UBLink.org 裕笠科技股份有限公司

如何防止 EMail 帳號密碼被盜也被詐走匯款

郵件安全問題

JanusLin

2013/8/23

http://www.ublink.org

目錄

如何防止 EMail 帳號密碼被盜也被詐走匯款

昨天同業通報，又發生一件了

先有因後有果
我們應該要先知道可能發生的原因

我們的猜測發生的狀況如下
1. 習慣使用免費的信箱，因爲免費信箱疏於管理，因此帳號跟密碼被盜也無法得知
2. 習慣通知對方匯款使用 Mail，公司管理過於鬆散
3. E-Mail 密碼沒有不定期更換
4. 使用的 Mail Server 沒有加密功能
5. 都跑過國外，回台灣之後沒馬上更改密碼
6. 抓到免費的網路訊號就用了
7. 公司的電腦給小孩玩 Game 共用
8. 收發 Mail 同時間有好幾台電腦或是好幾位同事共用一組郵件信箱
9. …

其他什麼狀況都有

該如何防止
既知發生之原因
要防止就比較簡單了
我們填寫相對應的解決方法

習慣使用免費的信箱，因爲免費信箱疏於管理，因此帳號跟密碼被盜也無法得知

Ans：公司還是要有一點形像，建立自己的 UMail Mail Server 系統，像我們公司有最少人數 10 人的專用 Server，有防護功能，我們公司也有 20 年以上的管理經驗的工程師可以爲您服務，所以可以盡量避免此問題的發生

習慣通知對方匯款使用 Mail，公司管理過於鬆散

會計小姐請想想，爲何有些有點規模的公司要求您影印公司匯款的簿本，這是一個很標準的作業流程，對方除了要確認匯款的銀行資料確認之外，也要求了身份的確認

E-Mail 密碼沒有不定期更換

Mail Server 的標準 Port SMTP TCP 25 和 TCP 110 他的傳輸帳號和密碼資料，Port 110 是明碼，稍有技術的人員可以透過很多工具直接取用，TCP 25 Port 採用的是 Base64 的編碼，比較高級一點的網路工程師也可以輕易的解碼，所以 E-Mail 這實在不是一個很安全的東西，所以定期更換密碼這是一個很重要的程序

使用的 Mail Server 沒有加密功能

承上一個問題，沒有加密，或是很容易被解密，因此您需要我們公司的一個專業的 UMail Mail

server，他有 SMTPs tcp/465，SMTPs tcp/587(密碼選純文字)，POP3s tcp/995，IMAPs tcp/993，HTTPS web manager tcp/88， HTTPS web Mail tcp/443 比較安全

