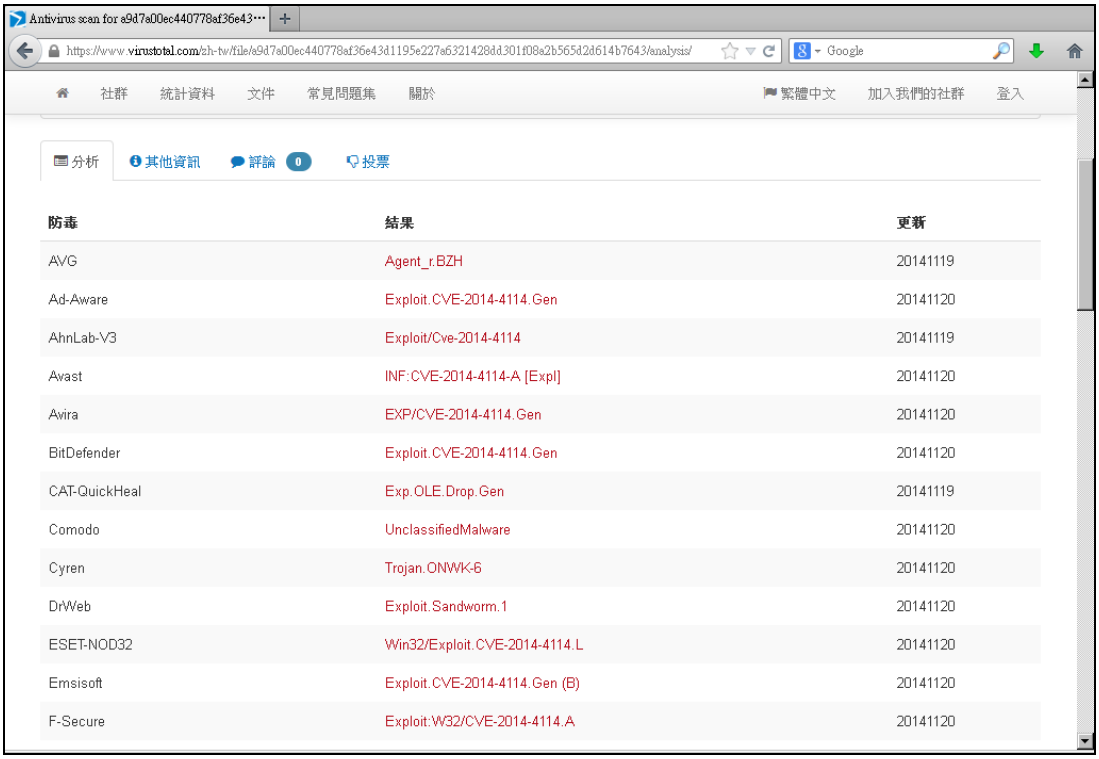


圖 8. 病毒信件附檔掃描測試

掃描後發現至少有數十個防毒引擎判斷有毒，此時應是可確定該檔案有資安問題了。而若覺得每次碰到疑似帶有資安風險的檔案時，都需要自行手動掃毒相當耗費人力的話，建議可以安裝如 MailGates 郵件防護系統此類郵件過濾機制，系統可自動偵測檔案，並將威脅隔離，維持郵件環境安全。

