# Email Threats Sample Report
# Q3 2012

Openfind™

## 垃圾信來源

根據 Openfind 電子郵件威脅實驗室於 2012 年 Q3 針對台灣、日本與中國三大地區的垃圾郵件的 IP 觀察，發現垃圾信來源國家的前三名分別為中國、印度與日本，依序占整體垃圾信的 23%、11%與 10%，第一名的中國與第二名的印度差異高達 12%。

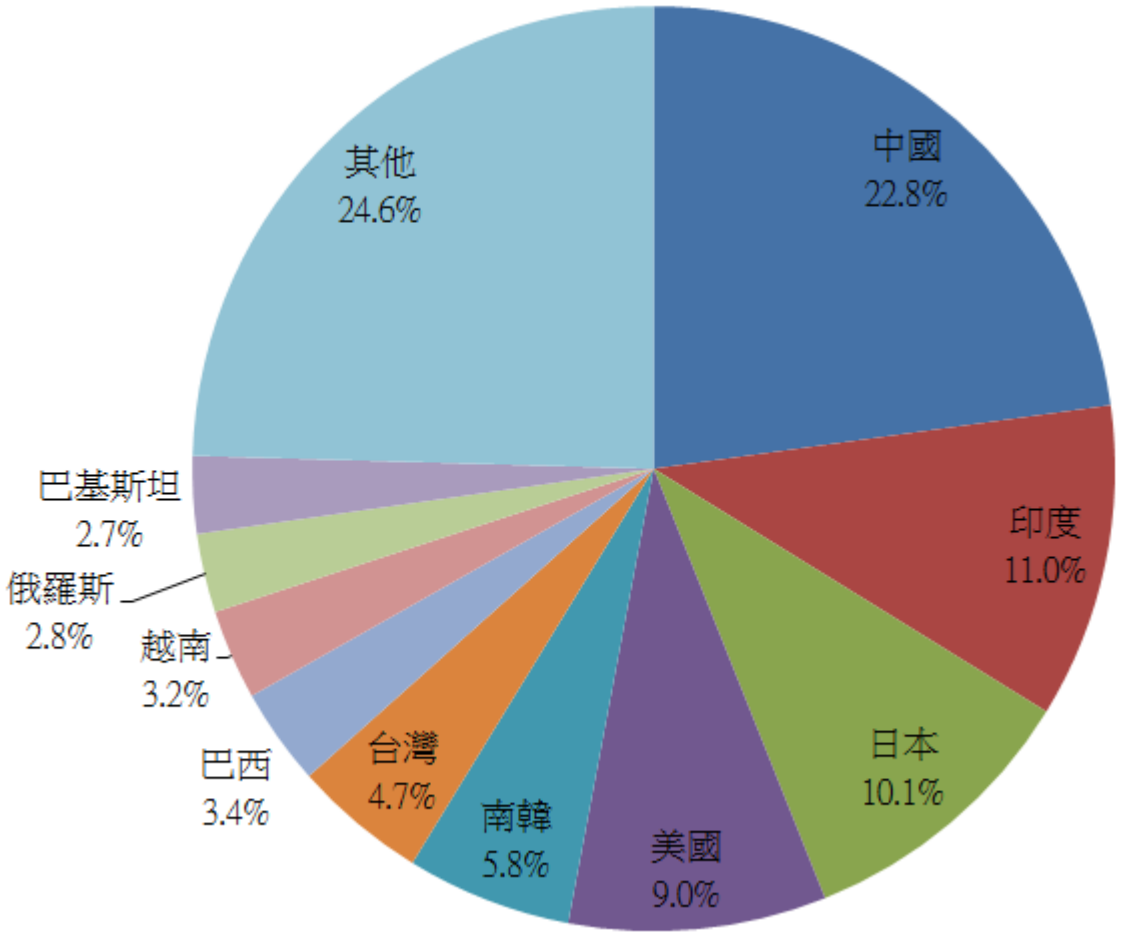



**圖 1. 垃圾信來源國家分布**

再從七、八與九月的詳細數據來看，可發現中國在八月與九月的垃圾信發送量突然飆高，印度與日本的數據相對下降，而其他國家則無太大差異。

**表 1. 垃圾信來源國家比例**

| 國家 | 七月 | 八月 | 九月 | 平均 |
|---|---|---|---|---|
| 中國 | 18.5% | 25.1% | 24.9% | **22.8%** |
| 印度 | 15.6% | 10.2% | 6.8% | **11.0%** |
| 日本 | 14.6% | 7.4% | 8.3% | **10.1%** |
| 美國 | 9.8% | 8.8% | 8.3% | **9.0%** |

| | | | | |
|---|---|---|---|---|
| 南韓 | 3.1% | 5.7% | 8.8% | **5.8%** |
| 台灣 | 3.2% | 5.5% | 5.4% | **4.7%** |
| 巴西 | 2.5% | 3.6% | 4.2% | **3.4%** |
| 越南 | 4.0% | 3.0% | 2.4% | **3.2%** |
| 俄羅斯 | 1.9% | 3.2% | 3.2% | **2.8%** |
| 巴基斯坦 | 5.8% | 1.5% | 0.7% | **2.7%** |
| 其他 | 20.9% | 25.9% | 27.0% | **24.6%** |