都跑過國外，回台灣之後沒馬上更改密碼

我們碰過幾件這樣的問題，尤其是在國外用完網路之後，帳號跟密碼也完了，被錄走了

抓到免費的網路訊號就用了

免費的最貴，這句話流行在 IT/MIS 的人員身上，但是也是適用於一般的人士，有免費的網路不要太高興，通常後面不知道有躲著那些高手在後面

公司的電腦給小孩玩 Game 共用

很多人爲了省電腦的錢，跟小孩子共用一台電腦，中毒中木馬常常不知道，等問題發生查的時後，通常電腦早就一蹋胡塗了

收發 Mail 同時間有好幾台電腦或是好幾位同事共用一組郵件信箱

這也是我們常碰到的原因之一，要做大生意真的不要省這個錢了，建議一個有公司形象的專業 UMail Server，讓您可以更安心

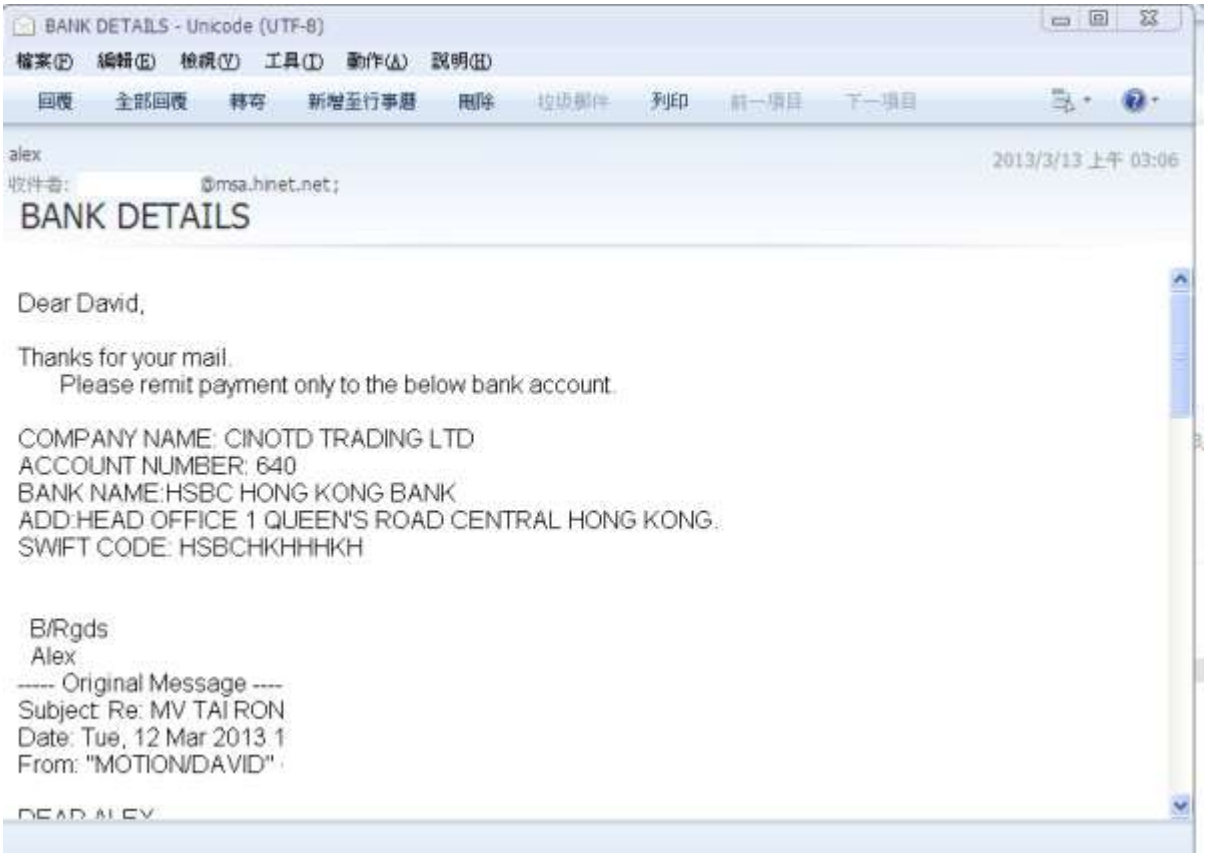
UMail Mail Server 介紹如下

http：//www.ublink.org/index.php/2010-02-27-09-11-23/ublink/umail-server.html

郵件追追追

如何追蹤郵件的真僞和寄件者的郵件表頭

同業回報
很多做貿易公司都收到這樣的 Mail



無法辨識真僞

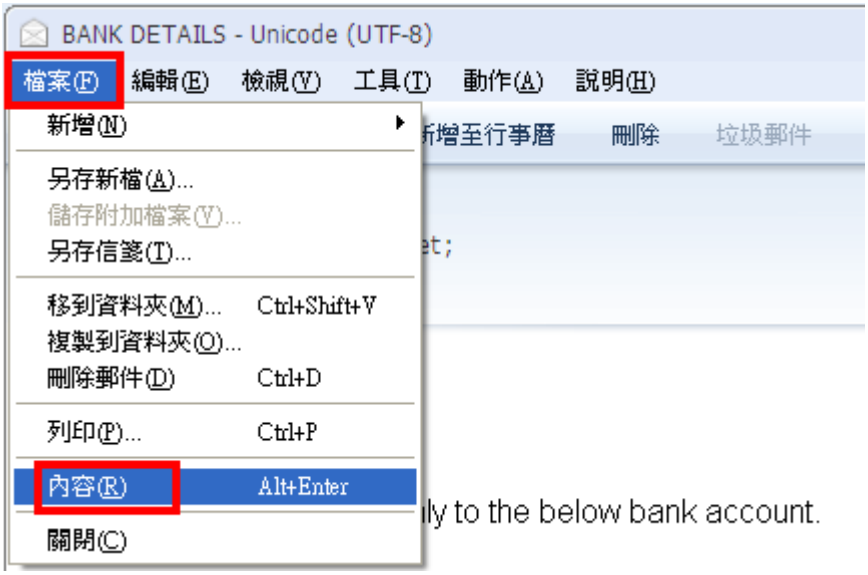
其實公司的管理面問題
當老闆跟管錢的會計真的要特別的注意
公司的帳款流程相當的重要