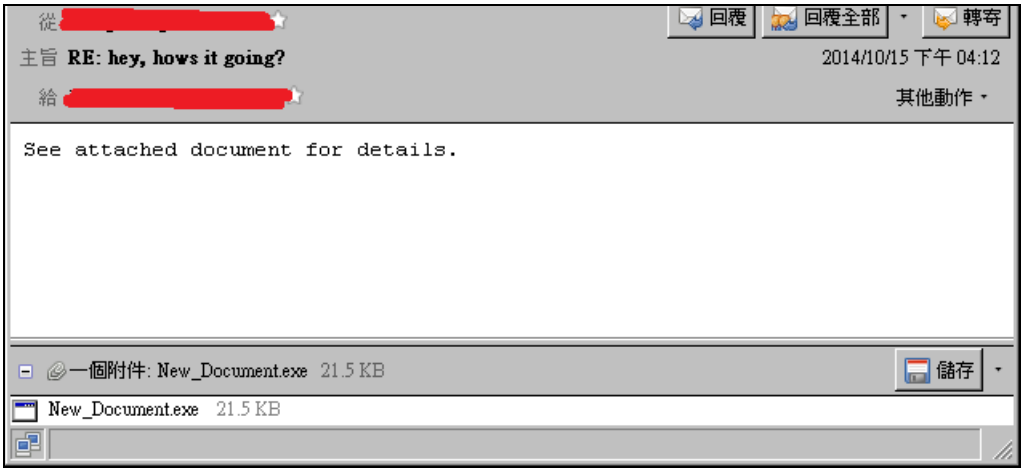


圖 9. 病毒信件之二

前一例病毒信件利用感染投影片來使收信者上當，而這一例卻毫不掩飾，直接將執行檔當作附檔寄給使用者，建議使用者遇到此類信件，連下載都不要，直接放到垃圾桶，以免誤觸而啟動惡意軟體。

