台北海洋技術學院

Taipei College of Miritime Technology

104 學年度資訊安全認知講座

時間:105 年 3 月 11 日 上午 9:00~12:00

地點:台北海洋技術學院淡水校本部謙禧樓 A202 電腦教室

講師:協科資訊 張英傑 先生

資安威脅無所不在

張英傑 Jesse Chang
協科資訊 資深技術顧問
專業證照：CEH , CHFI , EnCE , ISO25999

Agenda

- 密碼管理的重要性
- 都是病毒惹的禍
- 不可不知的社交工程
- APT攻擊的威脅
- 行動裝置的攻擊與日俱增
- 日益猖獗的勒索病毒
- 聯合防禦解決方案
- Q&A

遭到駭客入侵/病毒感染的代價

立即的影響	• 清除與復原的花費
中期的影響	• 客戶資料的外洩 • 鉅額的罰款與法律訴訟 • 高階管理階層人事異動
長期的影響	• 智慧財產權的損失 • 品牌與商譽的損失 • 投資信譽評級下調

SOPHOS

密碼的重要性

- 系統登入
- 網路購物
- 網路ATM

沒有不能破解的密碼

監視器還拍下，嫌犯拿著偷來的提款卡，
粗心的男大學生，把提款卡放在機車的置
生日，難怪竊賊同時偷了身分證及提款卡

高雄覺民所所長阮豐洋：「機車的置物箱
內，犯下一件竊盜案件所穿著的外套，一

竊賊以偷竊維生，偷遍高雄超商賣場，看
廂內的皮包和提款卡，不過賊星該敗因為

Dec 06 Fri 2013 駭客大動作Facebook Gmail等200萬帳戶密碼遭竊

分享 喀嚓 讚 0

讚 成為你朋友中第一個說這讚的人。

您是臉書(Facebook)、谷歌(Google)、雅虎(Yahoo)、推特(Twitter)的用戶嗎？那您可得注意了，網路安全公司Trustwave表示，上述公司遭駭客竊取近200萬組的帳戶名號和密碼。

CNNMoney和今日美國報12月4日報導，駭客在全球電腦安裝惡意軟體，側錄鍵盤輸入資訊；病毒會紀錄各大網站的登入個資，將帳戶名稱密碼回傳至遭駭客操控的伺服器。

11月24日，Trustwave追蹤到位於荷蘭伺服器，遭駭客操縱，發現共有93000個網站受到影響，其中臉書遭竊帳戶達31.8萬個，谷歌旗下網站(Gmail、Google+、YouTube)達7萬個，雅虎也有6萬帳戶受害。

照片

常見的密碼

#	Password	Change from 2011
1	password	Unchanged
2	123456	Unchanged
3	12345678	Unchanged
4	abc123	Up 1
5	qwerty	Down 1
6	monkey	Unchanged
7	letmein	Up 1
8	dragon	Up 2
9	111111	Up 3
10	baseball	Up 1
11	iloveyou	Up 2
12	trustno1	Down 3
13	1234567	Down 6
14	sunshine	Up 1
15	master	Down 1
16	123123	Up 4
17	welcome	New
18	shadow	Up 1
19	ashley	Down 3
20	football	Up 5
21	jesus	New
22	michael	Up 2
23	ninja	New
24	mustang	New
25	password1	New

密碼強度

- 密碼複雜度
  - 0 ~ 9
  - A ~ Z
  - a ~ z
  - 特殊字元(!@#$%^&*……)
- 密碼長度
- 定期更換

你的密碼有多強

- 測試一下你的密碼有多強

https://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html

暴力破解

電腦運算能力：每秒計算 10,000,000 次

字元組合	密碼長度	密碼組合	破解速度
0 ~ 9	8	100,000,000	**10秒**
A ~ Z / a ~ z	8	208,827,064,576	**6小時**
0 ~ 9 + A ~ Z + a ~ z	8	218,340,105,584,896	**7個月**