會造成此現象，可能的原因是垃圾信發送者透過殭屍網路或其他的跳板手法等種種的方式，將 IP 來源轉換至中國；但也有可能是因中國持續的經濟成長，造就許多人開始創業，這些剛起步的公司為了尋求業務開發的機會，而濫發許多廣告信。相信也許還有其他種種原因，雖然目前沒有明確的證據顯示狀況為何，但 Openfind 電子郵件威脅實驗室會持續觀察與監控，並在發現垃圾信威脅的第一時間內，透過雲端防護攔截技術，讓 MailGates 的用戶免除垃圾郵件的威脅。

此外值得一提的是台灣雖然只佔 5%（第六名），但也在前十名的排列中，且從七月的 3.2%後便攀升到 5.4%，此狀況也值得我們持續的觀察與監控。

## 垃圾信種類

本季需特別注意的駭客攻擊手法，主要是在信件外部連結的威脅上，此外排名前三的垃圾信種類如下表所列：

**表 2. 垃圾信總類排名**

| 排名 | 垃圾信種類 | 比例 |
|---|---|---|
| 1 | 透過轉址服務網站或其它手法間接轉址（Redirect） | 30.5% |
| 2 | 透過知名社群網站發送實為廣告信的通知信 | 13.8% |
| 3 | 內容未知的附檔 | 8.8% |

各種類的簡易說明如下：

1. **透過轉址服務網站或其它手法間接轉址（Redirect）**
   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，有些攻擊者自己也申請網路上的主機名稱，幫助作轉址及隱藏目標網站網址的功能，同時也好控制連結的可用性，這亦是垃圾郵件發送者慣用的手法之一。

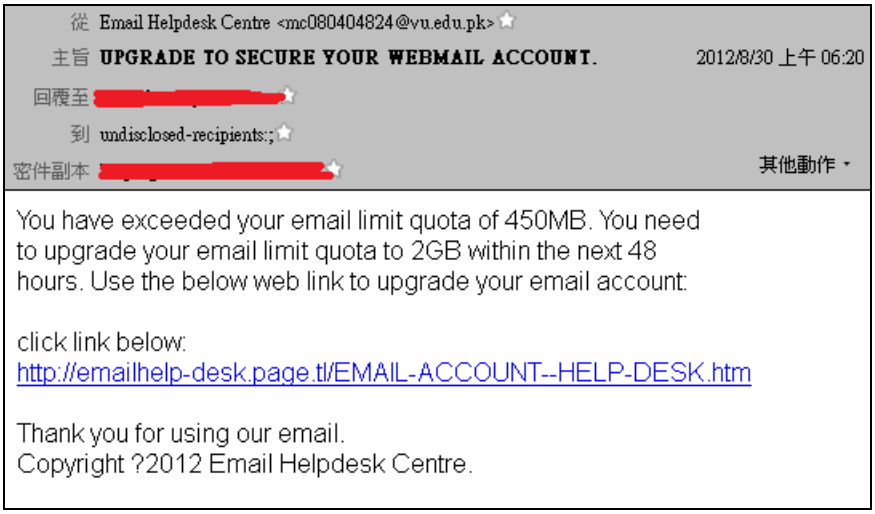
2. **透過知名社群網站發送實為廣告信的通知信**
   延續前季中觀察到藉由知名社群網站(Facebook、Google+ …等)發布廣告信的情況，本季中持續觀察到垃圾信發送者藉此發送垃圾信的例子，因此使用者在查看社群網站通知信時也須多加注意信中的超連結，以免誤觸發惡意軟體。

3. **內容未知的附檔**

   除了帶有超連結的垃圾信以外，本季中發現僅帶有附檔的垃圾信比率也上升了；此類垃圾信件通常利用諸如 word 文件檔或 winrar 壓縮檔等附檔夾帶廣告內容或是惡意軟體，因此面對帶有附檔的可疑信件時，最好儘量避免開啟附檔，以免中了附檔中的病毒或是木馬。

## 垃圾信樣本

和以往一樣，在獲得個資可能帶來的龐大利益上，駭客對於騙取使用者帳號密碼仍是樂此不疲，每隔一段時間便會有新方法出現，威脅使用者的個資安全，如下為一例釣魚信件：



從 Email Helpdesk Centre <mc080404824@vu.edu.pk>

主旨 **UPGRADE TO SECURE YOUR WEBMAIL ACCOUNT.** 2012/8/30 上午 06:20

回覆至 [redacted]

到 undisclosed-recipients:;

密件副本 [redacted] 其他動作

You have exceeded your email limit quota of 450MB. You need to upgrade your email limit quota to 2GB within the next 48 hours. Use the below web link to upgrade your email account:

click link below:
http://emailhelp-desk.page.tl/EMAIL-ACCOUNT--HELP-DESK.htm

Thank you for using our email.
Copyright ?2012 Email Helpdesk Centre.