● 台灣垃圾信樣本

本季收集到的垃圾信樣本廣告目標變化不大，仍以網路商城、進修課程、金融相關、成人相關等為主，不過在一些小地方上仍有持續改變，如：

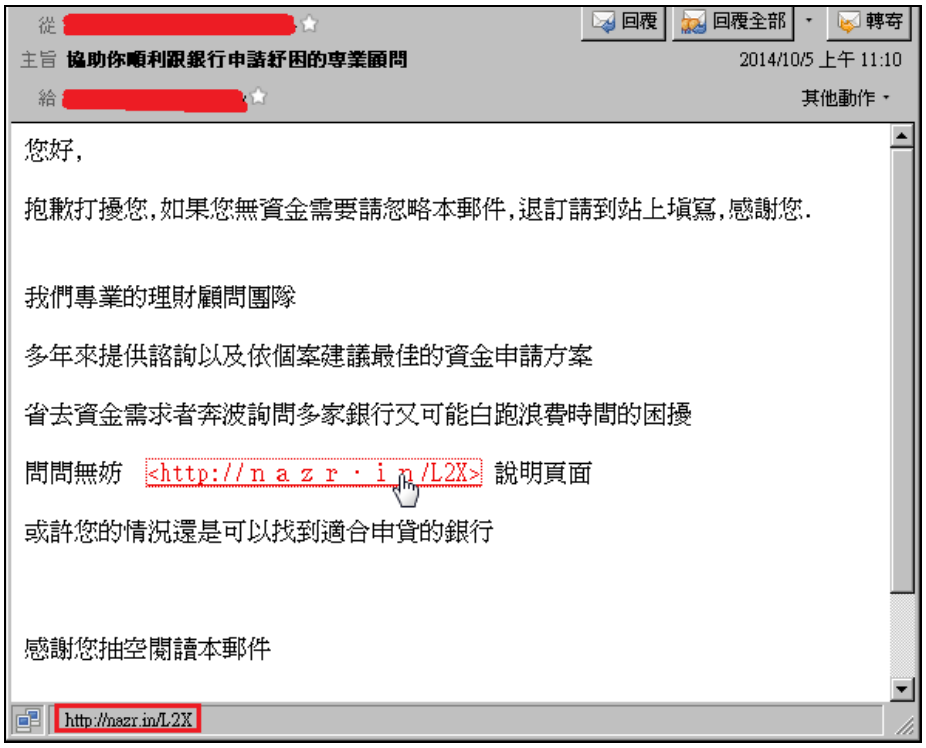


圖 10. 金融借貸廣告信

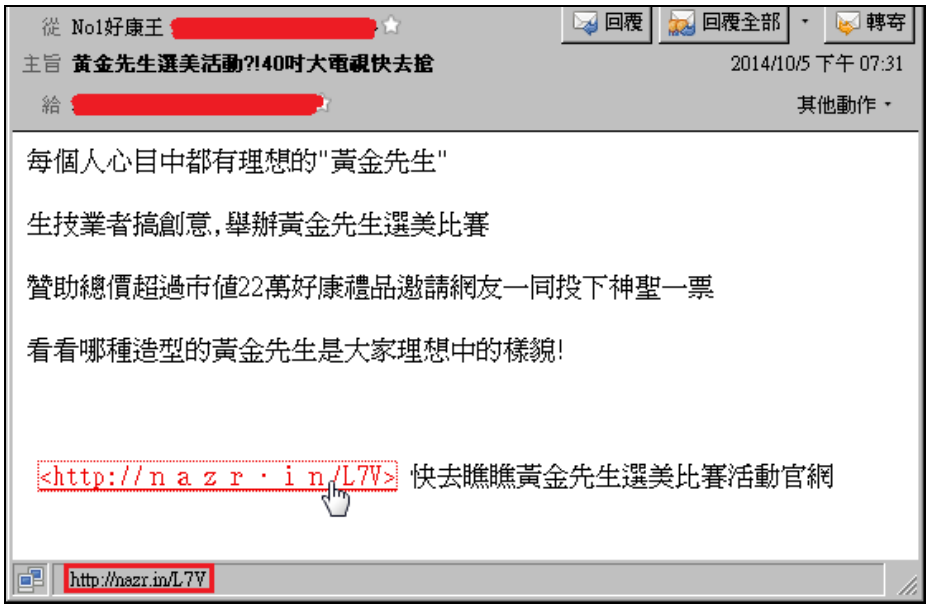


圖 11. 網路商城廣告信之一

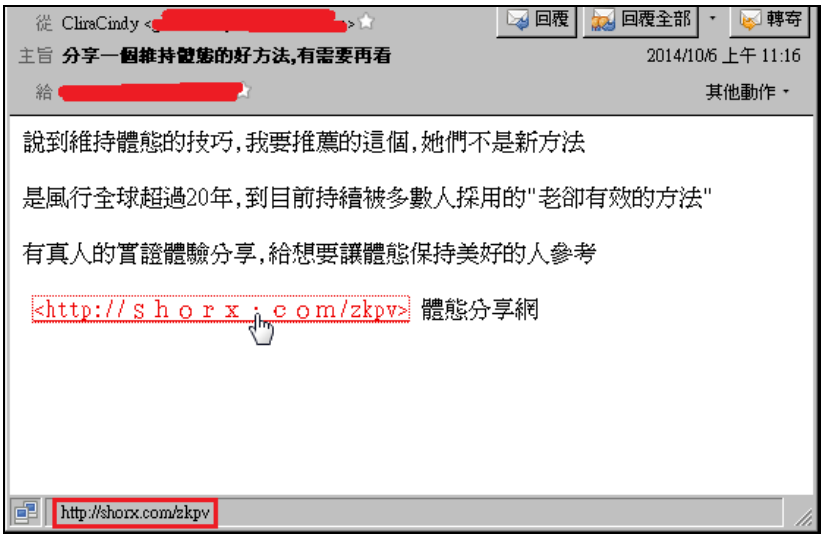


圖 12. 網路商城廣告信之二

上面幾例雖然都是普通的廣告信，但其用作超連結的短網址服務網站仍是會不定時的更新，比如以往常見的 0rz.tw、tinyurl.com 等，目前已相當少見，垃圾信發送者一再變換垃圾信中轉址用的網站的 host name，當一個用久了，就換下一個，以期規避垃圾信件的過濾。

