Openfind™ Software Engineered for Growth™

# Email Threats Analysis Report

# Q1 2013

# Openfind 郵件威脅分析報告 Q1 2013

## 目 錄

## 一、 全球垃圾信發送來源地區

根據 Openfind 電子郵件威脅實驗室於 2013 年 Q1 針對全球垃圾郵件來源 IP 觀察研究，垃圾信來源國家的前三名分別為中國、澳洲與日本，依序佔整體垃圾信的 31 % 、14% 與 8%。由此可見，延續上一季結果，中國仍為全球主要垃圾郵件來源，百分比例為第二名的澳洲的兩倍以上，而第三名則從上一季的美國易主為日本。台灣地區本季排名第 8，佔比 4%。此外，其他國家的佔比從上季的 30%大幅下滑到 19%，從這點可以看出本季的垃圾郵件發布地區有較為集中的趨勢。

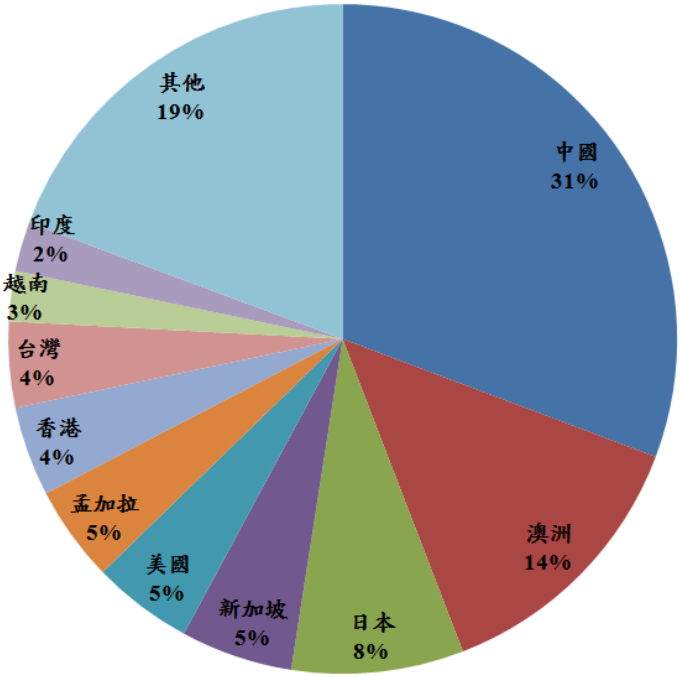



**圖 1. 2013 年第 1 季垃圾信來源國家分布**

細部觀察 1 月、2 月及 3 月的來源比例，中國一直位居領先位置，不過 2 月的時候可以發現，孟加拉及香港的比例有一度提高的趨勢，進入了當月前四名的位置，日本三個月的垃圾信發信來源一直維持在穩定且高比例的區間內，顯示來自日本的郵件威脅確實是必須重視及深入探討的議題。另外一個值得重視的垃圾信來源國為新加坡，從今年一月的 1.5% 至三月順向爬升到了 8.8 %，幾乎與日本比重相同，後續走勢值得觀察。

**表 1. 2013 年第 1 季垃圾信來源國家比例**

| 國家 | 一月 | 二月 | 三月 | 季平均 | 季排名 |
|---|---|---|---|---|---|
| 中國 | 36.5% | 19.4% | 34.4% | 30.7% | 1 |
| 澳洲 | 1.2% | 19.2% | 15.5% | 13.4% | 2 |
| 日本 | 8.8% | 8.7% | 7.9% | 8.3% | 3 |
| 新加坡 | 1.5% | 2.3% | 8.8% | 5.4% | 4 |

| | | | | | |
|---|---|---|---|---|---|
| 美國 | 6.6% | 4.1% | 4.5% | 4.9% | 5 |
| 孟加拉 | 0.3% | 12.9% | 2.0% | 4.6% | 6 |
| 香港 | 2.5% | 13.3% | 0.2% | 4.3% | 7 |
| 台灣 | 8.8% | 2.2% | 3.2% | 4.1% | 8 |
| 越南 | 2.3% | 0.4% | 3.6% | 2.4% | 9 |
| 印度 | 3.2% | 1.3% | 2.6% | 2.4% | 10 |
| 其他 | 28.5% | 16.1% | 17.2% | 19.4% | |

