Email Threats Sample Report
Q2 2012

Openfind™

根據 Openfind 電子郵件威脅實驗室於 2012 年 Q2 針對台灣地區電子郵件威脅樣本的觀察，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，使用者在開啟電子郵件時，請千萬注意以下細節：

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，攻擊者多半利用轉址服務或短網址服務網站，有些攻擊者甚至自行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：**
   類似以往垃圾信發送者較常使用知名郵件服務(Yahoo、Gmail、Hotmail …等)直接發送廣告信件的手法，本季中觀察到藉由知名社群網站(Facebook、Google+ …等)發布廣告信的新例子，除了信件到達率高之外，透過社群網站上的資料，垃圾信發送者也更容易尋找較可能開啟廣告信件的收件者，以提升廣告效益。
3. **大陸地區的偽造 eDM：**
   為了提高信件到達率，許多垃圾信發送者將其簡體商業網站垃圾信改進了內容，在信中加入了圖片、美觀的排版以及『取消订阅』、『如果您无法阅读此邮件，请点击这里』等類似字樣，以提高可信度，就像正常 eDM 一樣，但其本質還是垃圾信件。

近幾年中國貿易人口快速成長，電子商務蓬勃發展，廣大的電子商務用戶成了駭客眼中的肥羊，如以下這一則釣魚信件案例：

【假冒中國製造網確認信的惡意郵件】

雖然信中有許多可疑處，似乎可看出是對中文不熟悉的垃圾信件發送者所寄送，但仍可能有剛好在使用中國製造網服務的收件者會點開信中連結以檢視訊息；

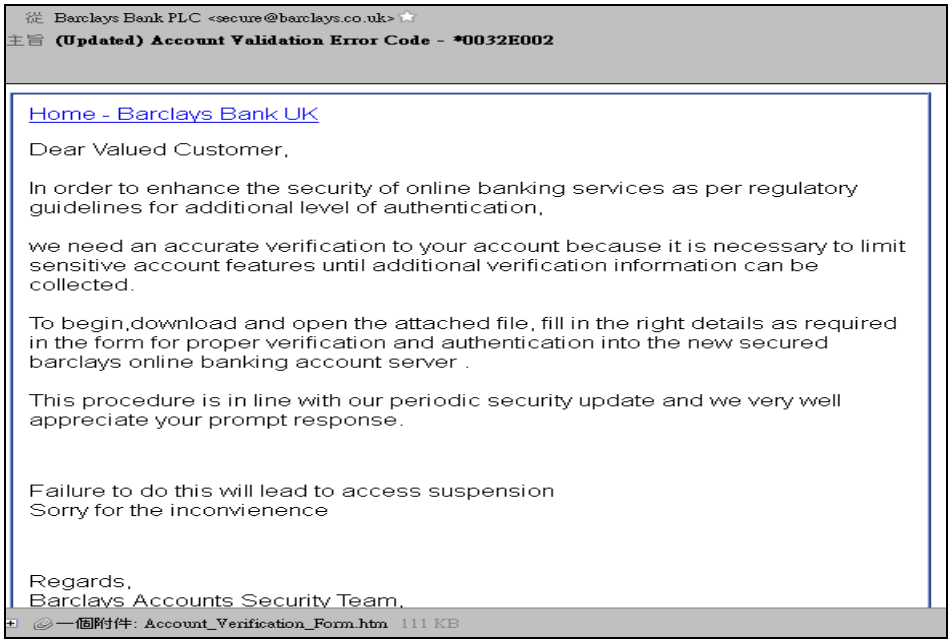
【假造的中國製造網用戶登入頁面】

點開其連結(www.darlingpetboutique.com/storefront/images/xxx.htm)後，和一般騙取帳號密碼的釣魚信件一樣，為假造的登入頁面，可注意到頁面中要求輸入的是電子郵件地址，以及要求再多輸入一次密碼，以確保正確性；另外，檢查其 html 原始碼，也可發現它的表格在傳送資料時，不是傳到中國製造網(http://cn.made-in-china.com/)，而是其他的站點(http://www.1eurohosting.nl/formmail/xxx.php)，便可知此頁面的確是釣魚頁面。