● **中國垃圾信樣本**

在簡體中文廣告信方面，商務課程廣告信、代開發票廣告信還有商城廣告信等，仍然是層出不窮，例如：

圖 13. 簡體中文商務課程廣告信

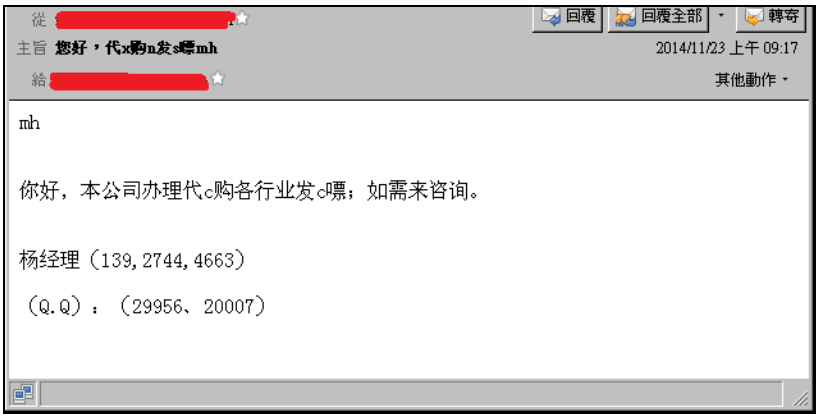


圖 14. 簡體中文代開發票廣告信

這一類廣告信其手法可能一直變動，比如使用附圖、附檔，不同的文字排列等等，但廣告目標都差不多，不過最近還有收集到其他商務型的廣告信：

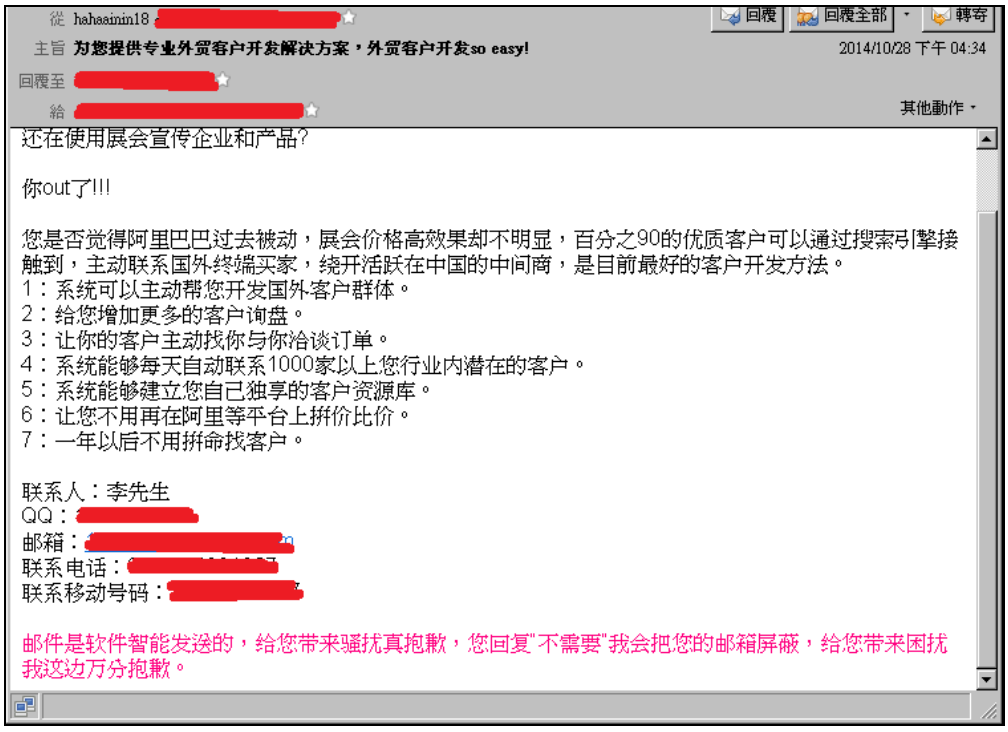


圖 15. 簡體中文商務系統廣告信

如上圖的系統廣告信，基本上算是 B2B 廣告信，系統開發者或擁有者向可能的商家散發廣告信，發信的數目可以控制在潛在買主名單下，而因為針對性較高，廣告達成率可能也比一般商品廣告信好，猜測此類廣告信可能會有增多的趨勢，值得觀察。