台灣目前在季排名位居第八，跟去年相比，名次有往後移，郵件威脅趨緩，從一月的 8.8%逐步下降至 3.2% 左右，而且今年的比例趨勢已不像去年一樣跟中國比例相似，反而走勢跟美國相近，呈現遞減的趨勢。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，深入觀察垃圾郵件所包含的 URL 網頁內容，並將網頁進行分類，圖 2 為本季網頁內容分類狀況。最多的網頁主題為購物相關類別，超過 5 分之 1 的垃圾郵件網址會導引收件人前往購買物品之網頁，多為商品廣告、EDM 與商品目錄等等購物訊息。

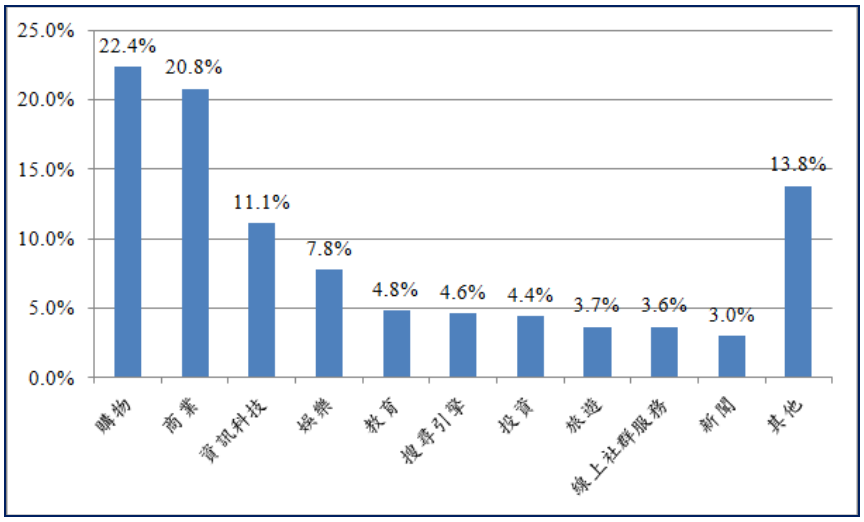



**圖 2. 2013 年第 1 季垃圾信 URL 網頁內容分類**

垃圾郵件內容所囊括的種類相當多元，但其實也間接反映出網路使用者普遍較為關心的主題，除了網路購物外，在財務方面對於商業訊息、投資快訊佔有重要比例。而在休閒議題上面，演藝娛樂、旅遊景點、或社群網路服務也都榜上有名。網路威脅越來越貼近民眾生活，除了建議網路使用者在開啟不明來源之郵件時，提高警覺之外，亦建議於系統端加強外部網頁安全風險等級自動化提示機制。

**表 2. 2012 年第四季與 2013 年第一季 URL 網頁內容分類比較**

| | 2012 Q4 | | 2013 Q1 | |
|---|---|---|---|---|
| **排名** | **類別** | **比例** | **類別** | **比例** |
| **1** | 購物 | 23.8% | 購物 | 22.4% |
| **2** | 商業 | 19.3% | 商業 | 20.8% |
| **3** | 資訊科技 | 10.8% | 資訊科技 | 11.1% |
| **4** | 娛樂 | 8.3% | 娛樂 | 7.8% |
| **5** | 教育 | 5.1% | 教育 | 4.8% |
| **6** | 搜尋引擎 | 5.1% | 搜尋引擎 | 4.6% |
| **7** | 投資 | 4.7% | 投資 | 4.4% |
| **8** | 旅遊 | 3.7% | 旅遊 | 3.7% |
| **9** | 線上社群 | 3.5% | 線上社群 | 3.6% |
| **10** | 新聞 | 2.6% | 新聞 | 3.0% |

觀察上述兩季 URL 網頁內容，可發現兩季前十大排名主題完全相同，甚至前三大類別（購物、商業與資訊科技）的比例也相似，以這前半年的觀察得知，若要著手處理郵件威脅及垃圾郵件的困擾時，可以先從購物、商業及資訊科技相關議題進行處理，設定特殊關鍵字或進行樣本訓練，便可有效預防大多數垃圾郵件問題。由於本季的觀察結果與上一季的觀察結果有著大幅度的雷同點，包含前十大類別的排名與比例，後續於 2013 年第 2 季中，可以再度確認這樣的排名趨勢是否已成型，或是產生其他變化。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