**圖 2. 假冒電子郵件服務中心的釣魚信件**

在此例中，垃圾郵件發送者以信箱信件超出容量以及需升級信箱為由，想騙取使用者點選信裡的超連結以進行後續動作，在此處便可觀察到寄件者的網域為 vu.edu.pk，而其超連結的網域則為 emailhelp-desk.page.tl，兩個網域相差甚大，且連到網域 page.tl 時，又被重導向到 www.own-free-website.com，發現是一個可免費申請 homepage 的網站，至此釣魚信件的嫌疑又更大了。

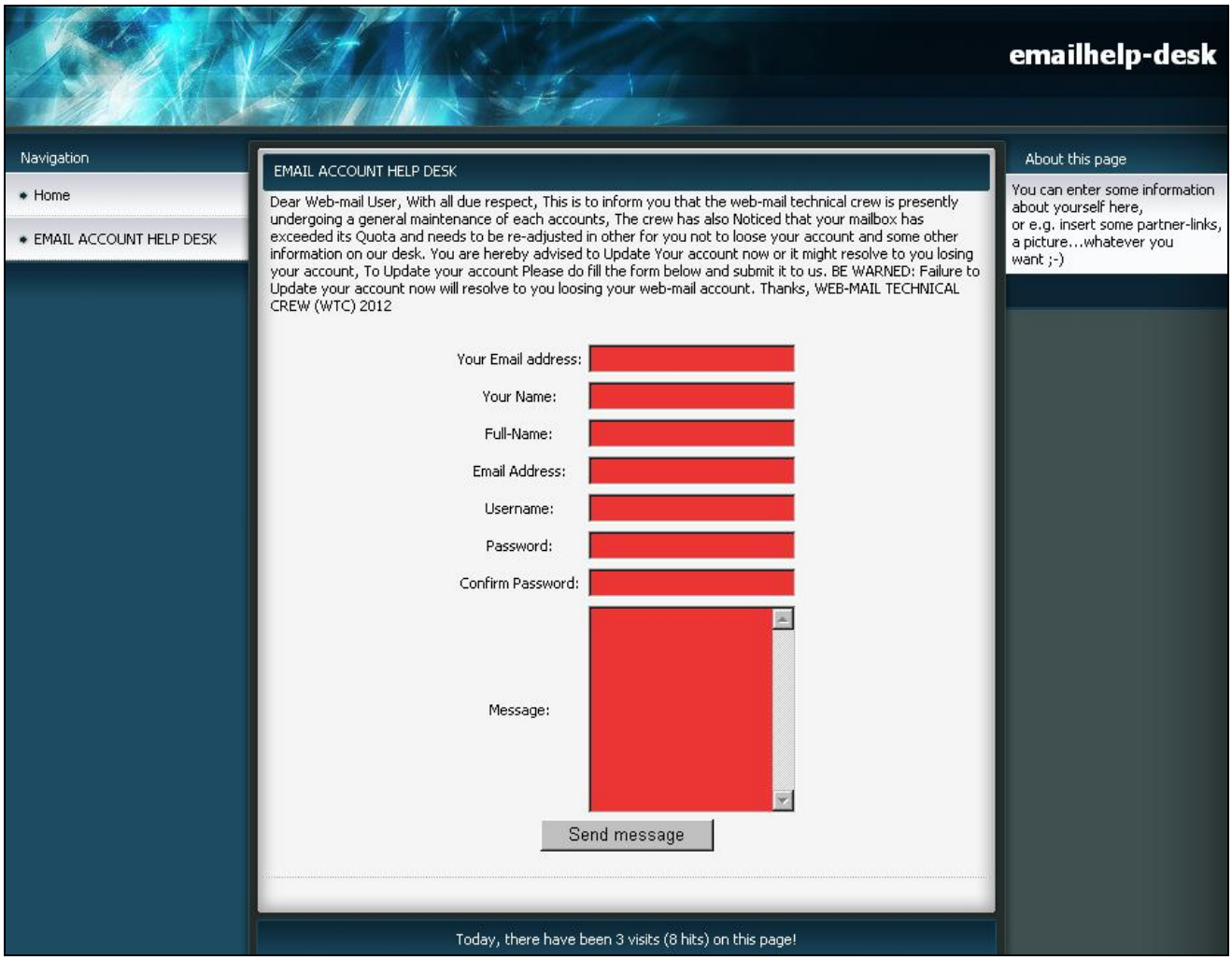



**圖 3. 假冒電子郵件服務中心的釣魚頁面**

連結到其網址後，果然有要輸入帳號密碼的表格，乍看之下好像要填很多資料，但其實主要只有 email address、password、user name 等等，且在頁面中除了此表格外，沒有其它的資訊了，與前季中的釣魚信件相比，多了許多破綻。