密碼保存

- 貼在螢幕邊
- 寫在筆記本
- 儲存在瀏覽器
- 儲存在檔案
- 儲存在密碼保存軟體

揭秘軟體30秒揭露

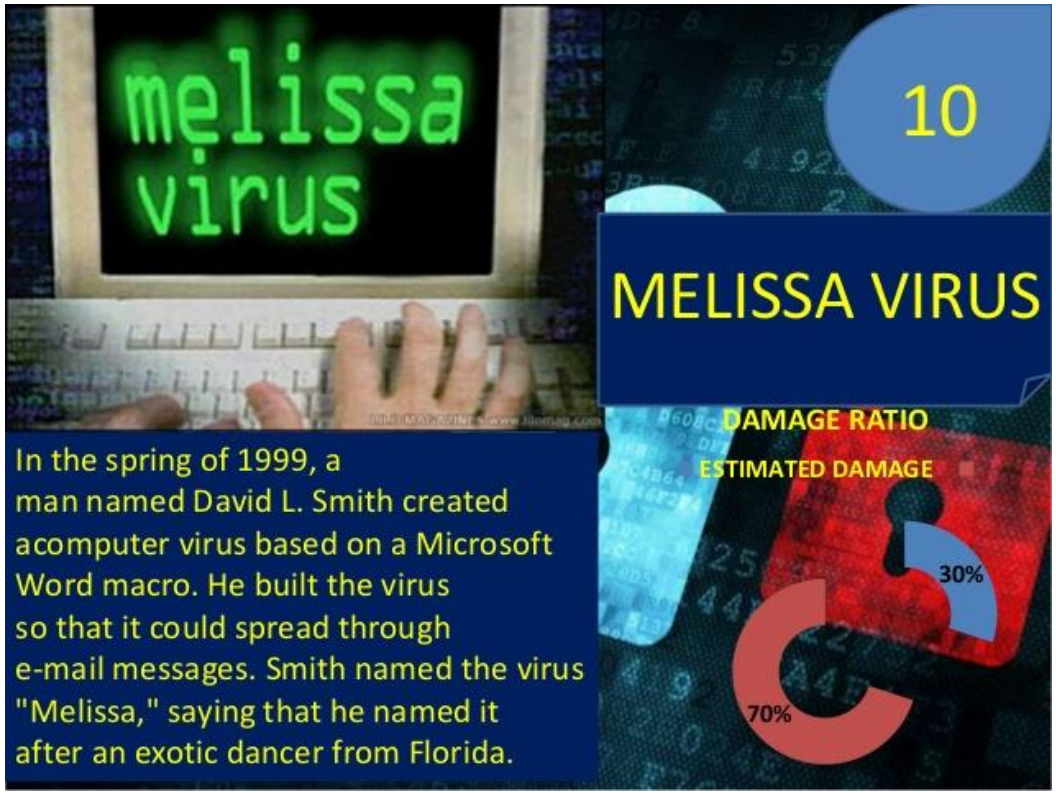
進階密碼管理方案

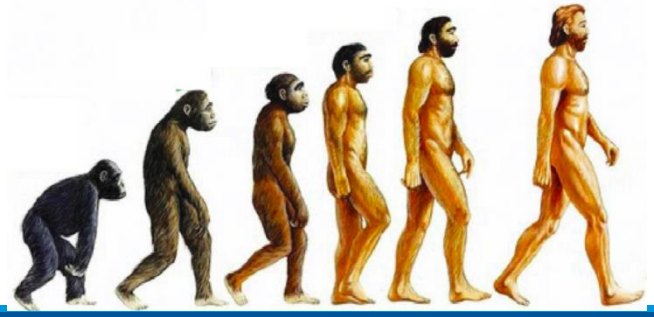
- 動態密碼
  - 每次密碼都不同(卡片 /鑰匙圈/簡訊/手機APP)
- 兩階段驗證(結合手機App / 簡訊)
- 目前應用
  - 網路銀行
  - Google

SOPHOS

都是病毒惹的禍

演進歷史





- 第一隻Melissa病毒於1999年誕生(17年歷史)

知名病毒及蠕蟲的歷史年表

1980年代 [編輯]

年份	日期	事件
1980年		Jürgen Kraus撰寫碩士論文：自我複製的程式（Selbstreproduktion bei programmen）。
1982年		一個執行於Apple II系統，稱為Elk Cloner病毒的電腦病毒出現，據信是第一個非實驗室製造的電腦病毒。
		Joe Dellinger在A+M大學撰寫了一個Apple II電腦病毒。
1986年	1月	大腦開機磁區病毒出現，可認為是第一個個人電腦病毒。此病毒也稱為拉合爾（Lahore）、巴基斯坦（Pakistani）或巴基斯坦大腦，因為它是在巴基斯坦的拉合爾誕生的。
1987年	10月	耶路撒冷病毒在耶路撒冷市被發現，它是一個計畫在十三號星期五啟動並毀滅所有可執行檔的病毒。
	11月	以Amiga為對象，稱為SCA病毒的開機磁區病毒出現，立刻造成病毒作者間的風暴。而不久之後瑞士鬼客聯合（SCA）馬上釋出另一個被認為更具破壞力的病毒：位元強盜。
1988年	6月	Festering Hate病毒與ProDOS病毒從私有BBS散布到主要網路上。
	11月2日	由羅伯特·泰潘·莫里斯創造的莫里斯蠕蟲（或稱I.Worm），可感染DEC VAX與SUN以BSD UNIX執行的網路機器，成為了第一隻荒野誕生（非實驗室製造）的蠕蟲，且是第一個利用緩衝區溢位漏洞的惡意程式。而乒乓病毒是本時代第一個知名的開機磁區感染病毒。
1989年	10月	第一隻跨領域病毒：鬼球病毒被Fridrik Skulason發現。