延續上一季垃圾信發布模式，轉址服務仍為垃圾信散布的主要手法，相關模式說明如下：

1. **隱藏具有威脅的非法網址**
   具有威脅或不正當目的的垃圾郵件多會夾帶危險性無法預期的網頁連結，常見的手法即是巧妙營造信件中超連結存在的合法性；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，幫助作轉址來隱藏目標網站網址。

2. **益發精緻化的偽造 EDM**
   傳統的垃圾信僅以文字、連結甚至是以簡體字所撰寫，讓收件者在收到信的當下即可瞬間辨識出的廣告信件，目前的廣告信件有著傾向更注重設計感及版面編排的趨勢，讓質感大幅提升至精美 EDM 等級，除了透過將超連結放置在漂亮的圖片中誘使收件人點擊外，還有更具吸引力的退訂連結，均可讓收件人連結至目標網站。

3. **社交工程攻擊**
   除了帶有超連結的垃圾信以外，本季中發現不少疑似社交工程攻擊的信件；此類垃圾信件通常會以與收件人熟識的立場撰寫郵件內文，再在信中夾帶如 Word 文檔或 WinRAR 壓縮檔等附檔，而收件者匆忙之中往往會不經意的開啟附檔而中毒；因此面對挾帶附檔的可疑信件時，最好先經過其他管道確認郵件真實性後再開啟附檔，以免中病毒或是木馬。

## 四、 垃圾信樣本詳細說明

一般垃圾信中的廣告信主要都是食品、服飾、非法的盜版光碟與藥物買賣等，不過近來非買賣物品的廣告信有上升趨勢，如前一季的旅遊廣告信，而本季則觀察到更多類似的例子。以下針對台灣地區、中國地區及日本地區提供本季垃圾信範例說明：

### 台灣地區常見垃圾信發送模式

下圖的祈福廣告信範例，提供有退訂通知的引誘連結：

**圖 3. 指南宮點燈廣告信上半部**

一打開信件，便可看到它的廣告目標網站為 www.g-utv.com，廣告的商品為其中的光明燈、太歲燈等點燈儀式的活動，接著檢查信件下方的取消訂閱連結，發現它的退訂網址為 http://enews.callin.net/SubscribeNew/，與廣告目標網站網域並不相同。

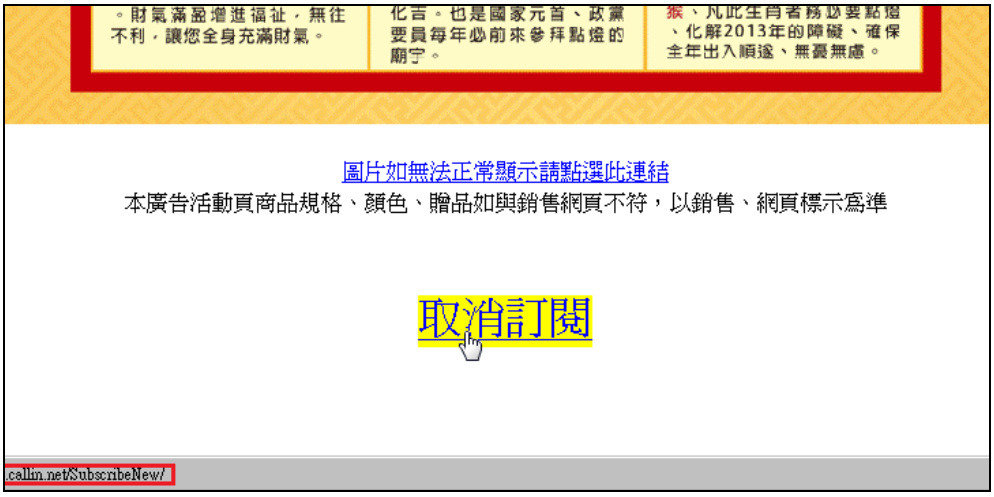



**圖 4. 指南宮點燈廣告信末**

接著實際點進去檢查後，雖然頁面中有表單可供使用者填入 e-mail address 以取消訂閱，但卻沒有其它關於要退訂的廣告信種類的訊息，再加上與廣告目標網站網域不同，請提高警覺再三確認這類網站的真實性，並小心勿將個人資料填入惡意網站之中。