前季中常出現的偽造的 HP 文件通知信，本季發現出現比率有微幅上升，信中的超連結的網頁會先秀出" Please wait a moment. You will be forwarded..."等字樣，此時瀏覽器已在重新導向到 .ru 網域的網站，導過去後則是廣告網站，要離開網站時還會出現"確定要離開嗎"之類的瀏覽器對話框，有些還會出現兩次，等於是強迫增加使用者瀏覽廣告的時間。

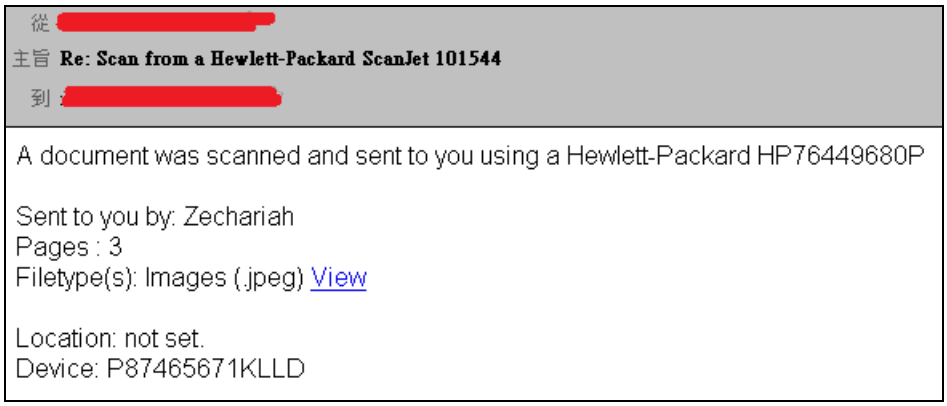



**圖 4. 偽造的 HP 文件通知信**

上述垃圾信的共通處，就是在騙取使用者點擊信裡的超連結，以進一步達到打廣告、騙取帳密或是發散惡意軟體的目的。此類信件甚至會偽造成商業信件，信中的雖然是要從事商業活動，而且下方還有保密注意事項，看起來煞有其事，但點擊該超連結後，卻出現了相當陽春的登入頁面，要求輸入帳號密碼，輸入完帳密後，卻被重導向到阿里巴巴的網站首頁，受害者此時才會恍然大悟，發現被欺騙。

