個案分析-

釣魚網站(Phishing)分析報告

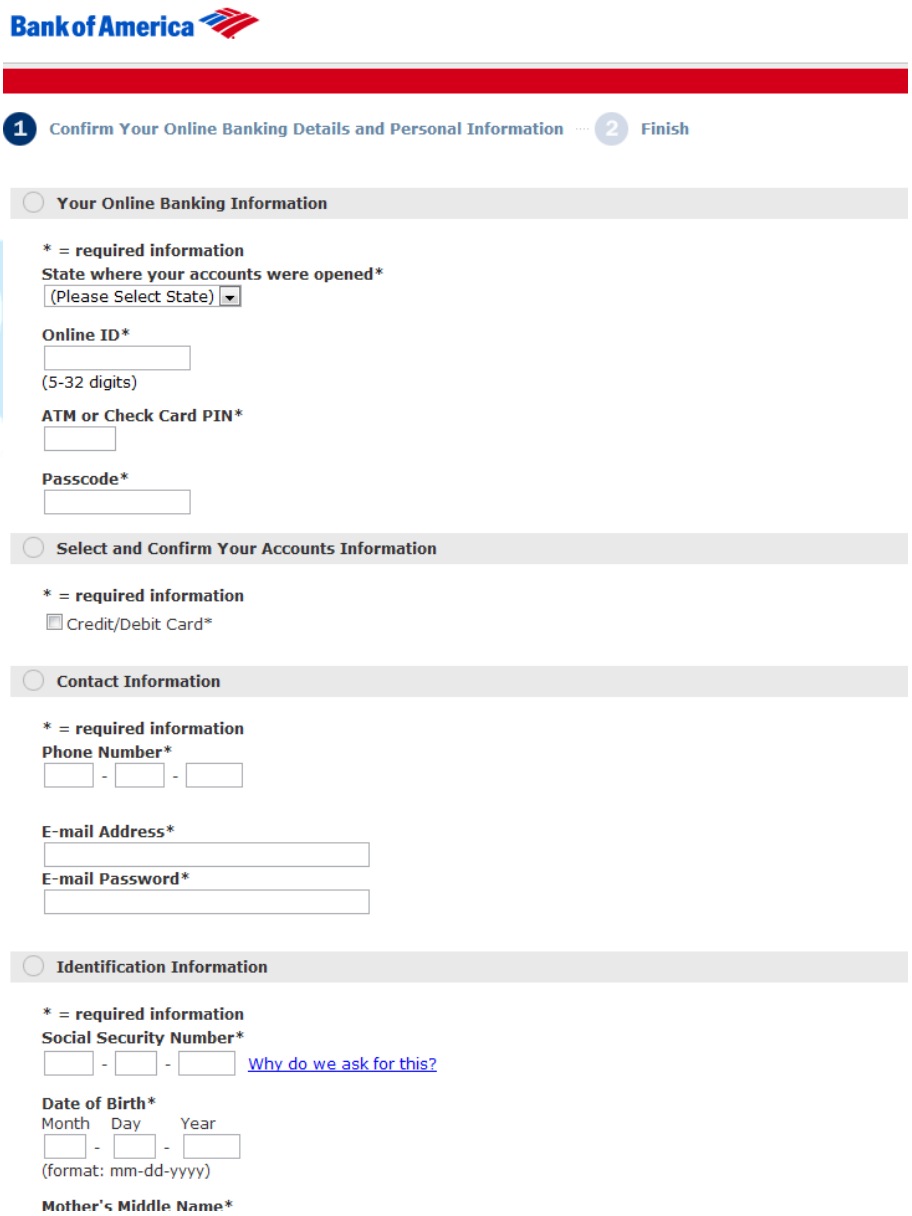
TACERT 臺灣學術網路危機處理中心團隊製

2012/8

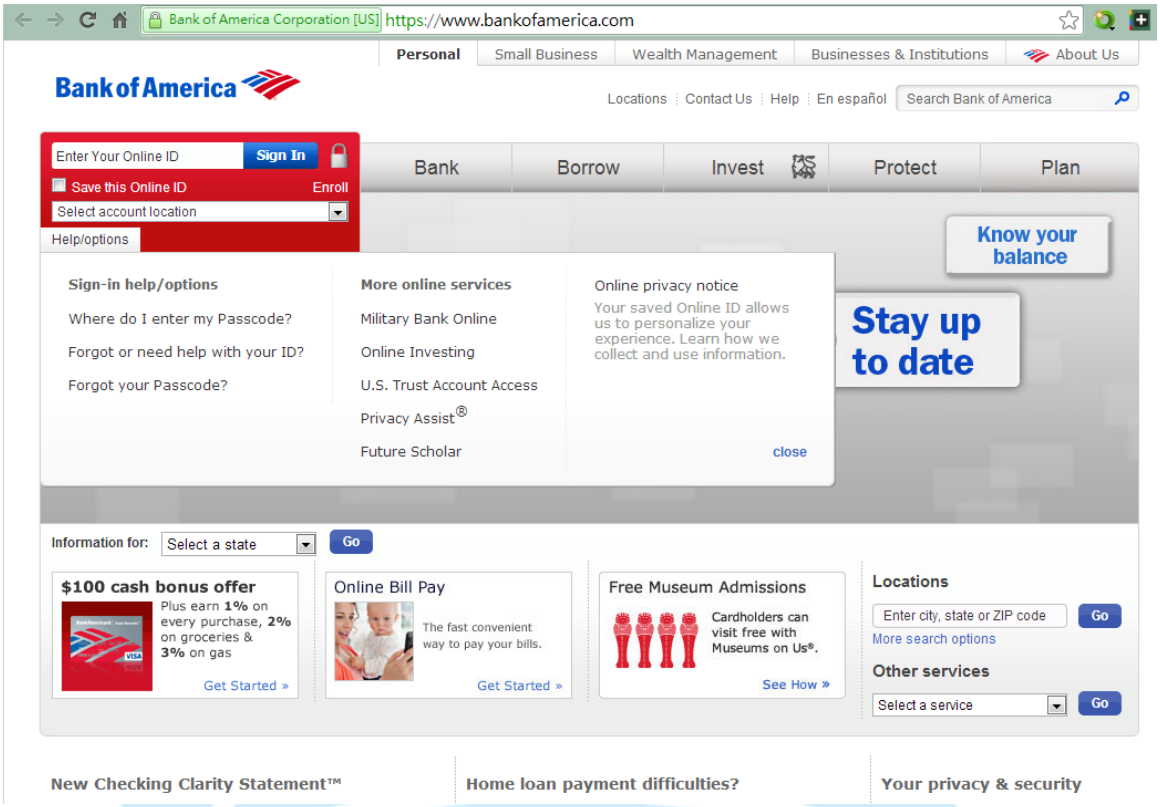
前言

釣魚網頁利用偽造的頁面，讓使用者相信它是合法的網頁，進而輸入個人資料，騙取個資。釣魚網頁風行已久，由於多數人習慣用眼睛辨認頁面，並不會二次確認頁面網址是否正確，導致這種簡單的攻擊手法歷久不衰。

此次事件的釣魚網頁如圖一，其整體配色以及設計與圖二合法的官網是一致的，如果沒有仔細觀察其網址，使用者很難察覺圖一頁面是假的。



圖一 釣魚網頁



圖二 真正的官網

事件說明