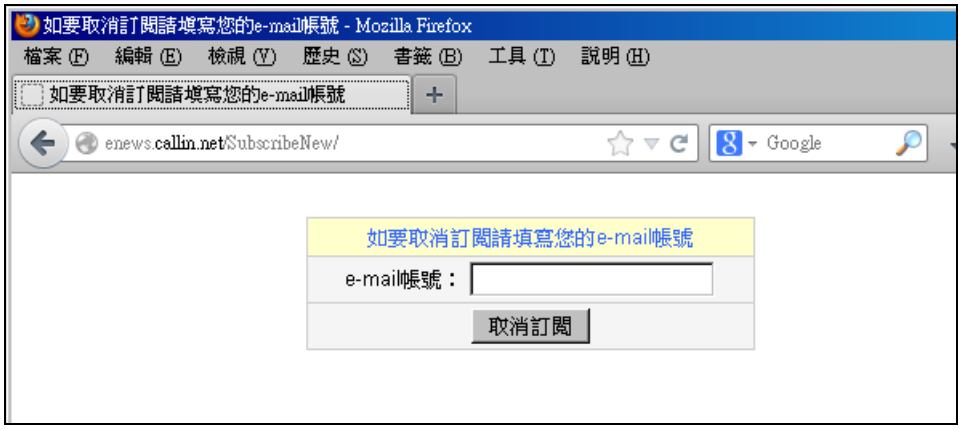
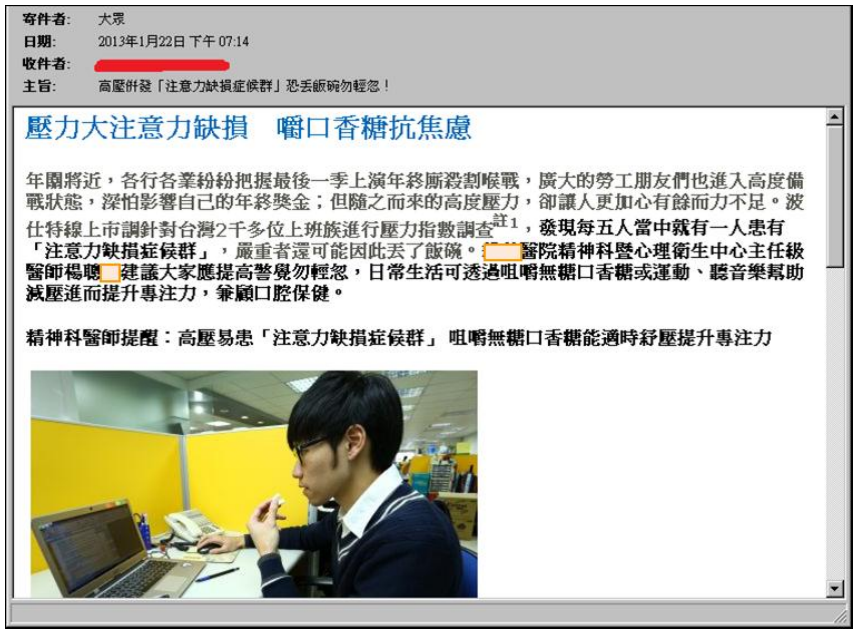



