優易資訊股份有限公司
SECURTEC
Professional Service Corporation

社交工程的介紹與防範

優易資訊　溫廷彰

什麼是木馬程式(特洛依)

基本是它是一個遠端控制的程式，程式本身可分為二個部份:

主控端:這部份是安裝在駭客端的程式，主要是用來控制已被植入木馬的電腦。 

被控端:這部份就是一般使用者被植入的程式，也就是大家所謂木馬程式，其主要用途是開啟電腦中的服務埠，以便讓駭客能夠在遠端操控這部電腦。 

木馬程式的特性一

- 開機時自動啟動
  - 多數的木馬程式均為此種類型，這樣一來駭客便能夠有較多的機會去入侵使用者的電腦。
  - 有另一類型的木馬為事件啟動型的木馬，也就是它不會在開機時啟動，而是當條件符合駭客事先設定的狀況時，它便會將程式啟動。(此類型的木馬較不易被查覺)

- 自身隱藏的能力
  - Windows的環境下，可用Ctrl+Alt+Del叫出工作管理員中的處理程序，它會將目前系統正在運行的所有程序顯示出來。
    針對這個部份，木馬程式已發展出新的技術，就算使用上述的方法你也無法查出它的存在。

- 開啟服務埠
  - 為了讓駭客能夠達到遠端操控的目的，木馬程式啟動後便會開啟一個服務埠，這個服務埠通常都在1024以上，這是為了降低木馬在執行中發生錯誤的機率。

木馬程式的特性二

- 自動恢復
  - 此類型的木馬程式會將運行的程式及來源程式分開存放，當你把運行中的木馬刪除後，它會自動由來源程式再複製一份，所以此類型的木馬要將其完全刪除必須找出其複製程序，並將來源檔一並刪除。

- 干擾系統防護軟體的運作
  - 此類型的木馬程式當其運行時，會將系統上所安裝的防護軟體(例如:防毒軟體)關閉或刪除，以避免其程式被防護軟體所偵測到。另外有些木馬程式為了不讓使用者發現其防毒軟體有異狀，會先將防毒軟體關閉後刪除，而且會將Logo替換掉，當下次電腦重新啟動後，雖然實際上已經沒有防毒軟體存在，但是使用者依然可看到其Logo出現，便會以為防毒軟體還是正常在運作。

為什麼會中木馬

這是一個耐人尋味的好問題，很多使用者都認為我的防毒碼都有定期更新、我有防火牆的保護、我不會開啟不明的郵件…，所以木馬應該就騎不到我頭上了吧，上述的條件只是一般的基本防護，就算你有這些基本的防護但是現在的駭客也都了解使用者的防護機制，所以木馬程式的開發都以破解這些防護機制為基礎。

因此有很多的企業儘管內部已經是萬馬奔騰  的狀況，但是使用者依然在防護措施完備的迷思下而不自知，當情況真正被發現後通常已經對企業造成了非常大的傷害。

基本上大部份的木馬程式並不像病毒程式一樣會有自我複製並且感染其它電腦的能力，所以它一定要讓使用者在不知情的狀況下去執行它的程式。這裏要強調的是在這個階段就是很多使用者會疏忽掉的地方，一旦執行了它你的惡夢就開始了。

駭客通常利用哪些方式呢

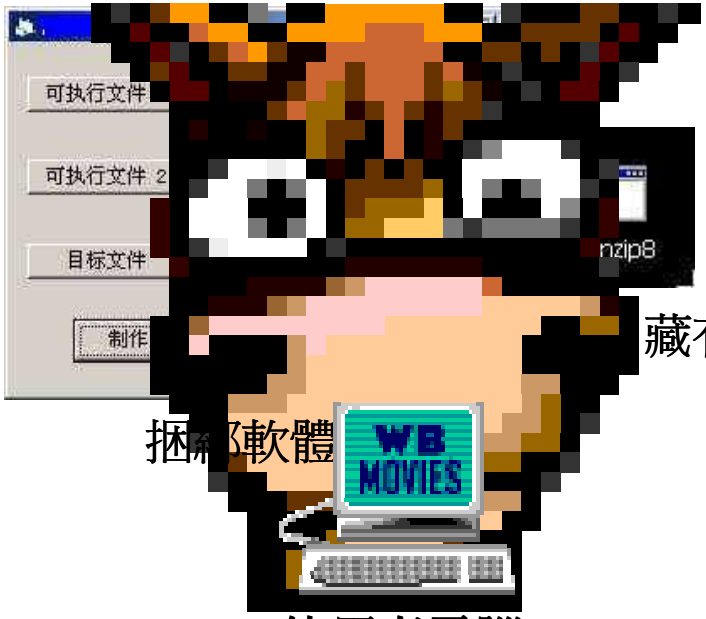
下列的方式為駭客較常使用方式:

- 惡意網頁/郵件
- 軟體的下載
- 社交工程
- 內部滲透

軟體的捆綁

正常程式

木馬程式



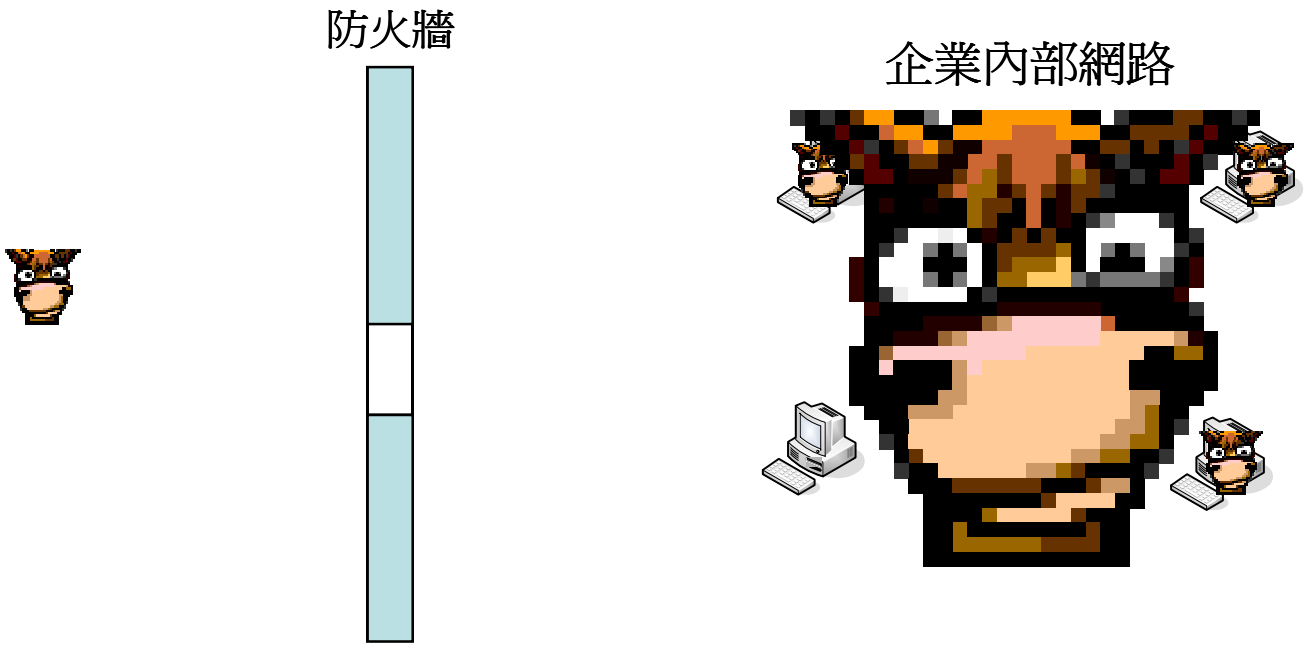
捆綁軟體

藏有木馬的軟體

使用者電腦

內部滲透

通常當木馬成功的植入企業內部的某一台電腦後，企業的災難也就跟著發生了。這就等於你把一位駭客放在公司內部，也因為企業內部的安全防禦措施通常都比較不足，因此駭客能夠使用更多手法去擴增自己的領土，以便能夠竊取更多的資料。



內部滲透的媒介

SECURTEC
Professional Service

- 網路上的芳鄰

  這是一般企業內部最常疏忽的地方，為了讓檔案傳輸上的方便，很多的企業都會開啟這個服務，這也等於每台電腦都開啟了一扇大門。

- 檔案伺服器

  將木馬程式捆綁在Server上的某一個檔案供使用者下載，這部份的傷害力最大，因為使用者不會懷疑公司檔案伺服器上的檔案，通常下載後就直接安裝或開啟了。

- 電子郵件

  取得內部組織的郵件清單後，將木馬程式大量的寄送給使用者，這樣一來便能夠讓駭客在短時間內控制大量的電腦。

- 主機上的漏洞

  主要是針對伺服器，因為伺服器通常不會用來收取信件或下載一些小軟體，因此駭客便會利用系統上的漏洞進而入侵該部主機。

什麼是社交工程

很多人對於”社交工程”這四個字不是很熟悉，基本上它是利用人與人之間的關係，所以它是偽冒成使用者信任的來源，例如家人、同事、長官….等等。駭客便是利用這一點偽裝成可信任的寄件者，然後將木馬程式夾在e-mail中，當使用者收到這封信時因為寄件者是他所信任的人，因此對於附件的檔案較無警戒心，一旦開啟附件後木馬就順利植入了。

這裏一定會有人認為”只要附件中是執行檔就絕不開啟”是不是就沒事了，答案是否定的，因為駭客也知道以執行檔的類型是騙不到使用者的， 因此目前的型態是將木馬藏在文件或圖檔、影音檔中，這樣一來就成功的機率就大為增加了。

您有沒有打開過類似的郵件

SECURTEC Professional Service

郵件主旨:超級美食任務-1~40集店家一覽表

超級美食任務

	A	B	C	D	E
1	超級美食任務第一集到第四十集美食一覽表				
2	美食	店名	電話	縣市	地址
3	魚頭	新天地海產	(04)6562222	台中縣	台中港梧棲路159號
4	粿	燒炸粿	(04)6882369	台中縣	台中縣大甲鎮文武路37號
5	餅	大甲奶油酥餅(裕珍馨)	(04)6810969,6872559	台中縣	台中縣大甲鎮光明路6914號
6	羹	中港海鮮樓(杏菜吻魚羹)	(04)6561888,6578888	台中縣	台中縣梧棲鎮中興路20號
7	肉圓	白頭菜清水肉圓	(04)6232592	台中縣	台中縣清水鎮中山路187號(台中商銀對面)
8	鴨	東山鴨頭	(04)6313672	台中縣	台中縣龍井鄉東海別墅泳池巷5號
9	點心	龍井蜜汁蕃薯	(04)6313675	台中縣	台中縣龍井鄉新東村中港路99號
10	冰品	東海蓮心冰	(04)6320182	台中縣	台中縣龍井鄉新興路一巷1號
11	麵	王家麵館	(02)27319148	台北市	台北市八德路二段273號
12	螃蟹	蟹大王奶油螃蟹	(02)27717641, 27512663	台北市	台北市八德路二段325號
13	粽子	王記肉粽	(02)27754032	台北市	台北市八德路二段413號
14	羹	炒花枝羹		台北市	台北市士林夜市
15	腸	富利得利(德國乳酪香腸)	(02)28312741	台北市	台北市士林區克強路17號
16	包子	大樹下小饅頭	(02)28617242	台北市	台北市士林區菁山路平菁街9號
17	意大利菜	PianoPiano(皮亞諾.琵雅挪)	(02)27016860	台北市	台北市大安區四維路208巷10號一樓
18	腸	紅花香腸	(02)27330987	台北市	台北市大安區通化街225號1樓
19	麵	高麗棒韓國料理	(02)27728649	台北市	台北市大安路一段51巷40號
20	燒烤	好吃國	(02)27733003	台北市	台北市大安路一段73號2樓
21	日本料理	玫瑰緣別館	(02)28381779	台北市	台北市大安路一段83巷8號
22	米粉	星洲炒米粉	(02)25331717	台北市	台北市大直北安路535之一號
23	雞	雞家莊本店	(02)25815954, 25514068	台北市	台北市中山北路一段105巷
24	明星開的店	青葉	(02)25517957	台北市	台北市中山北路一段105巷1號
25	日本料理	瀧乃園	(02)25230339, 25236567	台北市	台北市中山北路二段50巷15號
26	肉圓	彰化涼圓	(02)25311566, (047)244810	台北市	台北市中山北路二段65巷35號
27	火鍋	箱根日本料理	(02)2521305, (02)125811330	台北市	台北市中山北路二段65巷6號
28	日本料理	玫瑰緣別館(分店)	(02)27216688	台北市	台北市中山北路六段268號

您有沒有打開過類似的郵件

郵件主旨:美麗的漁人碼頭夕陽

社交工程最大的幫手

社交工程的攻擊手法之所以成為駭客最喜歡使用的手法，其原因大概有下列幾個:

1、使用者難以防範

2、可以進行大量式的攻擊

3、技術門檻不高

4、使用者會協助攻擊

而社交工程最大的幫手就是第四項，各位一定會覺得很奇怪，為什麼使用者會協助駭客進行攻擊呢?原因就是大家都抱持著好東西要與好朋友分享的觀念，因此常常收到信件時甚至還沒看過就轉寄給親朋好友了。因此駭客只要有幾封信件成功的寄入企業中，通常在很短的時間內大部份的員工應該都會收到該封惡意郵件。