1990年代 [編輯]

年份	日期	事件
1992年	3月6日	米開朗基羅病毒製造了一次數位大災難。
1995年		第一個巨集病毒Word concept病毒誕生。
1998年	4月26日	第一版CIH病毒v1.0問世。
1999年	3月26日	Melissa蠕蟲出現，攻擊Microsoft Word的全球模板Normal.dot，所有新建立的檔案都被感染，瞄準了使用Microsoft Word與Outlook的系統，病毒感染Microsoft Outlook通訊錄上的前50個用戶，並造成大量網路流量以及擁塞，本日全球許多大企業的信件伺服器因而停止運作一天。
	4月26日	CIH病毒在全世界各地爆發。
	6月6日	可摧毀Microsoft Office檔案的ExploreZip蠕蟲首次被發現。

知名病毒及蠕蟲的歷史年表

2000年代及以後 [編輯]

年份	日期	事件
2000年	5月	ILOVEYOU病毒，或稱VBS/Loveletter現身。並造成如同2004年一般可怕的商業損失，大約有100億美元。
2001年	1月	一個類似Morris蠕蟲，稱做Ramen蠕蟲襲擊安裝Red Hat Linux 6.2或7版的機器，使用了三個在wu-ftpd、rpc-statd與lpd的漏洞。
	5月8日	悲傷心情蠕蟲藉由一個在SUN上Solaris（資訊安全告示區00191）與Microsoft上IIS（MS00-078）的漏洞而傳播。
	7月	Sircam蠕蟲釋出，藉由電子信件以及未保護的網路分享傳播。
	7月13日	紅色警戒蠕蟲釋出，此蠕蟲攻擊Microsoft IIS的Index Server ISAPI Extension的漏洞（描述在MS01-033），且造成非常嚴重的商業損失。
	8月4日	一個完全重新撰寫的紅色警戒蠕蟲，稱為紅色警戒蠕蟲II被惡意釋出，來源據說在中國。
	9月18日	Nimda蠕蟲被發現，並藉由許多方式傳播，傳播方式敘述於MS01-044，且利用了紅色警戒蠕蟲II與悲傷心情蠕蟲留下的後門。
	10月26日	Klez蠕蟲第一次被發現且辨別。
2003年	1月24日	SQL slammer蠕蟲，也稱為藍寶石蠕蟲，攻擊了Microsoft SQL Server與MSDE的漏洞，詳情公布於MSDE described in MS02-039與MS02-061，造成了網際網路上的廣泛的災情。
	8月12日	衝擊波蠕蟲，又稱為**Lovesan**蠕蟲，藉由Microsoft Windows在MS03-026第一次與稍後於MS03-039描述的漏洞進行攻擊。
	8月18日	Welchia蠕蟲（假好心蠕蟲，或Nachi蠕蟲）出現，此蠕蟲試圖移除衝擊波蠕蟲並修復Windows。
	8月19日	太上蠕蟲（Sobig蠕蟲）藉由電子信件與網路分享快速傳播。
	10月24日	清醒蠕蟲（Sober蠕蟲）第一次出現，並且以多種變種維持到2005年。
本年衝擊波與太上蠕蟲的同時攻擊造成非常大的傷害。		