我們追查了幾件
發現寄件都是僞造的

我們教一下大家怎麼查
不管對方的 E-Mail 信件裝的多熟
當處理錢的問題時

電話和傳真的確認是相當重要的

我們教一下大家怎麼查這封是僞造的信件
不管您是用 Outlook/Outlook Express/Live Mail…
那一種收信軟體
點開信件之後



檔案
內容

詳細資料
郵件原始檔

爲保護受害者我們把關鍵字都 Mark 掉

上面這個圖就是我們常講的郵件表頭
他會記錄這一封 Mail 經過的路徑
這一封 Mail 是 alex 發給 msa.hinet.net
我們查一下他第一個 Received
這是從這台電腦發出的
第二個 Received
這是經過第一台的 Mail server
第二的點很重要
如果貴公司都是用 Free 的 Mail Server
你跟本百口莫辯
人家對方公司一口咬定就是你發的 Mail

人客啊
經營公司不要再省那個錢了
我們公司的 Mail Server 系統很好用
還可以追蹤誰收走那封 Mail
詳洽本公司各區服務處
http://www.ublink.org
help@ublink.org

到第二個 Received 已經可以證明該封 Mail 不是 alex 發出的
如果功力夠的 User
看到最底下的那個紅色區塊
就可以發現
Reply-To:alexchenxxxxx@rocketmail.com
跟僞造寄出的 From:”alex”<alex-chen…..>
已經是不一樣的地方了

這一封已經是明顯的僞造了
但是會有多少的使用者 User 有這等的功力去查這樣的 E-Mail

還是奉勸各位老闆和管錢的會計小姐
電話和傳真確認很重要

處理錢就是小心小心再小心

郵件追追追第三曲

但是客人們又提出問題了

1. 他們是怎麼監聽郵件的
2. MIS/IT 怎麼查郵件 Log
3. 如何讓公司同事在公司外面安全的收信
   甲、家中非信任的電腦
   乙、家中非信任的 ISP 社區寬頻業者
   丙、外面的飯店

要講第一個的時後
門神 JanusLin 要告訴您一個很殘酷的事實
POP3 收信的動作
帳號和密碼的驗證過程是明碼
而且我們只要你的網路封包經過我們設下的點
其實 SMTP 驗證的編碼只要是有心人士還是可以解碼

目前我們觀察到的郵件詐款駭客行爲大部份都是詐騙買方
比如 A 是賣方
B 是買方
兩方當中其實只要去詐騙要付錢的那一邊就可以了
所以通常是 B 買方中槍

而且發現了一個很有趣的問題
有時候甚至兩方都是懂中文的人
還是寫了一堆英文
因爲都是貿易公司
然後駭客也都是很懂英文的人
他的機會就很高了

駭客通常很會等待
等待你們一筆交易快完成到達匯款時
他用假冒的郵件地址介入談話
如第二篇所寫的方式一樣
他叫做 AlexChung
他就用 Alex-Chung 跟你聊

曾有 User 問我
是賣方被入侵嗎

不見得
因爲兩方其實只要聽一方的郵件即可
後面他轉到駭客他自己的郵件地址跟你談就可以了

在第一篇中我們就提出很多的網路使用該注意的事項跟方法了
http://www.ublink.org/index.php/component/content/article/13-apps/409-email.html
但是總還是有很多的例外
比如電腦中木馬

MIS/IT 怎麼查 Log
我們公司所推鑑的 Mail Server 很好查
但是如果您是用 Exchange/Notes/…我們會建議您最好把 pop3/smtp log 開啓來
如果不會操作 Exchange/Notes/…怎麼辦
至少 MIS/IT 應該會有配合的廠商吧
打個電話問一下該怎麼處理應該是 ok 的
或者可以使用側錄設備也 OK
比如我們的 IDR 系列
或是 UTM 系列
或是 SmartMonitor 系列
都可以記錄郵件的收發