而在真正的中國製造網的用戶登入頁面(http://membercenter.cn.made-in-china.com/login/)中，其要求的是登錄名或電子郵件信箱、密碼以及驗證碼等三項，和釣魚頁面有非常大的不同。

【真正的中國製造網用戶登入頁面】

除了針對中文的垃圾信以外，以往針對歐美地區人士的釣魚信件也仍持續不斷的出現，如下假冒英國 Barclays Bank 的詐騙信，但較不同的是，駭客直接將釣魚用的網頁頁面夾帶在信中，使用者只要點開附檔的網頁便可瀏覽釣魚頁面，危險性高了許多。



【假冒英國 Barclays Bank 帳戶確認信的釣魚信件】

將其夾帶的網頁檔案抓下來後，用筆記本開啟，可看到如下的內容，明顯是利用 Javascript 編碼後，增加分析人員解讀的難度，等待瀏覽器讀取時，會自動執行編碼過的 Javascript 程式碼，將其導到釣魚頁面。

```
<script
type="text/javascript">document.write('\u003C\u0021\u0044\u004F\u0043\u0054\u0059\u0050\u0045\u
0020\u0068\u0074\u006D\u006C\u0020\u0050\u0055\u0042\u004C\u0049\u0043\u0020\u0022\u002D\u002F\
u002F\u0057\u0033\u0043\u002F\u002F\u0044\u0054\u0044\u0020\u0058\u0048\u0054\u004D\u004C\u0020
\u0031\u002E\u0030\u0020\u0054\u0072\u0061\u006E\u0073\u0069\u0074\u0069\u006F\u006E\u0061\u006
C\u002F\u002F\u0045\u004E\u0022\u0020\u0022\u0068\u0074\u0074\u0070\u003A\u002F\u002F\u0077\u00
77\u0077\u002E\u0077\u0033\u002E\u006F\u0072\u0067\u002F\u0054\u0052\u002F\u0078\u0068\u0074\u0
06D\u006C\u0031\u002F\u0044\u0054\u0044\u002F\u0078\u0068\u0074\u006D\u006C\u0031\u002D\u0074\u
0072\u0061\u006E\u0073\u0069\u0074\u0069\u006F\u006E\u0061\u006C\u002E\u0064\u0074\u0064\u0022\
u003E\u000D\u003C\u0068\u0074\u006D\u006C\u0020\u0078\u006D\u006C\u006E\u0073\u003D\u0022\u0068
\u0074\u0074\u0070\u003A\u002F\u002F\u0077\u0077\u0077\u002E\u0077\u0033\u002E\u006F\u0072\u006
7\u002F\u0031\u0039\u0039\u0039\u002F\u0078\u0068\u0074\u006D\u006C\u0022\u0020\u0078\u006D\u00
6C\u003A\u006C\u0061\u006E\u0067\u003D\u0022\u0065\u006E\u002D\u0047\u0042\u0022\u0020\u006C\u0
061\u006E\u0067\u003D\u0022\u0065\u006E\u002D\u0047\u0042\u0022\u003E\u003C\u0068\u0065\u0061\u
0064\u003E\u000D\u003C\u006D\u0065\u0074\u0061\u0020\u0068\u0074\u0074\u0070\u002D\u0065\u0071\
u0075\u0069\u0076\u003D\u0022\u0063\u006F\u006E\u0074\u0065\u006E\u0074\u002D\u0074\u0079\u0070
\u0065\u0022\u0020\u0063\u006F\u006E\u0074\u0065\u006E\u0074\u003D\u0022\u0074\u0065\u0078\u007
4\u002F\u0068\u0074\u006D\u006C\u003B\u0020\u0063\u0068\u0061\u0072\u0073\u0065\u0074\u003D\u00
49\u0053\u004F\u002D\u0038\u0038\u0035\u0039\u002D\u0031\u0022\u003E\u000D\u0020\u0020\u0020\u0
020\u000D\u000D\u000D\u003C\u006D\u0065\u0074\u0061\u0020\u0068\u0074\u0074\u0070\u002D\u0065\u
0071\u0075\u0069\u0076\u003D\u0022\u0043\u006F\u006E\u0074\u0065\u006E\u0074\u002D\u004C\u0061\
u006E\u0067\u0075\u0061\u0067\u0065\u0022\u0020\u0063\u006F\u006E\u0074\u0065\u006E\u0074\u003D
\u0022\u0065\u006E\u002D\u0047\u0042\u0022\u003E\u000D\u0020\u0020\u0020\u0020\u000D\u003C\u007
4\u0069\u0074\u006C\u0065\u003E\u004F\u006E\u006C\u0069\u006E\u0065\u0020\u0042\u0061\u006E\u00
6B\u0069\u006E\u0067\u0020\u0056\u0065\u0072\u0069\u0066\u0069\u0063\u0061\u0074\u0069\u006F\u0
06E\u0020\u002D\u0020\u0020\u0020\u004D\u0079\u0020\u0042\u0061\u0072\u0063\u006C\u0061\u0079\u
0073\u003C\u002F\u0074\u0069\u0074\u006C\u0065\u003E\u000D\u0020\u0020\u0020\u0020\u000D\u000D\
u003C\u006C\u0069\u006E\u006B\u0020\u0068\u0072\u0065\u0066\u003D\u0022\u0068\u0074\u0074\u0070
\u003A\u002F\u002F\u0039\u0037\u002E\u0037\u0034\u002E\u0032\u0033\u0030\u002E\u0036\u0034\u002
F\u0045\u006D\u0061\u0069\u006C\u0041\u0064\u0076\u0065\u0072\u0074\u0069\u0073\u0065\u006D\u00
65\u006E\u0074\u002F\u0069\u006D\u0061\u0067\u0065\u0073\u002F\u0062\u0061\u0072\u0063\u006C\u0
061\u0079\u0073\u002F\u0062\u0061\u0072\u0063\u006C\u0061\u0079\u0073\u002E\u0063\u0073\u0073\u
0022\u0020\u0072\u0065\u006C\u003D\u0022\u0073\u0074\u0079\u006C\u0065\u0073\u0068\u0065\u0065\
u0074\u0022\u0020\u0074\u0079\u0070\u0065\u003D\u0022\u0074\u0065\u0078\u0074\u002F\u0063\u0073
\u0073\u0022\u0020\u006D\u0065\u0064\u0069\u0061\u003D\u0022\u0073\u0063\u0072\u0065\u0065\u006
```