釣魚網頁主機為C大學的職員工作機，以下是使用者提供的主機資訊：

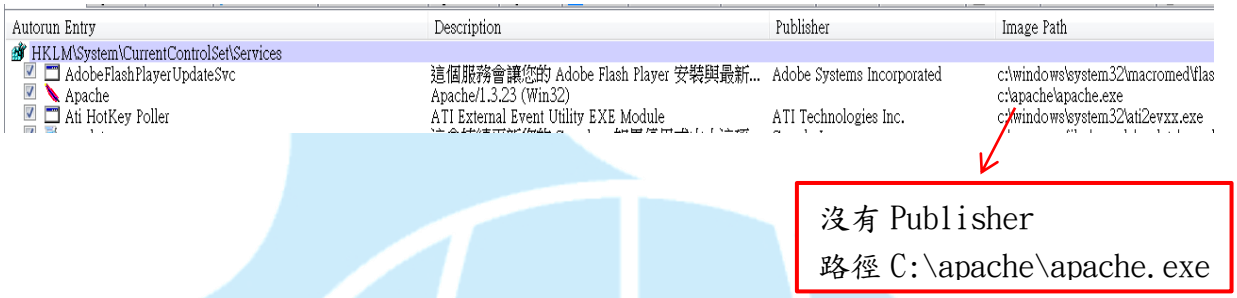
- 位於 C 大學
- IP：140.xxx.121.130
- Windows XP
- 普通文書機
- **沒有安裝網頁伺服器**
- 有安裝防毒 NOD32
- **有開啟遠端登入**

該主機僅是一般使用者的文書機，預設不提供網頁服務，不過其網路狀態確實開啟了80 port，使用該埠號的程式為 Apache.exe，乍看與真正的網頁伺服器apache無異，如圖三。登錄檔上關於Apache的部份Publisher為空白，如圖四。進入主機上的Apache.exe（位於C:\apache\）所在資料夾，裡面有一些異常的檔案，分別用瀏覽器和文字編輯器