IDR POP3 的詳細記錄

UTM 的連線記錄

Vigor SmartMonitor 的畫面
MIS/IT 人員還是需要有好的工具去做分析的

詳細簡報請洽本公司各區服務人員
http://www.ublink.org

更笨的方法
可以把 pop3 封掉
但是一樣沒辦法根治
我們說過了 SMTP 還是可以解碼

那第三點就出現了
如何讓公司同仁能在外面比較安全的收信
首先出門在外我們會建議一定要用有 s 的協定(SSL)
比如 WebMail https
POP3s
SMTPs
IMAPs

但是也會有 MIS/IT 跳出來講
我家的 Mail Server 都沒有安全的 s
該怎麼辦
答案很簡單
看查一下貴公司的 Firewall 防火牆有沒有 VPN 的功能
PPTP/L2TP/IPsec/SSL VPN 都可以

讓同事在外面的時後
可以讓他強制的連 VPN 之後再收發信件就可以了

如果貴公司的防火牆沒有 VPN 功能
簡單
找我們公司一定有

如何降低被對方主機列入 Spam 廣告信的機率

之後又接到 User 使用者詢問
如何降低被對方主機列入 Spam 廣告信的機率

MIS/IT 人員有沒有看過以下的通知

親愛的用戶您好：
　　本公司接獲申訴說明您的電腦(IP：59.125.9.x)
持續對其它用戶或單位發動網路攻擊行爲，並已影響對方主機，
可能爲以下情況所致：

1.電腦中毒
2.遭受駭客入侵成爲跳板
3.網域內有不法份子從事駭客行爲
爲避免不必要之麻煩及危害，敬請盡速予以處理。

貴公司的 Mail Server 常被列入
SBL
PBL
Spamhaus
也算是另類的常客吧 XD

其實我們查過的狀況有下列幾種

1. DNS 設定問題
   DNS 代管無法帶出 SFP
   DNS 代管無法送出 Domain Key
   DNS 代管無法送出 Send-ID
2. IP 不足 256 個 IP 需要向 ISP 申請 PTR 的值，貴公司根本沒申請
3. NS 的設定正確與否
4. IP 不要跟 Firewall 同 IP，以免和電腦跟 Mail Server 上 Internet 同 IP，電腦中毒猛發廣告信或是病毒信
5. Open relay 或是帳號和密碼被猜中，或是根本沒有更改預設的帳號跟密碼，被發廣告信
6. 轉寄發同一份笑話信，或是一直都是重覆的同一封 Mail 重覆發送
7. 大量發廣告行銷信
8. 查無此收件者 User know 的退信讓對方誤以爲攻擊
9. Web Server 主機跟 Mail Server 主機同一個 IP，Web Server 主機用的網站套件有漏洞