**圖 5. 廣告信的退訂網頁**

接著以下範例郵件，標題和內文乍看之下只是分享保健訊息的郵件。


寄件者: 大眾
日期: 2013年1月22日 下午 07:14
收件者: [redacted]
主旨: 高壓併發「注意力缺損症候群」恐丟飯碗勿輕忽！

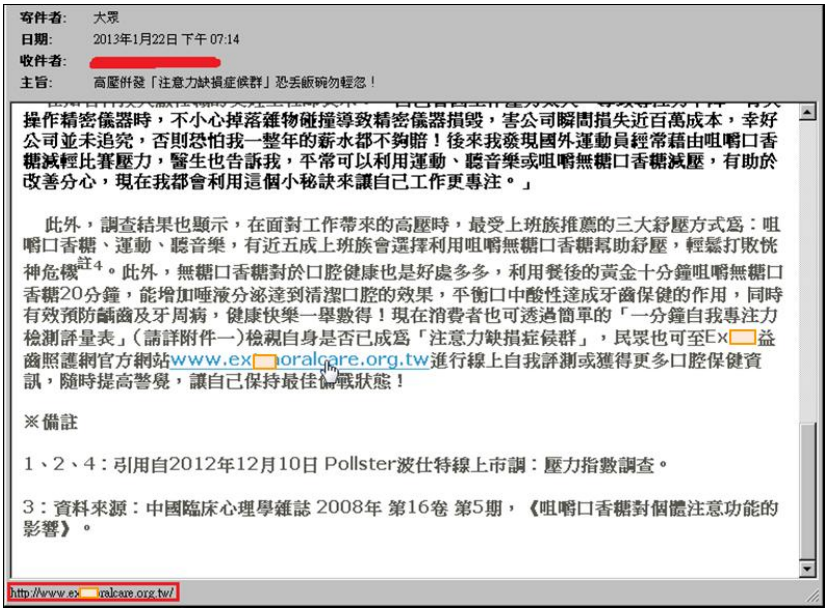
壓力大注意力缺損　嚼口香糖抗焦慮

年關將近，各行各業紛紛把握最後一季上演年終廝殺割喉戰，廣大的勞工朋友們也進入高度備戰狀態，深怕影響自己的年終獎金；但隨之而來的高度壓力，卻讓人更加心有餘而力不足。波仕特線上市調針對台灣2千多位上班族進行壓力指數調查[註1]，發現每五人當中就有一人患有「注意力缺損症候群」，嚴重者還可能因此丟了飯碗。[redacted]醫院精神科暨心理衛生中心主任級醫師楊聰[redacted]建議大家應提高警覺勿輕忽，日常生活可透過咀嚼無糖口香糖或運動、聽音樂幫助減壓進而提升專注力，兼顧口腔保健。

精神科醫師提醒：高壓易患「注意力缺損症候群」 咀嚼無糖口香糖能適時紓壓提升專注力

**圖 6. 口香糖廣告信上部**

但到了信末，卻出現潔牙口香糖相關網站的介紹及連結，若是客觀的保健資訊，按理應不會有私人企業資訊在內，再加上信中著重於嚼口香糖經驗分享，可見應是藉保健資訊置入行銷的廣告信，只是與前例不同的是此例信中並無退訂連結及其它資訊，難以追蹤到垃圾信發送業者。


寄件者: 大眾
日期: 2013年1月22日 下午 07:14
收件者: [redacted]
主旨: 高壓併發「注意力缺損症候群」恐丟飯碗勿輕忽！

操作精密儀器時，不小心掉落雜物碰撞導致精密儀器損毀，害公司瞬間損失近百萬成本，幸好公司並未追究，否則恐怕我一整年的薪水都不夠賠！後來我發現國外運動員經常藉由咀嚼口香糖減輕比賽壓力，醫生也告訴我，平常可以利用運動、聽音樂或咀嚼無糖口香糖減壓，有助於改善分心，現在我都會利用這個小秘訣來讓自己工作更專注。」

此外，調查結果也顯示，在面對工作帶來的高壓時，最受上班族推薦的三大紓壓方式爲：咀嚼口香糖、運動、聽音樂，有近五成上班族會還擇利用咀嚼無糖口香糖幫助紓壓，輕鬆打敗恍神危機[註4]。此外，無糖口香糖對於口腔健康也是好處多多，利用餐後的黃金十分鐘咀嚼無糖口香糖20分鐘，能增加唾液分泌達到清潔口腔的效果，平衡口中酸性達成牙齒保健的作用，同時有效預防齲齒及牙周病，健康快樂一舉數得！現在消費者也可透過簡單的「一分鐘自我專注力檢測評量表」(請詳附件一)檢視自身是否已成爲「注意力缺損症候群」，民眾也可至Ex[redacted]益齒照護網官方網站www.ex[redacted]oralcare.org.tw進行線上自我評測或獲得更多口腔保健資訊，隨時提高警覺，讓自己保持最佳[redacted]戰狀態！