社交工程成功後能做什麼

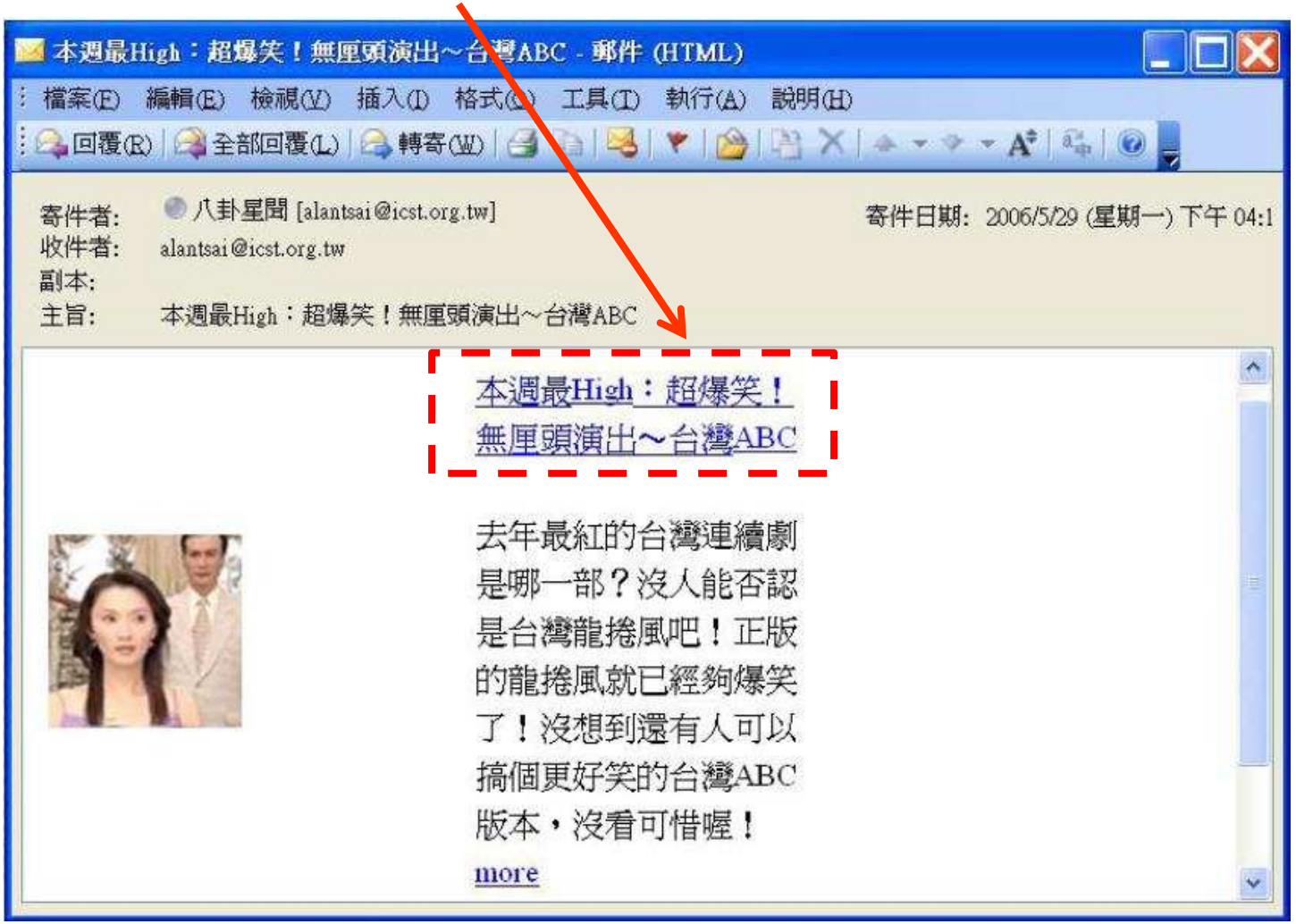
如果駭客的社交工程攻擊成功後，到底對我的電腦有什麼影響呢?這個問題的答案有N種，簡單來說你這台電腦的主控權已經交給駭客了，他想做什麼都可以。

當你的電腦被社交工程攻擊成功後，大概會有下列幾種常見的結果:

1、垃圾郵件發信主機
2、機密資料外洩
3、攻擊他人主機的跳板
4、非法資料的存放主機

社交工程信件範例-八卦主旨

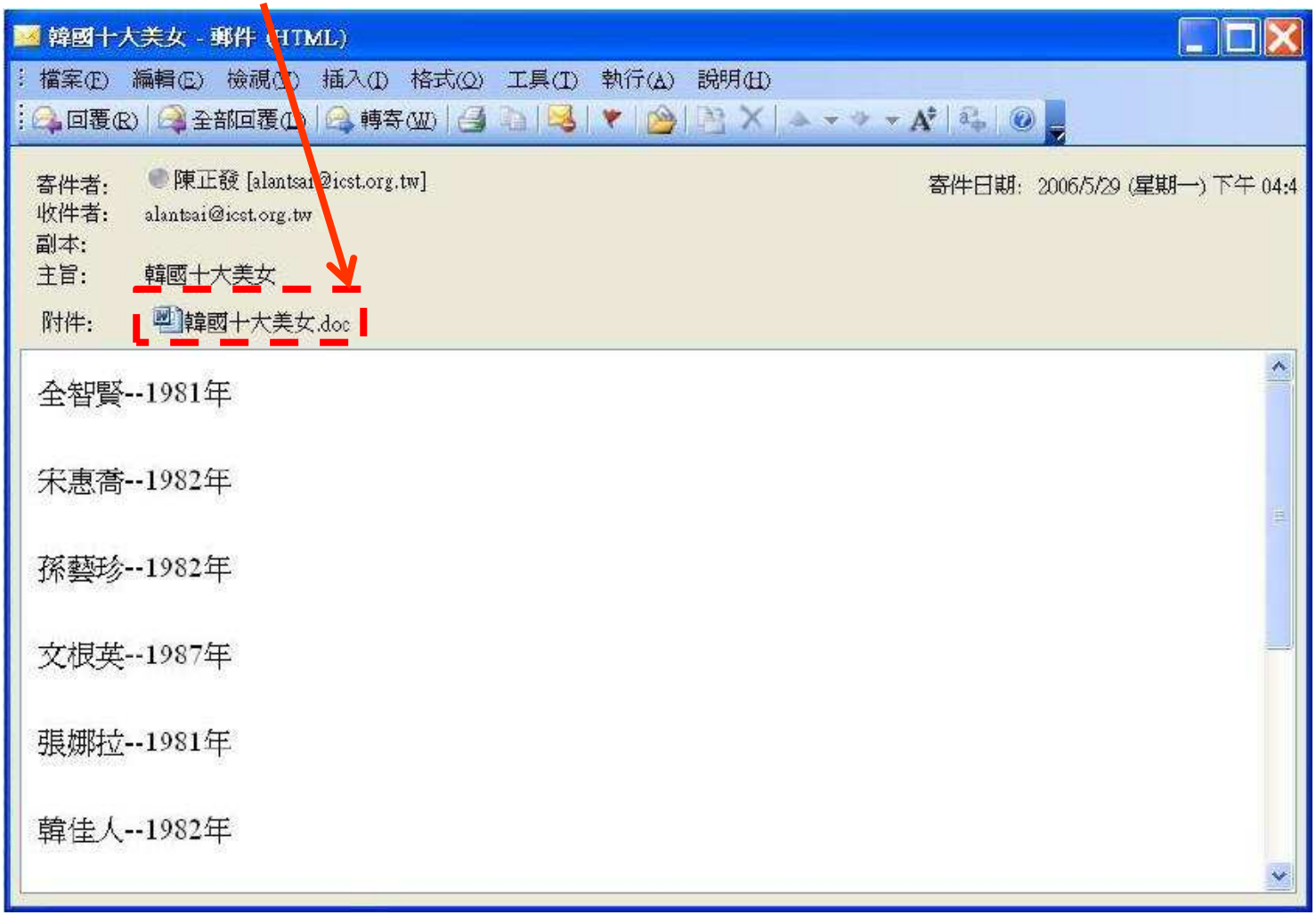
攻擊類型:惡意網頁連結



資料來源:國家資通安全會報

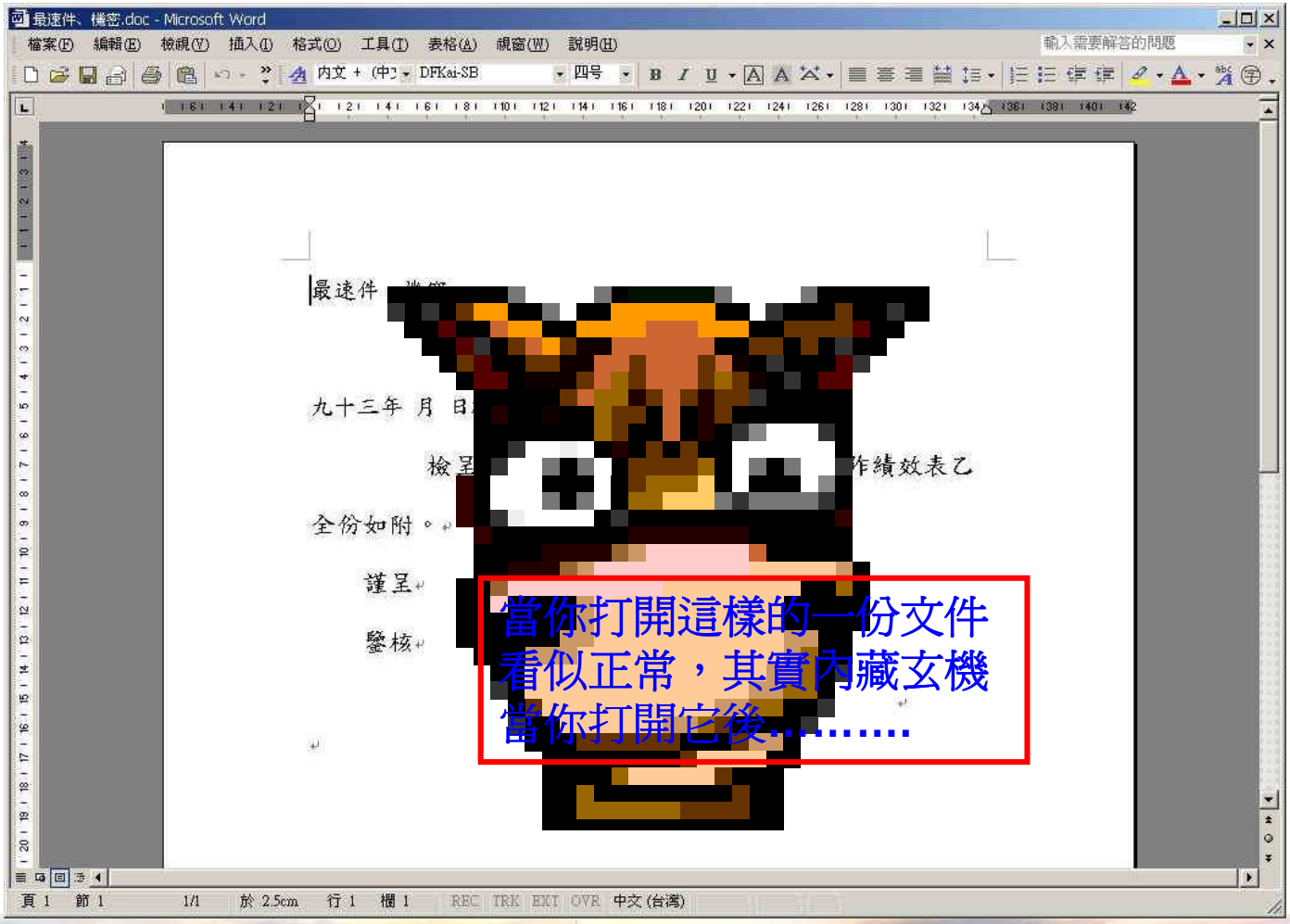
社交工程信件範例-八卦主旨

攻擊類型:惡意Word檔

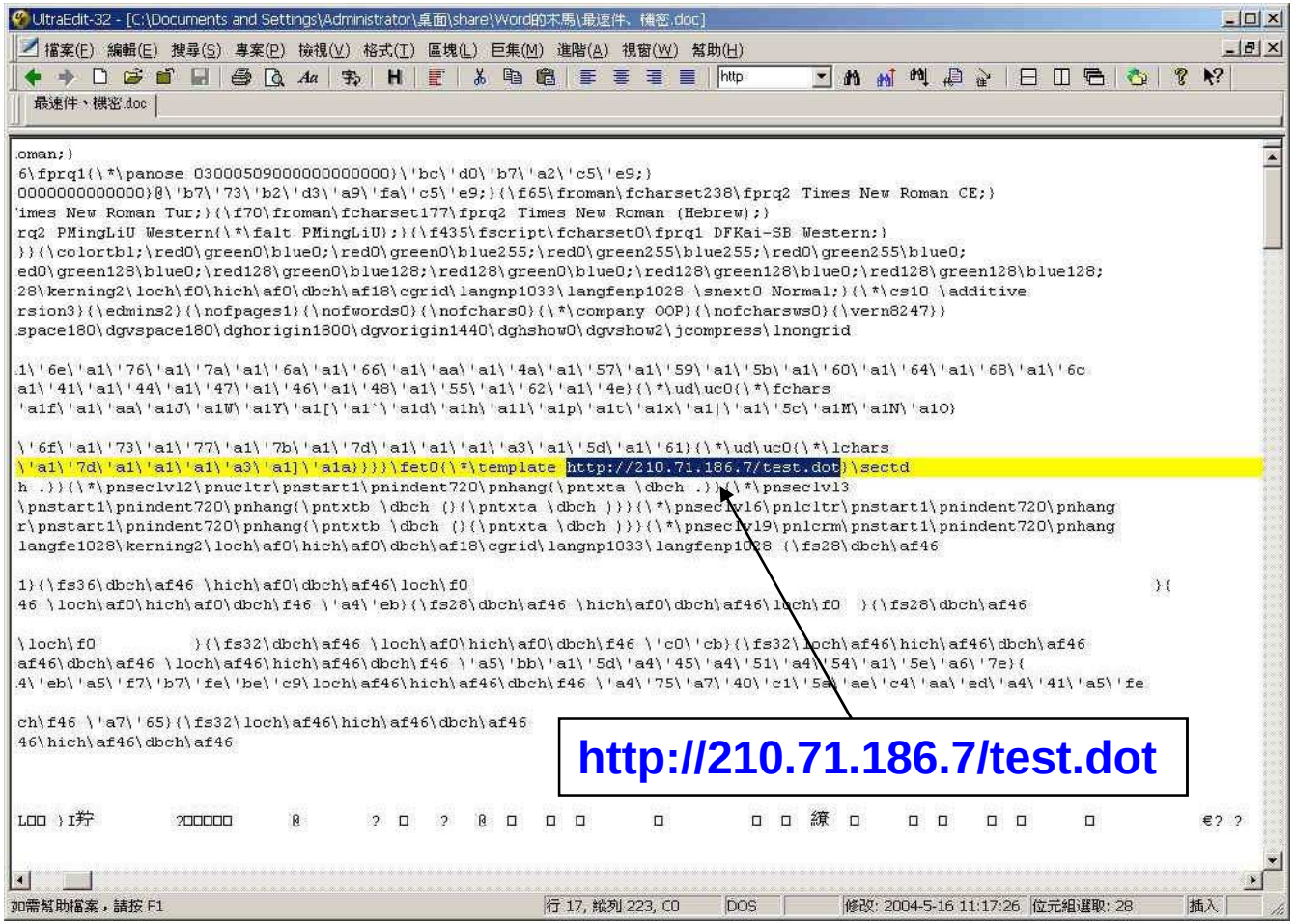


資料來源:國家資通安全會報

文件型木馬