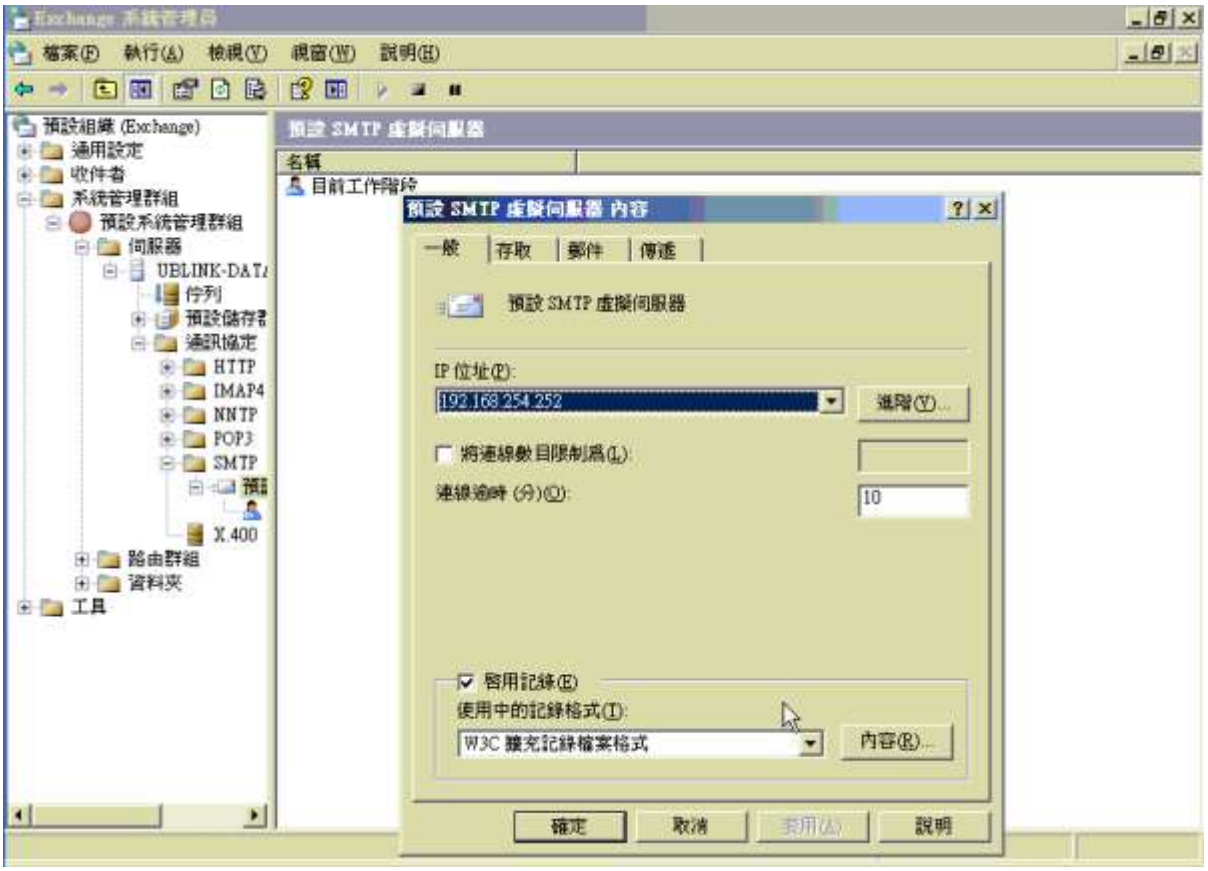
10. 新申請的 IP 早就在黑名單內
11. 發信速度過於頻繁，每秒或是每分鐘超過對方限定的幾次，對方可能有郵件阻斷攻擊服務 Mail-Dos
12. …