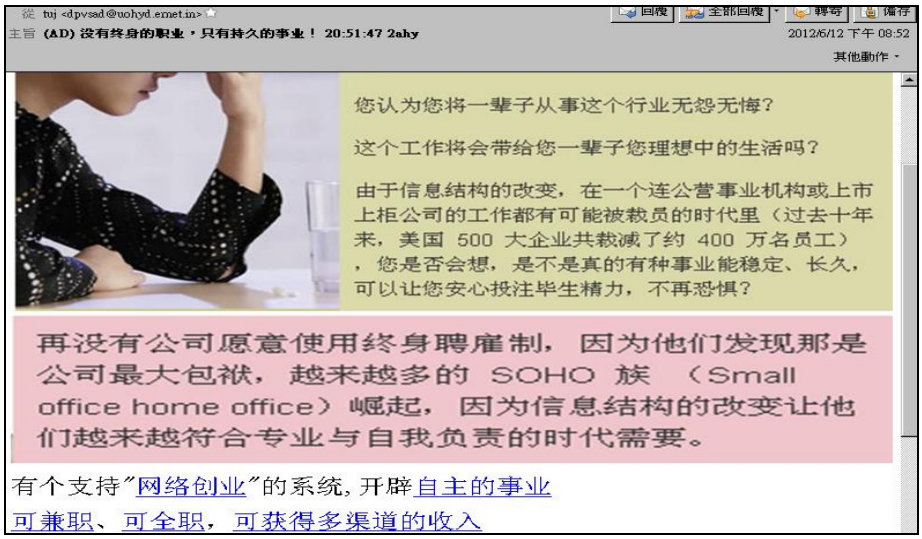
【部分假冒英國 Barclays Bank 註冊頁面的釣魚網頁原始碼】

在將此釣魚網頁解讀之後，發現它會將使用者在註冊表格中填入的資料送至 http://195.140.132.196/~dan12454/images/complete.php(已失效)。

如同利用知名郵件服務(Yahoo、Gmail、Hotmail …等)發送廣告信件，垃圾信發送者也開始利用社群網站發送廣告訊息，此手法為垃圾信發送者先在社群網站上申請帳號，申請完後便藉著社群網站的便利性尋找可發送廣告信的”潛在客戶”，如下圖便是利用 Google+ 發送的在家工作廣告信：