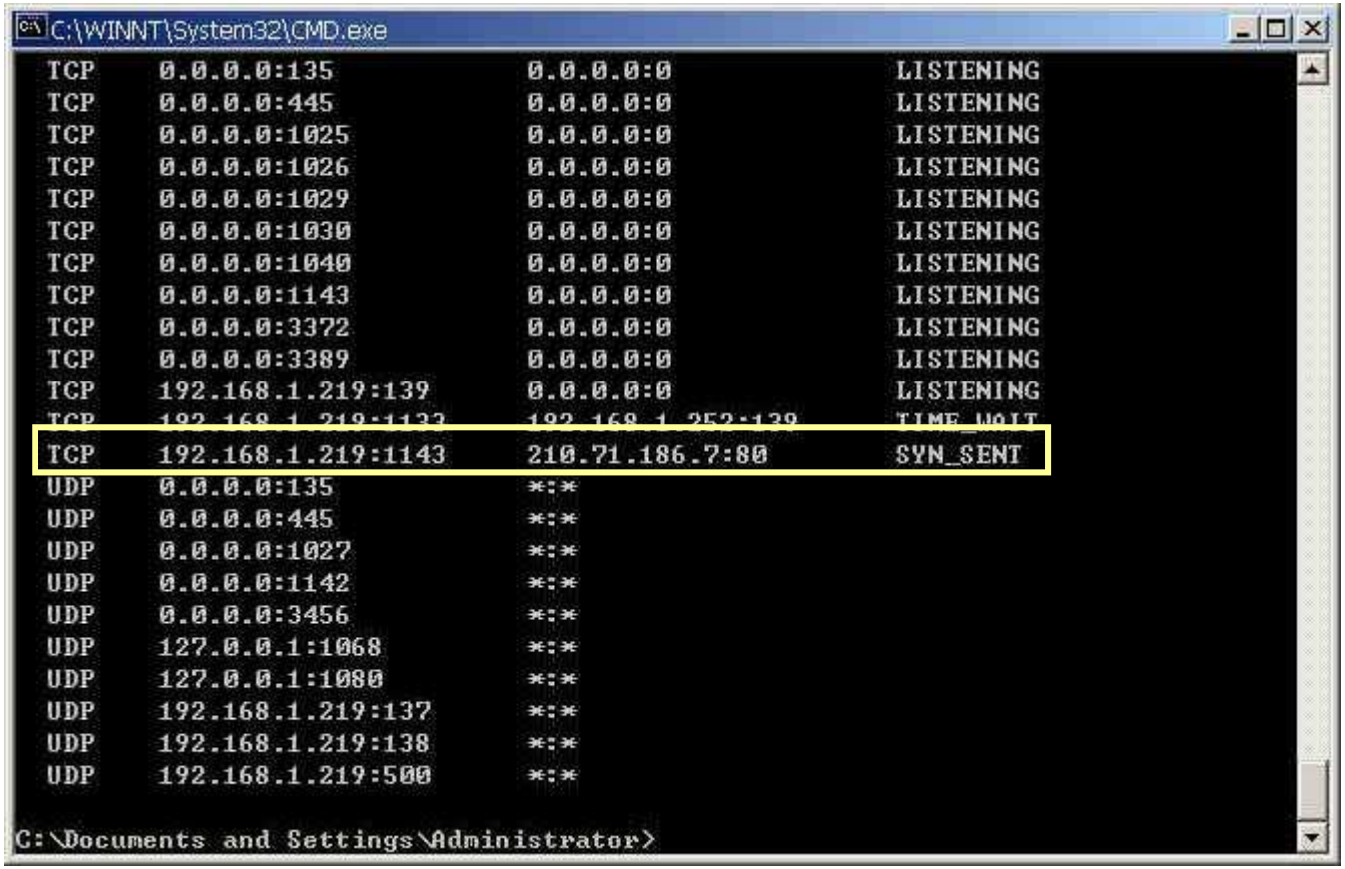

最速件、機密.doc - Microsoft Word
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 表格(A) 視窗(W) 說明(H)
輸入需要解答的問題
最速件
九十三年 月 日
檢呈
作績效表乙
全份如附。
謹呈
鑒核
當你打開這樣的一份文件
看似正常，其實內藏玄機
當你打開它後.....
頁 1 節 1 1/1 於 2.5cm 行 1 欄 1 REC TRK EXT OVR 中文(台灣)