我們查過的差不多就是這樣

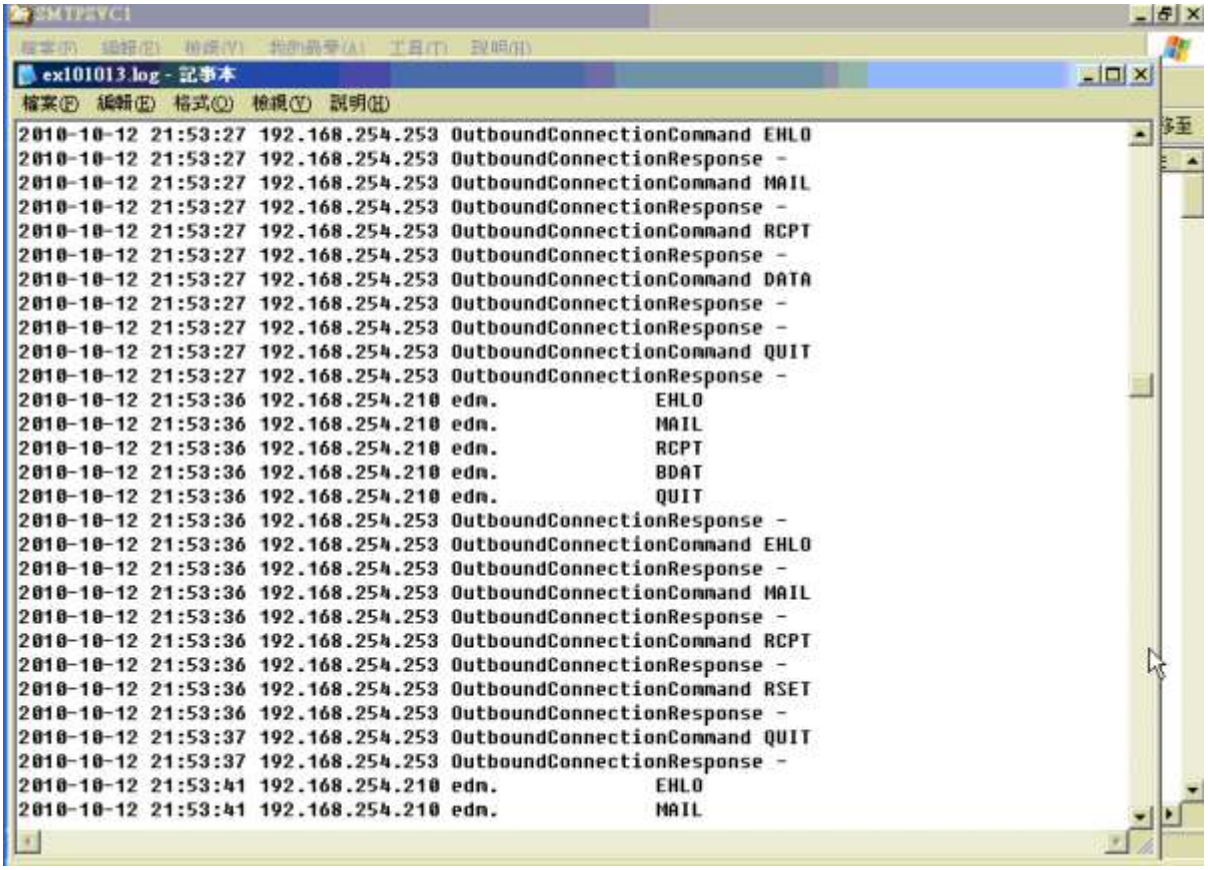
Exchange 爲何有些網域 Q 信一堆郵件追追追第五曲

Exchange 爲何有些網域 Q 信一堆
MIS/IT 人員沒有好的工具還真是痛苦

其實 Exchange 還是有 Log 可以查的



設定的方法

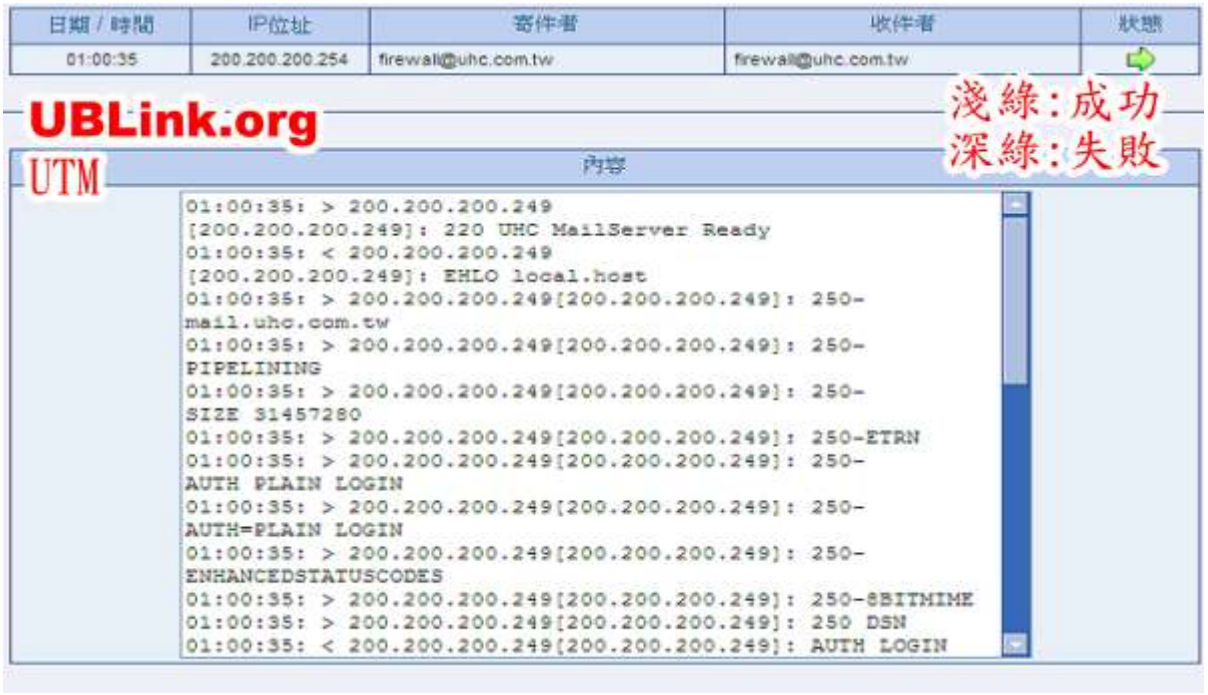


但是一堆文言文

看的懂的有幾個

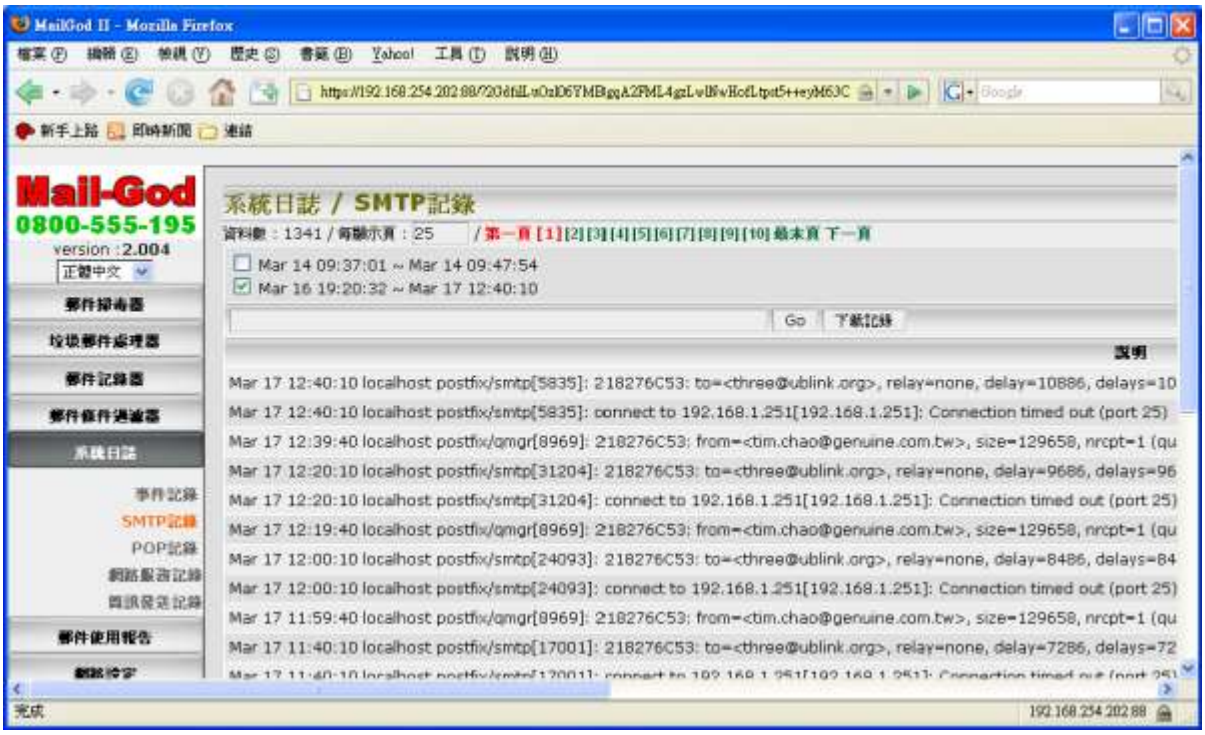
如果有我們公司的 UTM 或是 Mail-God

這 Log 就簡單多了



UTM 系列

Mail-God



Mail-God 連流水帳都有

這樣 UTM/Mail God 查 SMTP Log
是不是比 Exchange 查詢方便多了
而且還可以加統一簽章
做個資法宣言
或是公司簽章

UTM 畫面

Mail-Gog 各 Domain 都可以獨立一個簽章

而且經過的信件還可以指定轉寄

或是備份查詢(UTM-1500 以上含 Mail-God,詳細簡報請洽本公司)

UTM 存檔部份畫面

以上專業設備有詳細的簡報和說明
歡迎洽詢

以上產品如果有其他問題
請洽本公司各區服務處
http://www.ublink.org