● 日本垃圾信樣本

本季中收集到的廣告信基本上仍以博弈類廣告信、優惠詐騙信及色情廣告信等為主，例如：

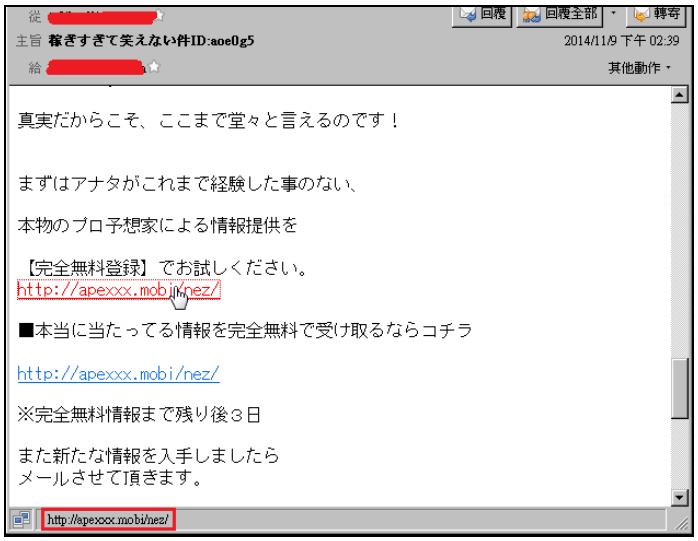


圖 16. 日文賽馬廣告信

圖 17. 日文賽馬廣告信超連結頁面

像上圖此例中的賽馬廣告信，或是其它博弈相關廣告信，仍然是日文廣告信中的大宗，只是依各個垃圾信發送者用的手法不同而有些許不同而已。

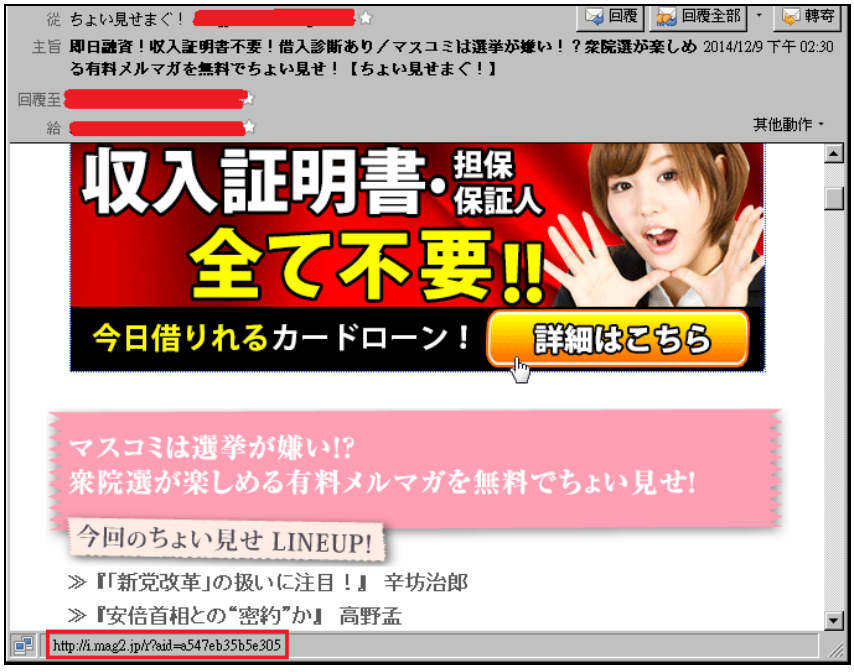


圖 18. 日文金融借貸廣告信

圖 19. 日文金融借貸廣告信超連結頁面

如上圖，本季中另外有收集到較少見的金融借貸廣告信，此例是利用專門寄送廣告信的網站服務來寄送，和一般常見的純文字廣告信相比，這例廣告信作的較像 EDM，且廣告目標頁面有連到正派經營的銀行網站，跟一般的大量散發的垃圾信相比感覺較安全，不過還是要建議使用者，當開啟沒有上過的網站時，最好先注意資安相關的問題，例如是否要輸入個人帳密，是否要安裝某些不知用處的瀏覽器外掛，或是也可以利用線上掃毒網站，來對有疑慮的網頁作掃描，畢竟若是真的中招要補救時，所花費的心力可是會比事先預防要來的多。

Openfind 電子郵件威脅實驗室，特別從 2014 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/。