知名病毒及蠕蟲的歷史年表

2004年	1月下旬	世界末日蠕蟲（MyDoom蠕蟲）現身，並創下最快散播速度的信件病毒記錄。
	3月19日	Witty蠕蟲是一隻打破多項紀錄的蠕蟲。它感染ISS產品的多項漏洞。它是最快散布的蠕蟲，也是第一個攜帶毀滅性程式碼的蠕蟲。
	5月1日	震盪波蠕蟲藉由一個敘述於MS04-011的LSASS漏洞現身，造成網際網路癱瘓，甚至影響商業活動。
	12月	Santy蠕蟲，據信是第一隻**網頁蠕蟲**。它藉由一個敘述於BID10701的PhpBB漏洞以及使用Google以發現新目標。它在Google過濾並防止此蠕蟲散布之前已感染了40000個網站。
2005年	8月16日	利用敘述於MS05-039漏洞的Zotob蠕蟲與數個變種的惡意軟體被發現。它的影響非常轟動，因為數個美國媒體出口網站被感染了。
	10月13日	Samy病毒成為2006年最快散布的電腦病毒。
2006年	1月20日	Nyxem蠕蟲出現，它散布大量電子信件，且在2月3日後，試圖在每月的三號發作，使資訊安全相關軟體與檔案分享機制失效，並摧毀某類型的檔案，例如Microsoft Office檔案。
	6月28日	研究者指出Farid Essebar可能創作了數量高於20的病毒，包括MyDoom病毒的變種：MyDoom-BG病毒、Zotob蠕蟲演變的Mytob蠕蟲[1]。
2010年	6月	震網蠕蟲被發現，此蠕蟲專門針對伊朗核設施的電腦硬體。

https://zh.wikipedia.org/

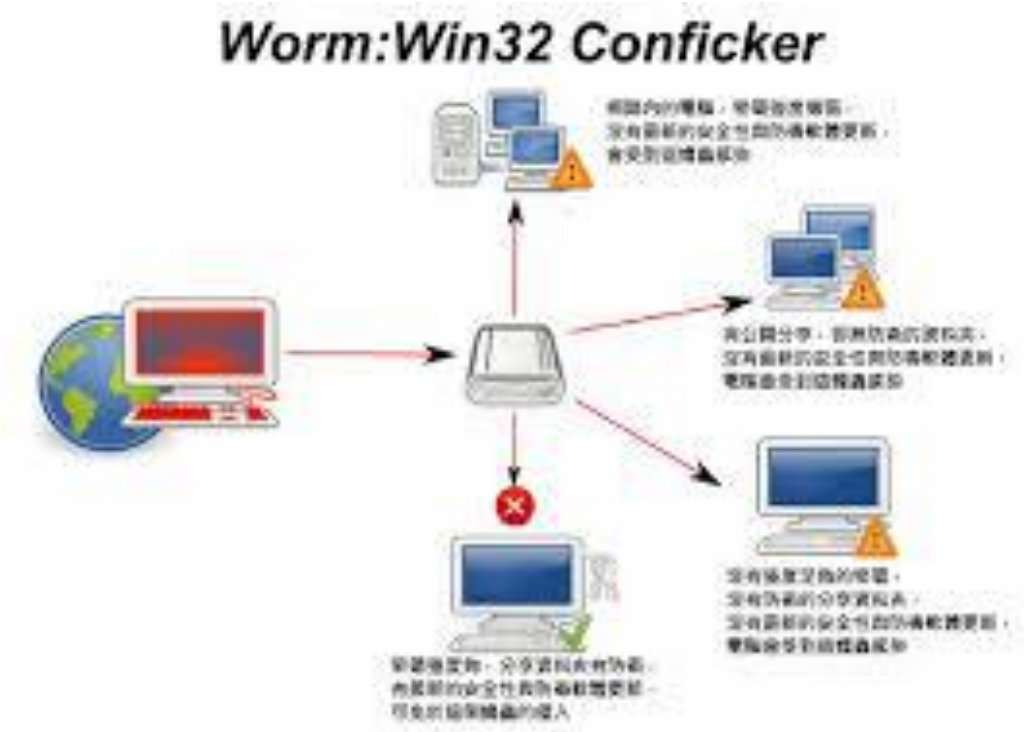
- 1998年 **CIH** 感染全球 6000 萬台電腦, 造成 **10 億美元**商業損失
- 1999年 **Melissa**(word 巨集病毒)利用Email快速擴散感染全球 10 萬台電腦, 迅速灌爆全球Email伺服器, **迫使企業主動關閉 Email 服務**
- 2000年 **I Love You**(vbs病毒)同樣利用Email迅速蔓延全球造成全球 **55 億美**元商業損失
- Code Red , Nimda , Code Red II ...
- 2003年 **Blaster** 造成多數企業內部網路完全癱瘓
- SASSER
- .....