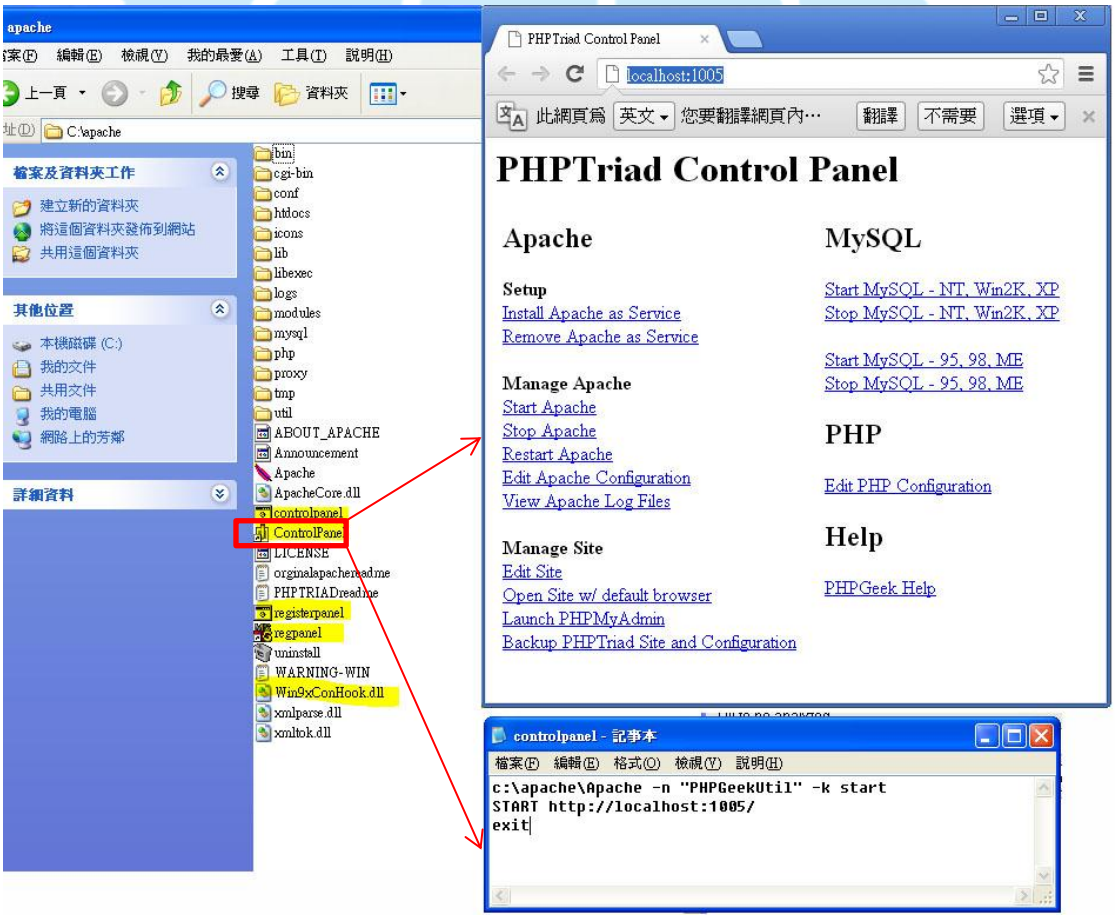
打開之後如圖四，從上面的文字可以看得出來，是控制Apache和 MySql的GUI。

```
C:\Documents and Settings\Administrator>netstat -anob

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       1568
  [Apache.exe]
```

圖三 140.xxx.121.130 網路狀態



圖四 主機上 Apache 沒有 Publisher



圖四 左 140.xxx.121.130 放置 Apache.exe 的資料夾內容；右上 controlpanel 直接點擊的內容；右下 controlpanel 用筆記本打開的內容

初步判斷，這是一個無須安裝直接點擊就可以使用的Apache伺服器，其controlpanel中Setup 項目下的 Install Apache as Service 選項，可以把Apache註冊到登錄檔裡面，使其開機自動執行。由於使用者對自己主機上面的Apache完全沒有印象，加上該主機開啟了遠端桌面，使用簡單帳號密碼，C槽有apache.rar，故推測駭客可能是由遠端桌面登入之後，下載apache.rar，手動解壓縮進行Apache安裝，設置釣魚網頁相關設定。

結論

弱密碼一直是資訊安全上面很大的弱點，無論硬體設備以及技術如何進步，人為的密碼設定礙於記憶不便，一直都有強度不夠的問題，本次例子即為一例。建議登入主機的密碼一定要高強度，一旦使用弱密碼被猜測出來，等同於整台主機使用者交到駭客手上。