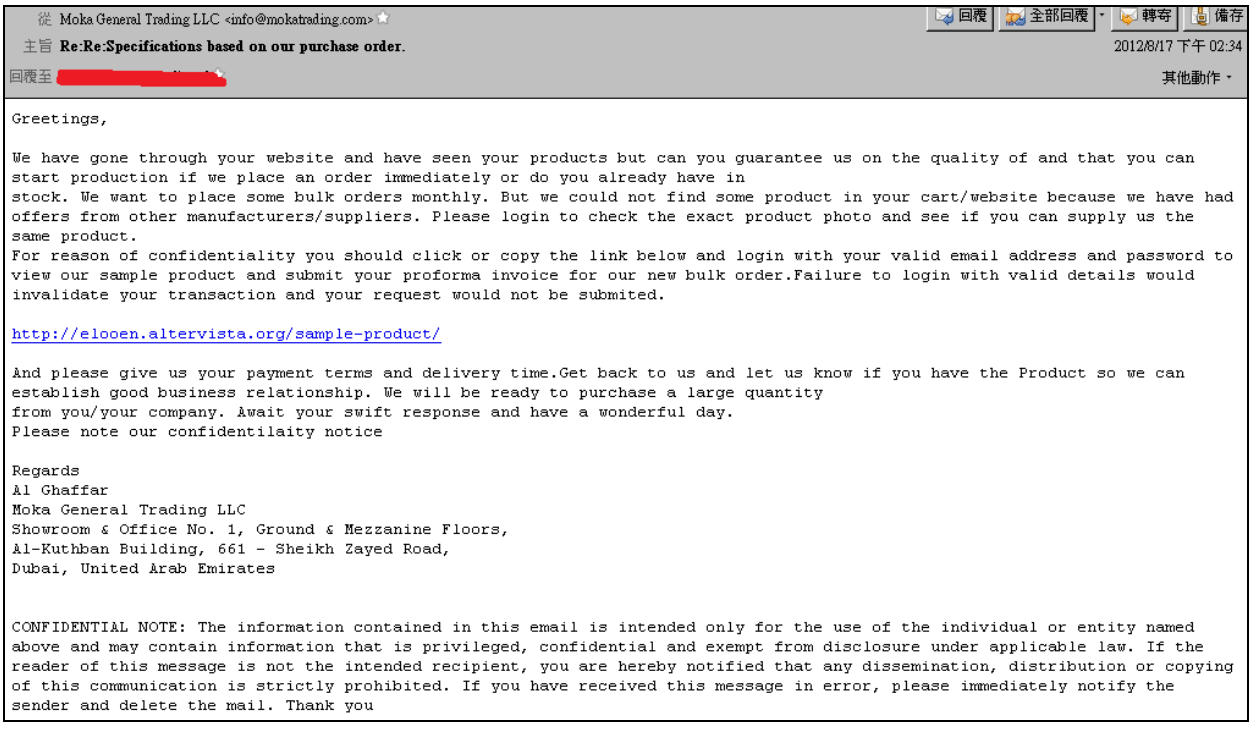



**圖 5. 惡意的商業邀請信件**


**圖 6. 惡意的商業邀請信件點開連結後的釣魚頁面**

常常許多人也會收到色情相關垃圾信件，如下圖例便是某一色情網站的廣告，較值得注意的是信中超連結並非如畫面中所顯示，除了會讓受害者點擊後連結到其他網站之外，該隱藏連結也是利用其它專門提供連結路徑的網站而設，如 http://this-is-a-sample.com/xxxxxxx-yyyyyyyyyy-zzzzzzzzz，只要更改後面的 xyz 字串，便可改連到其它的頁面。