文件木馬的剖析



用**Ultraedit**將其打開，可看到內部藏有一個**http**的連結

文件木馬的剖析



用**netstat**查看後發現它開始連線了

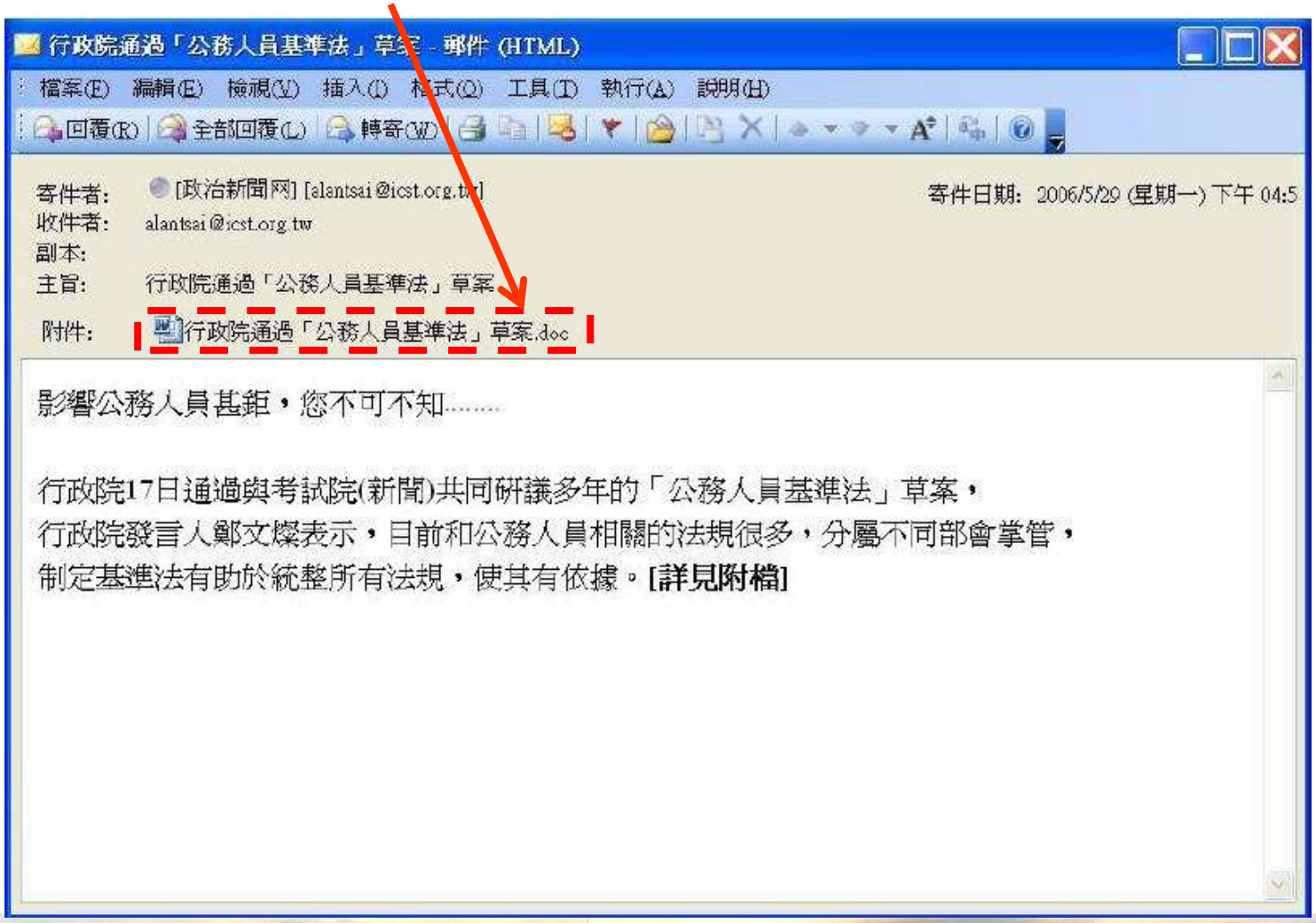
社交工程信件範例-情色主旨

攻擊類型:惡意圖片檔

資料來源:國家資通安全會報

社交工程信件範例-政治主旨

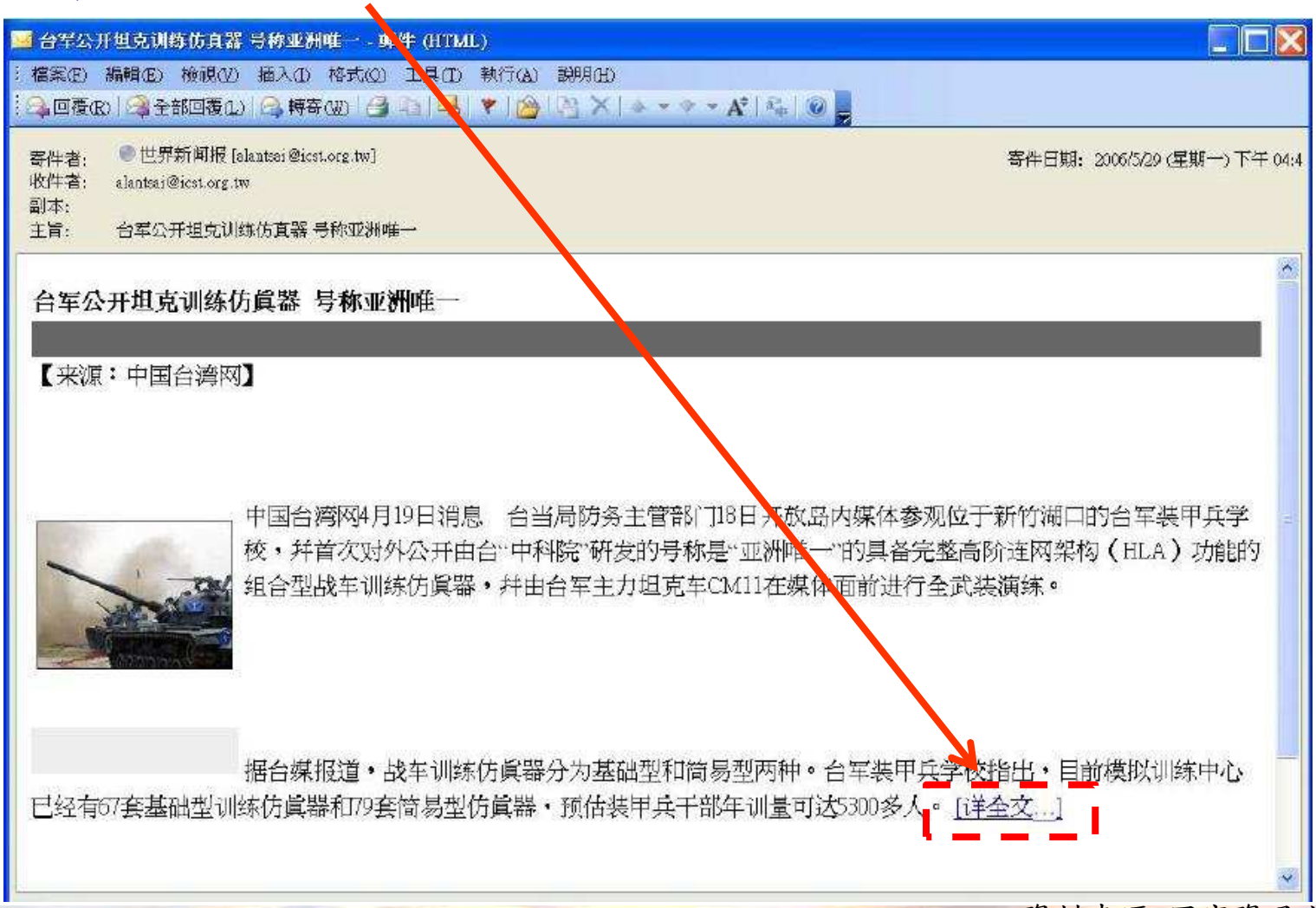
攻擊類型:惡意Word檔



資料來源:國家資通安全會報

社交工程信件範例-政治主旨