【利用 Google+ 發送的廣告信件】

此外，在家工作的廣告信，最近也開始出現了針對中國大陸地區的簡體信件，並且透過社群網站散佈，但目前觀察到的數量跟台灣地區原本的繁體或英文比較起來，屬於相對少數。



【利用 Google+ 發送的廣告信件】

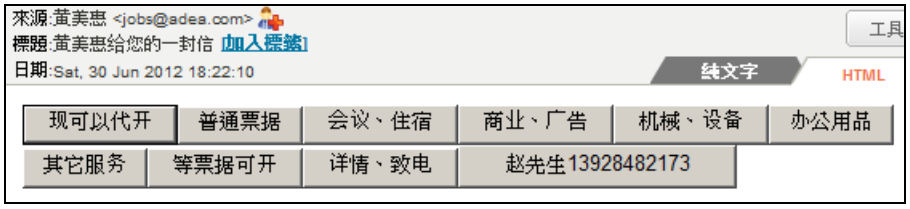
中國地區近來電子商務的興盛，誘使各商家也開始散發廣告垃圾信，以吸引寄件者登門拜訪並進而提高營收，像是下圖以賣酒為主的味多團購網的垃圾信，雖然是垃圾信，卻作的美輪美奐，與一般 eDM 相差無幾，提高收件者的興趣，進而瀏覽網站。

【大陸地區的偽造 eDM 之一】

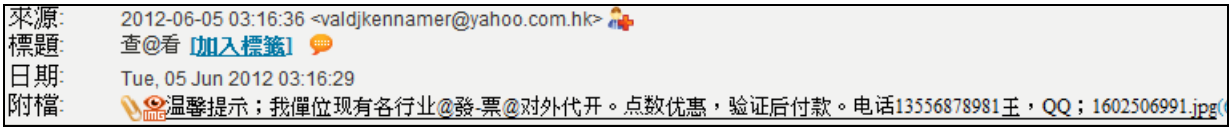
此類的垃圾信件的內容比一般垃圾信漂亮，且與正常 eDM 不同之處，在於為了躲避過濾，大部分都會變換寄件者，如下圖中，寄件者皆與打廣告的商家網站無關。

【大陸地區的偽造 eDM 之二】

除了前一類仿 eDM 的廣告垃圾信外，垃圾信的呈現型態也有另類發展的趨勢，如下圖幾種：

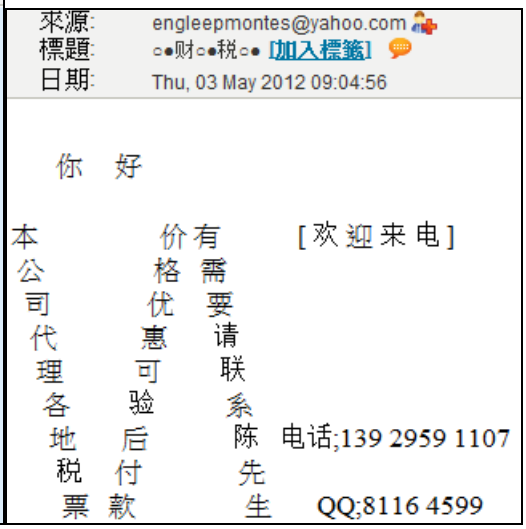


【變形垃圾信之一】



【變形垃圾信之二】

【變形垃圾信之三】



【變形垃圾信之四】

這類針對代開發票的廣告垃圾信種類繁多，在視覺方面做各種變化，使用技巧各有不同，但和以往大多使用一般語句當作標題的垃圾信不同，最近此類信件在標題或寄件人等便會加入些許亂七八糟的字樣，使用者在開信前即可察覺為此類廣告信件。

在 Q2 期間出現的垃圾信之中，資安相關的惡意信件出現的頻率較以往降低許多，廣告垃圾信的比率與種類則是相對上升，使用者在收信時可多加留心信件中的超連結和可疑附檔，若有疑慮便不開，即可避開潛伏著的資安威脅。

Openfind 電子郵件威脅實驗室，特別從 2012 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/。