**圖 7. 日本某色情網站 spam**

除了和資安議題較相關的垃圾信件外，還有純粹打廣告為主的垃圾信件。在本季中也發現有許多垃圾信是延續前一季的利用社群網站通知信來發散廣告的手法。

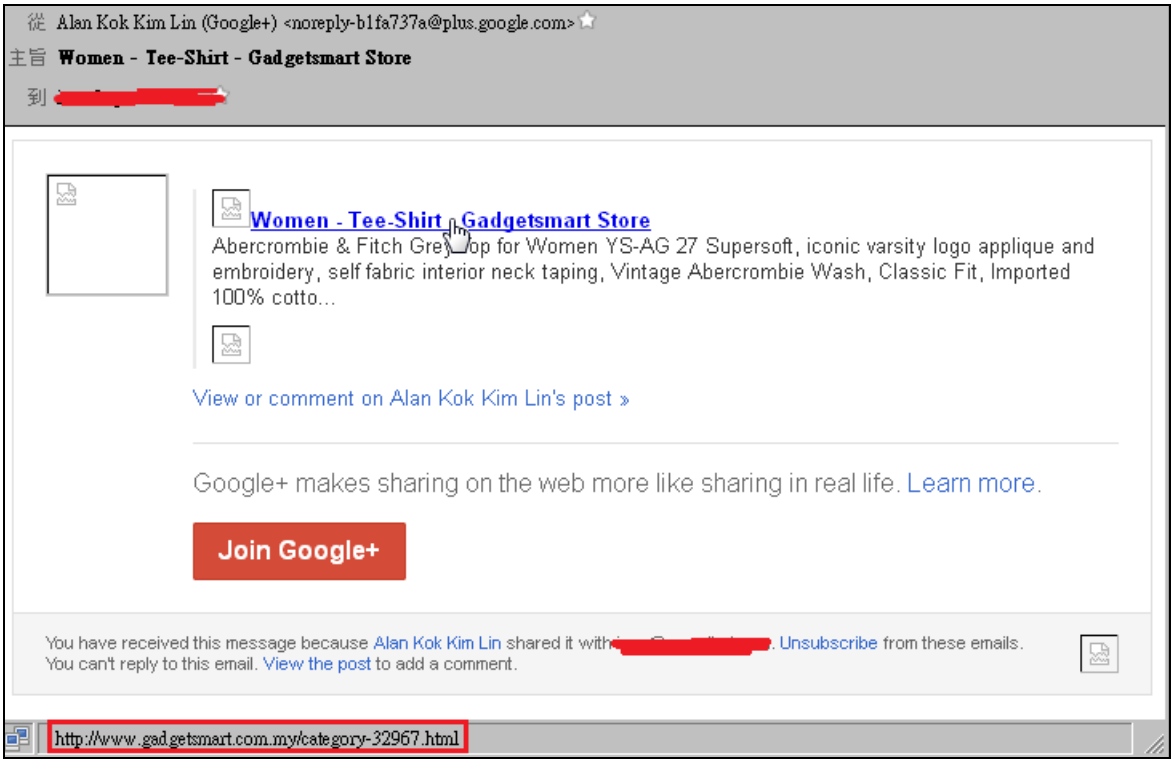



**圖 8. 利用 Google+邀請信發送廣告**

如上圖範例的 Google+社群邀請信，實際上是馬來西亞某一網路商店的廣告信，信中夾有廣告文以及其網路商店商品頁面的超連結。

下圖例中則為利用大陸網路商店的邀請信發送開發票的廣告，信中夾帶有主要的廣告文。


**圖 9. 利用嘀嗒团邀請信發送廣告**

除了發送廣告之外，自然也還是有夾帶惡意程式或連結的惡意信件，如下圖例中的 LinkedIn 邀請信，信中的超連結實際上是連至非 LinkedIn 網域的頁面。

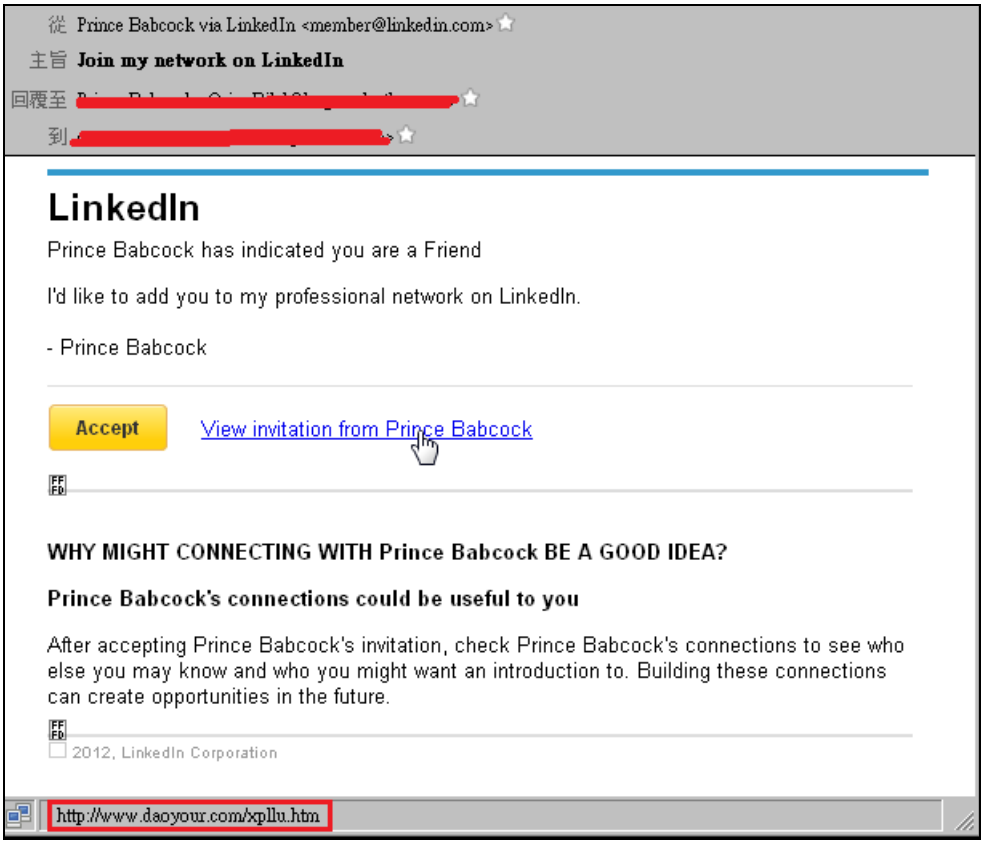



**圖 10. 利用 LinkedIn 邀請信發送惡意信件**

並利用 JavaScript 作掩護，實則在背後收集使用者電腦的資訊，或下載惡意程式；這種利用 JavaScript 的手法到今天已是駭客們的常用技巧，使用者若是發現在網頁原始碼中有出現一長串有規律格式的亂碼，或是點擊超連結後瀏覽器秀出"Please wait a moment. ..."，卻等了很久都沒動靜，此時可能便是誤點惡意連結。