攻擊類型:惡意網頁連結



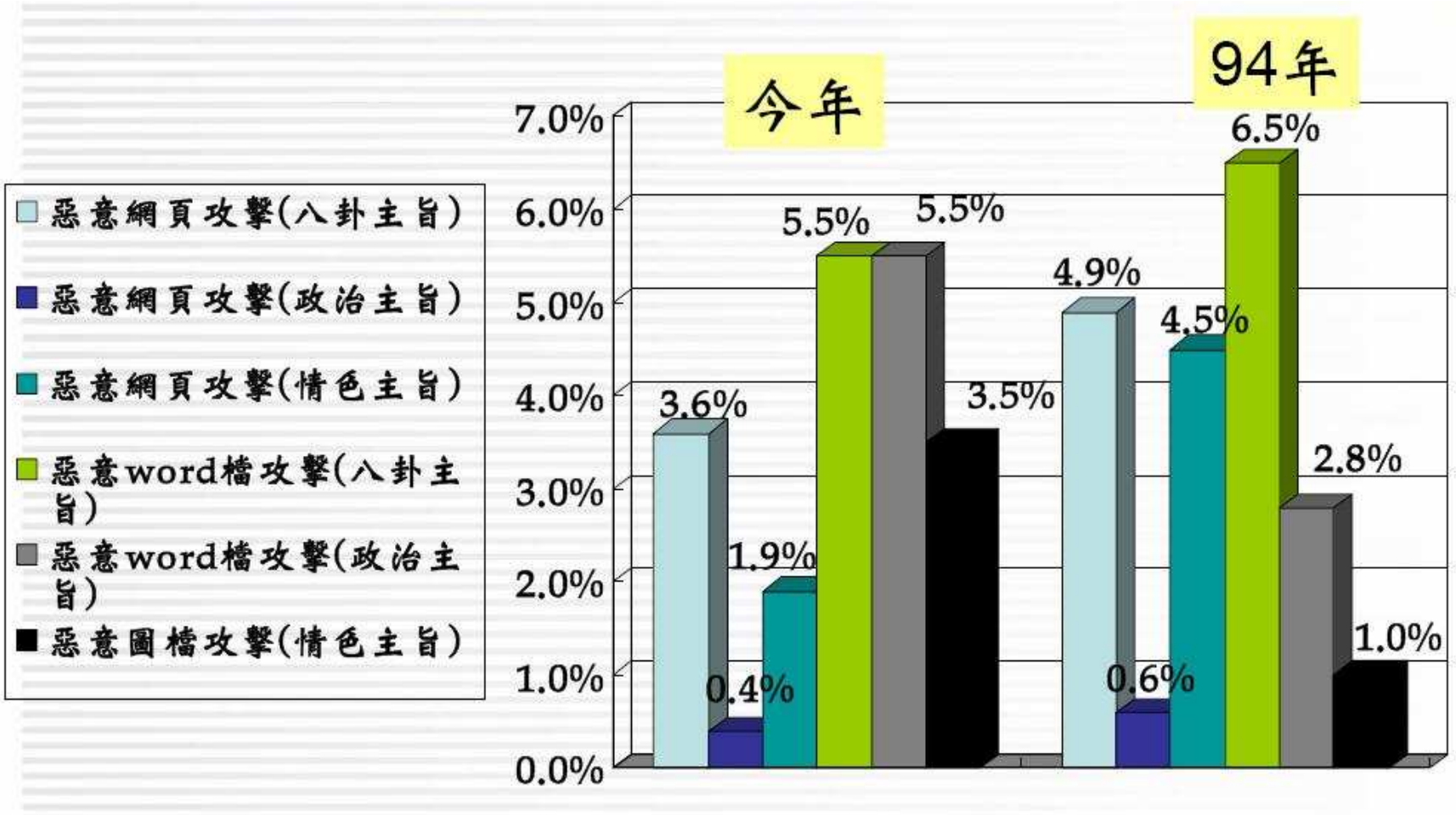
資料來源:國家資通安全會報

社交工程攻防演練成果

- 演練目的：測試資安聯絡人資安警覺意識
- 測試對象：6,630 政府機關，13,575位資安聯絡人
- 總發信量：81,450封
- 寄發六種社交工程信件類型：
  - 惡意網頁攻擊(八卦主旨)
  - 惡意網頁攻擊(政治主旨)
  - 惡意網頁攻擊(情色主旨)
  - 惡意word檔攻擊(八卦主旨)
  - 惡意word檔攻擊(政治主旨)
  - 惡意圖檔攻擊(情色主旨)