※備註

1、2、4：引用自2012年12月10日 Pollster波仕特線上市調：壓力指數調查。

3：資料來源：中國臨床心理學雜誌 2008年 第16卷 第5期，《咀嚼口香糖對個體注意功能的影響》。

http://www.ex[redacted]oralcare.org.tw/

**圖 7. 口香糖廣告信末**

除了知識性文章帶出商品主題的廣告信外，下面的範例則是以類似社交工程攻擊的手法，製造寄件人跟收件人關係親密的假象，撰寫廣告信件內文，藉以卸下收件人的警覺心，引誘其點選郵件內潛藏威脅之外部連結。


**圖 8. 寬頻業者廣告信範例**

一般來說，網路行銷業者幫特定產品或服務做行銷是可以被理解的，當然在本季中同樣也出現許多行銷廣告信，下圖範例特別值得注意的一點是其中還附加了業務窗口的聯絡資料，算是此類網路行銷廣告信中較少見的。


**圖 9. 網路行銷廣告信範例**

**中國地區廣告信趨勢**

從中國發送的廣告信類別仍和往常一樣有商業課程、代開發票與物品買賣等，且同一商品或服務的呈現方式會持續變化，以下提供某酒商自去年 Q3 至今年 Q1 起觀察到的廣告信變化：


**圖 10. 中國酒商 2012Q3 廣告信**


**圖 11. 中國酒商 2012Q4 廣告信**


**圖 12. 中國酒商 2013Q1 廣告信**

由上面三張圖可發現，信中的超連結網域都不同，但實際連結後，發現都是連到同樣內容的網站，可以猜測是因為當垃圾信發送者使用某網域當作廣告連結一段時間後，為避免網域被黑名單阻擋而失去廣告效果，因而需要新網域作為新的廣告連結。

此外，隨著中國拍賣商城、購物網站平台的穩定發展，其商家的行銷需求量也是有增無減，因此與前幾季相比，本季中類似廣告信的數量仍是穩定緩慢成長，而其廣告信手法也是隨之變化，比如本季觀察到的某一拍賣網站廣告信，信中的超連結為 http://t.cn/zTyOrLK?dctba，為某縮址服務網域，實際連結後，發現會多重轉址：

http://t.cn/zTyOrLK?dctba 轉址到 下面網址

http://weiurl.duapp.com/?id=715641 再轉址到 下面網址

http://s.click.taobao.com/t?e=zGU34CA7K%2BPkqB07S4%2FK0CFcRfH0GoT805sipKjwgTG9pQ%2B903kUBXCYGhyE6InqZnxGOK4H6SDAvoOInAX5DiLVYMxdUB2hzkg37z7Ozbqd 再轉址到 下面網址

http://s.click.taobao.com/t_js?tu=http%3A%2F%2Fs.click.taobao.com%2Ft%3Fe%3DzGU34CA7K%252BPkqB07S4%252FK0CFcRfH0GoT805sipKjwgTG9pQ%252B903kUBXCYGhyE6InqZnxGOK4H6SDAvoOInAX5DiLVYMxdUB2hzkg37z7Ozbqd%26ref%3D%26et%3DjFBC6p5YmD3ERA%253D%253D 再轉址到 下面網址

http://detail.tmall.com/item.htm?id=7867971423&ali_trackid=2:mm_29583798_0_0:1366022634_4k4_2135280136 (目標網站)

會利用如此複雜的轉址，可能是為了要防礙分析而作，否則一般正常 EDM 幾乎不會有如此多層轉址的現象。

**日本地區郵件威脅趨勢**

在日本語的垃圾信方面，延續之前的觀察到的現象，目前廣告信主題仍以成人約會為最大宗，接著是博奕類及賽馬類；發送手法承襲以往利用註冊貌似毫無特別意義的亂數域名作為轉址用網站，範例如下：

http://qwazbtufidd.info/t/login.php?id=236160&pass=76THfZxZ 轉址到 下面網址

http://19tsmbga.jp/p/login.php?id=236160&pass=76THfZxZ (目標網站)

推測應是可以利用亂數網域，以減少網域被黑名單記錄時的損失。

Openfind 電子郵件威脅實驗室，特別從 2013 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 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.tw/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