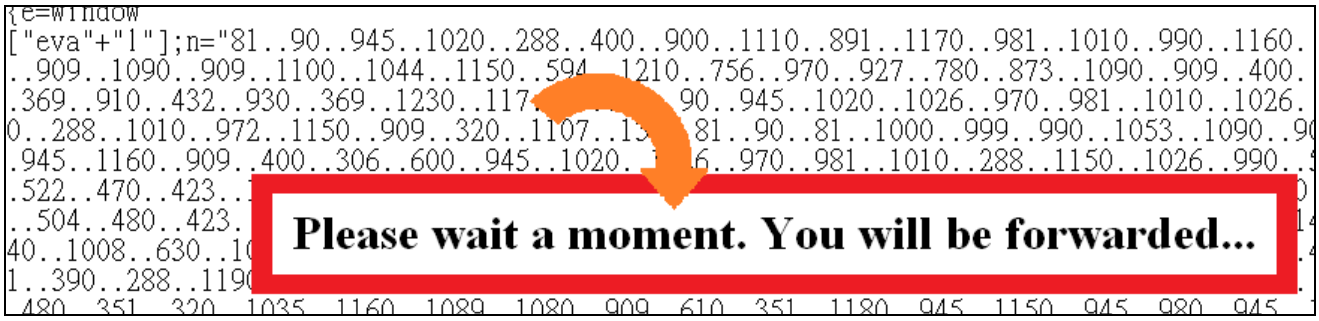



**圖 11. 此類惡意連結顯而易見的特徵**

以往出現過的大陸課程廣告信，不外乎是直接秀出廣告文字、放置廣告文件檔、秀出廣告網站超連結等，而這次收集到的則是利用外部圖片連結的例子：垃圾郵件發送者將所要廣告的文字全部放入圖片中，再將圖片放在外部網站圖床，當信件開啟時便會自動將圖片讀入、秀出廣告，雖然外部圖片連結是很普通的方法，但由於其廣告文字多，圖片也相對的大，如下圖例中的廣告圖便有 755x6583 像素，也可能在使用者開啟信件時對瀏覽器產生某些影響，而對使用者造成麻煩。

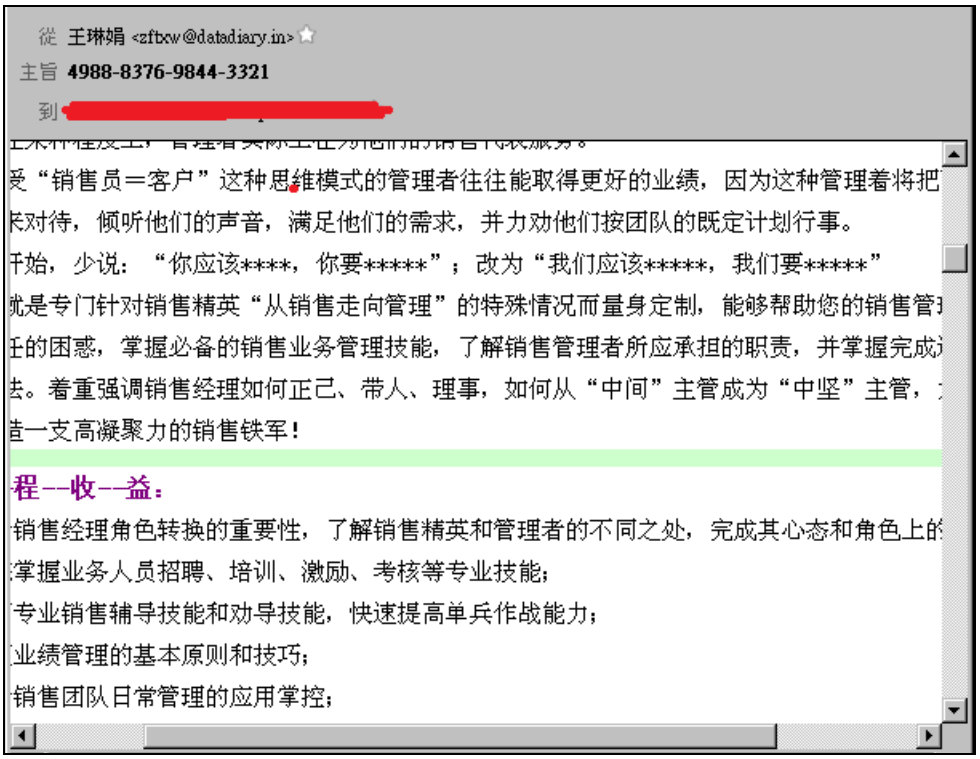



**圖 12. 再度變型的大陸課程廣告信**

另外，帶有未知附檔的垃圾信最危險的地方便是會引誘人想下載附檔來查看內容，若因好奇而下載附檔，便很可能中了駭客的招數而不自知，如下圖例，全信的內容只有一長串數字、保密聲明、簽名檔以及一個 pdf 附檔，讓人搞不清楚到底是作什麼用的，而檢查後發現附檔內容為大陸課程廣告，雖然似乎沒有夾帶惡意軟體，但打開附檔後使用者也看到了廣告，等於讓垃圾郵件發送者成功發送廣告了。