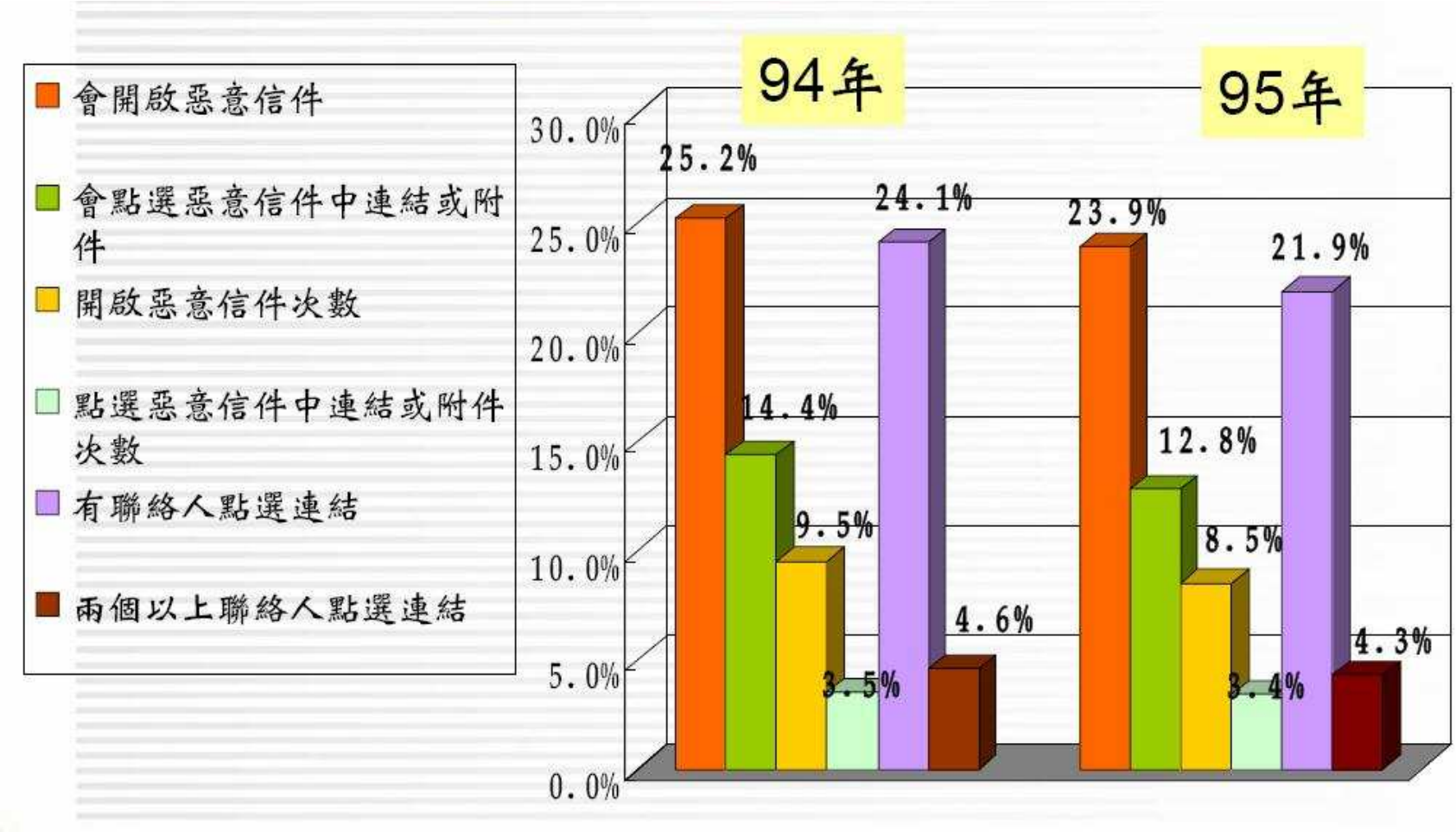
資料來源:國家資通安全會報

社交工程演練結果統計



資料來源:國家資通安全會報

社交工程演練結果統計

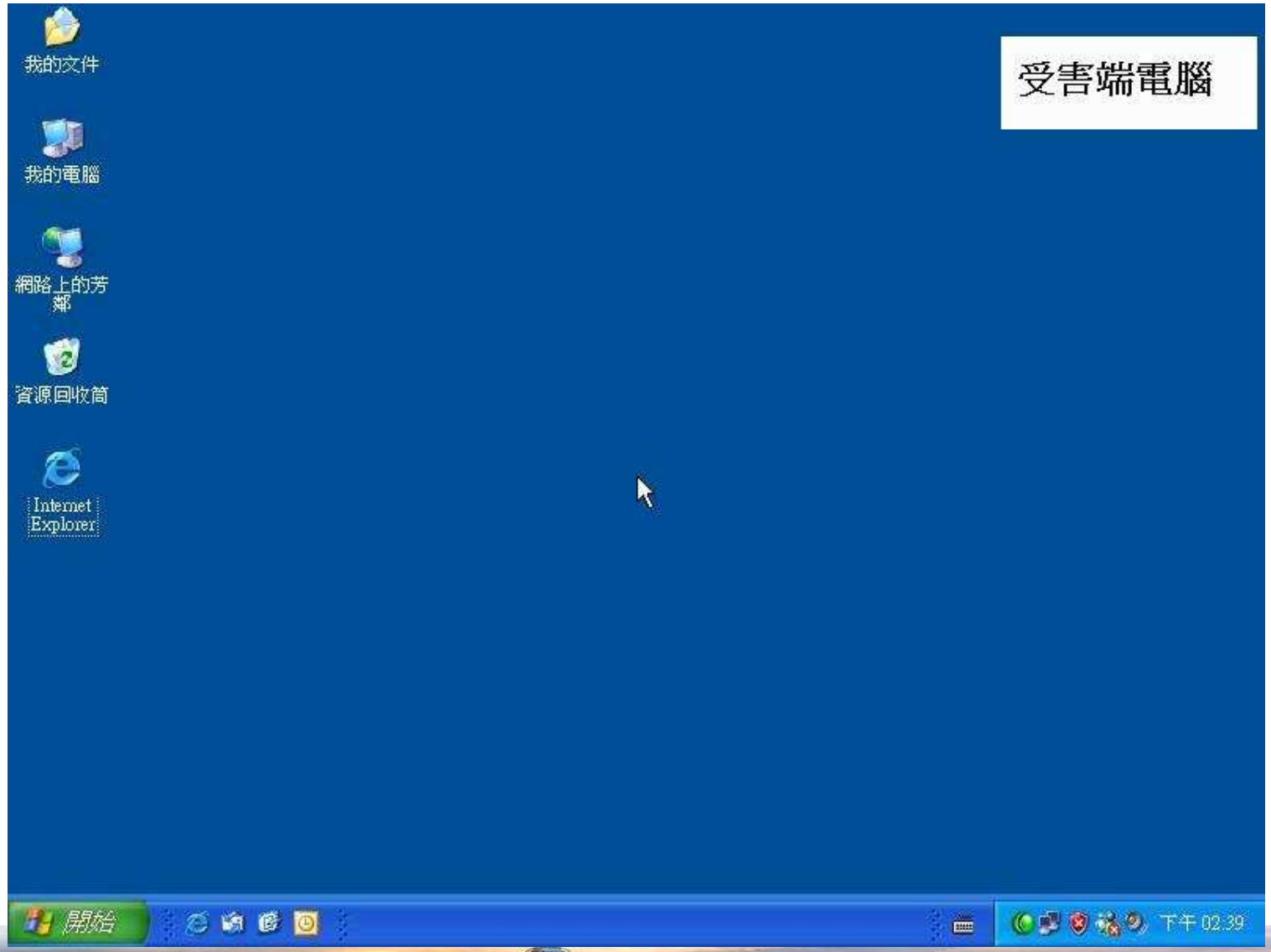


資料來源:國家資通安全會報

網頁惡意鏈結展示影片

示範影片

社交工程展示影片



如何防範社交工程

這個問題最好的解決方案就是良好的使用習慣，不論收到的郵件內容為何，社交工程的本質就是詐騙，因此有下列幾點給大家參考:

- 絕不開啟跟自己無關的郵件及附件檔
- 不隨便開啟郵件中的超鏈結
- 不要任意的轉寄信件
- 不要任意的安裝軟體
- 不要貪圖小便宜
- 安裝個人防火牆