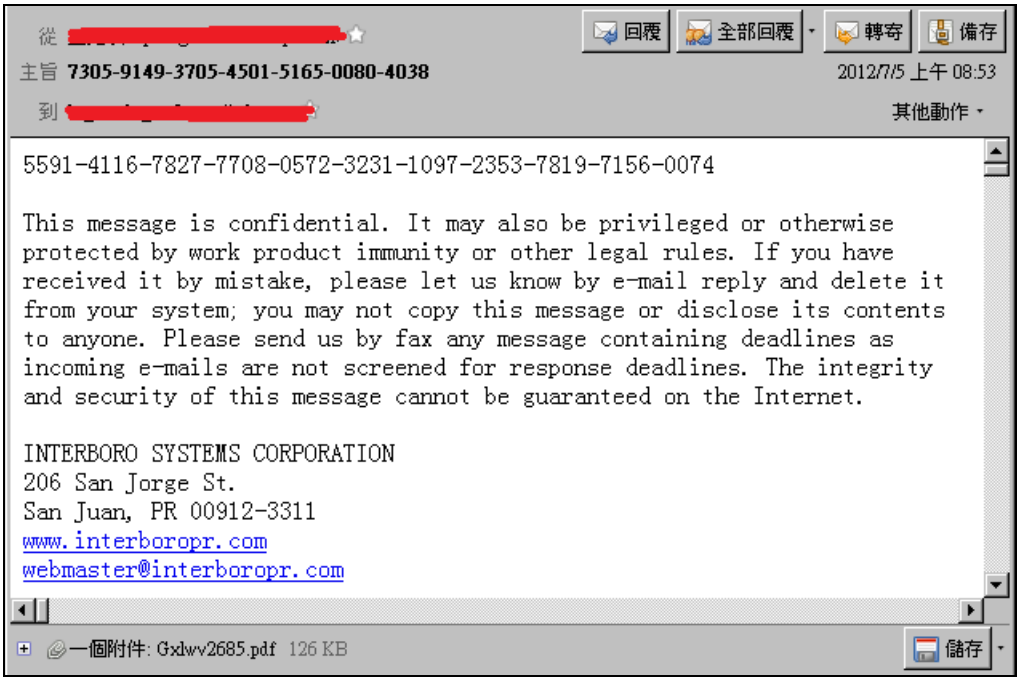



**圖 13. 帶有未知附檔的垃圾信**

在 Q3 期間出現的垃圾信中，資安相關的惡意信件及廣告垃圾信的比率和以往相較並未有大幅度的變化，只是其手法會不時的有小變化以騙取使用者上當，但不管如何變化，絕大部分都離不開超連結和附檔，因此使用者面對有疑慮的超連結和附檔時，並需要審慎評估，避免潛在的資安威脅。

Openfind 電子郵件威脅實驗室，特別從 2012 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 是一款結合郵件系統保全、內容過濾、郵件稽核與加密、統計報表與系統負載平衡設計的全方位郵件郵件防護系統，其具備的雙雲端郵件過濾引擎，結合在地化樣本與全球即時探測的零時差防禦技術，能精準地攔截惡意、垃圾與病毒信件的威脅。同時，MailGates 提供的郵件稽核與紀錄追蹤功能，能讓管理者完整管控郵件伺服器的郵件傳遞政策與使用狀況，預防機密郵件外洩及追查郵件不當使用，捍衛企業訊息安全，並提升組織營運競爭力。 更多產品訊息，請瀏覽產品網頁：http://www.openfind.com/taiwan/products/mailgates/info.html

**關於 Openfind 個資法解決方案**

Openfind 個資法解決方案，以閘道防護與探勘稽核設計導向，秉持「迅速導入」、「建置障礙低」、「不干擾組織內部使用者」、「無須改變現有流程」等特色，協助企業進行個資盤點、電子郵件個人資料外洩、舉證報表等個人機敏資訊外洩防護。更多訊息，請瀏覽公司網站：http://www.openfind.com/taiwan/solution/issue/dataprotection.html

**關於 Openfind 雲端訊息保全解決方案**

近年針對全球虛擬化、雲端技術和資料稽核、探勘需求加溫的趨勢，Openfind 正式提出 Message Assurance 訊息保全方案 ─ 提供組織完整的資訊外洩防護，符合相關資安法規，並支援企業建構的各種虛擬化（VMware、Citrix、Hyper-V）平台，是企業走向雲端世代時，最佳的訊息安全選擇。此外，透過支援各式各樣的智慧型行動裝置，Openfind Message Assurance 訊息保全方案也能協助企業建構全方位的行動通訊與安全訊息溝通環境，真正落實雲+端的訊息溝通新體驗。更多訊息，請瀏覽公司網站：http://www.openfind.com/taiwan/solution/issue/cloud.html

**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、加密、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/