惡意程式 Malware

- Virus - 病毒
- Worms - 蠕蟲程式
- Trojan Horses - 特洛伊木馬程式
- Spyware - 間諜程式
- Keylogger – 鍵盤側錄程式
- Adware - 廣告程式
- Scareware -流氓程式
- Ransomware -勒索程式

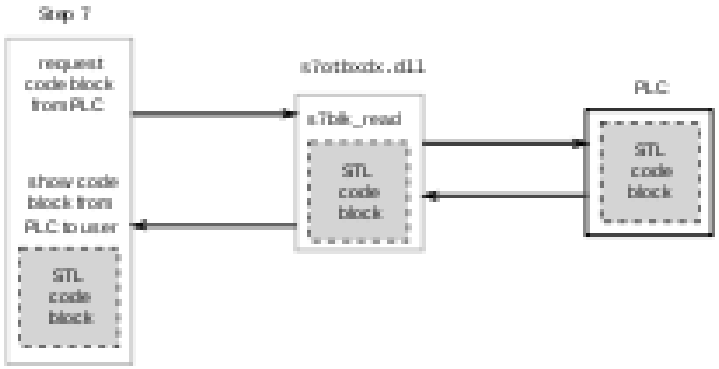
Conficker病毒

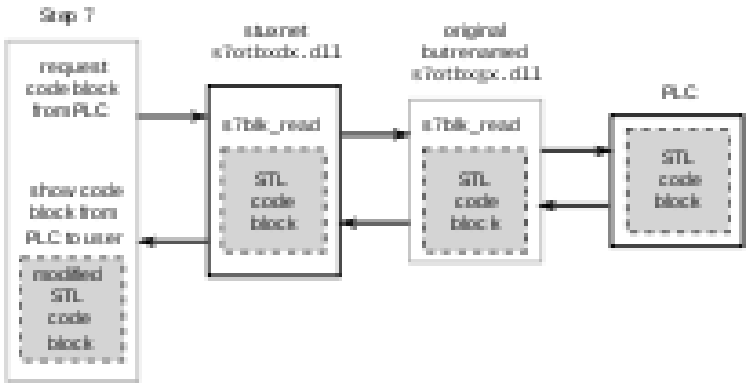
- 2008年被發現
- 感染Windows平台
- 回報惡意中繼站
- 可透過網路及USB擴散
- 可下載變種更新自己、內部通訊方式及中繼站位址
- 殭屍網路成員
- 目的：竊取個資,發送垃圾郵件,跳板攻擊...



Stuxnet病毒

- 2010年首度發現
- 攻擊並感染Windows平台
- 透過USB擴散跳轉
- 最終目標：感染西門子核子設施PLC
- 目的：使核子離心機運轉失控





Zeus病毒

- 2006年首度現身
- 超過30家銀行, 3萬個企業/個人之銀行帳戶遭竊, 損失高達4700萬美元以上
- 感染用戶電腦及行動裝置, 藉以破解雙因子驗證(攔截簡訊)
- 感染橫跨 Android , iOS , BlackBerry , Symbian

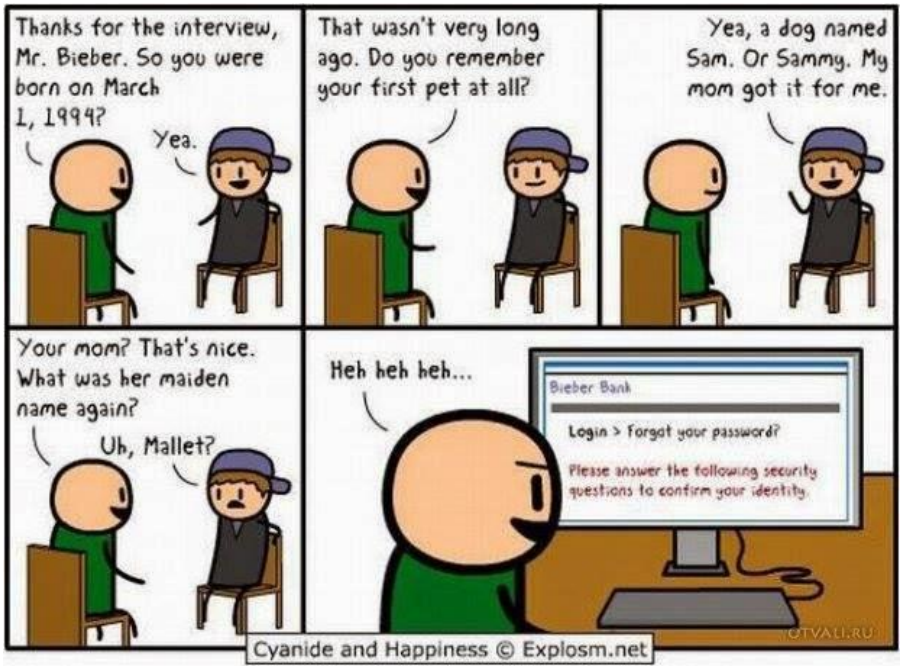
SOPHOS

不可不知的社交工程


Social Engineering
An attack vector most intricate to handle!

社交工程 Social Engineering

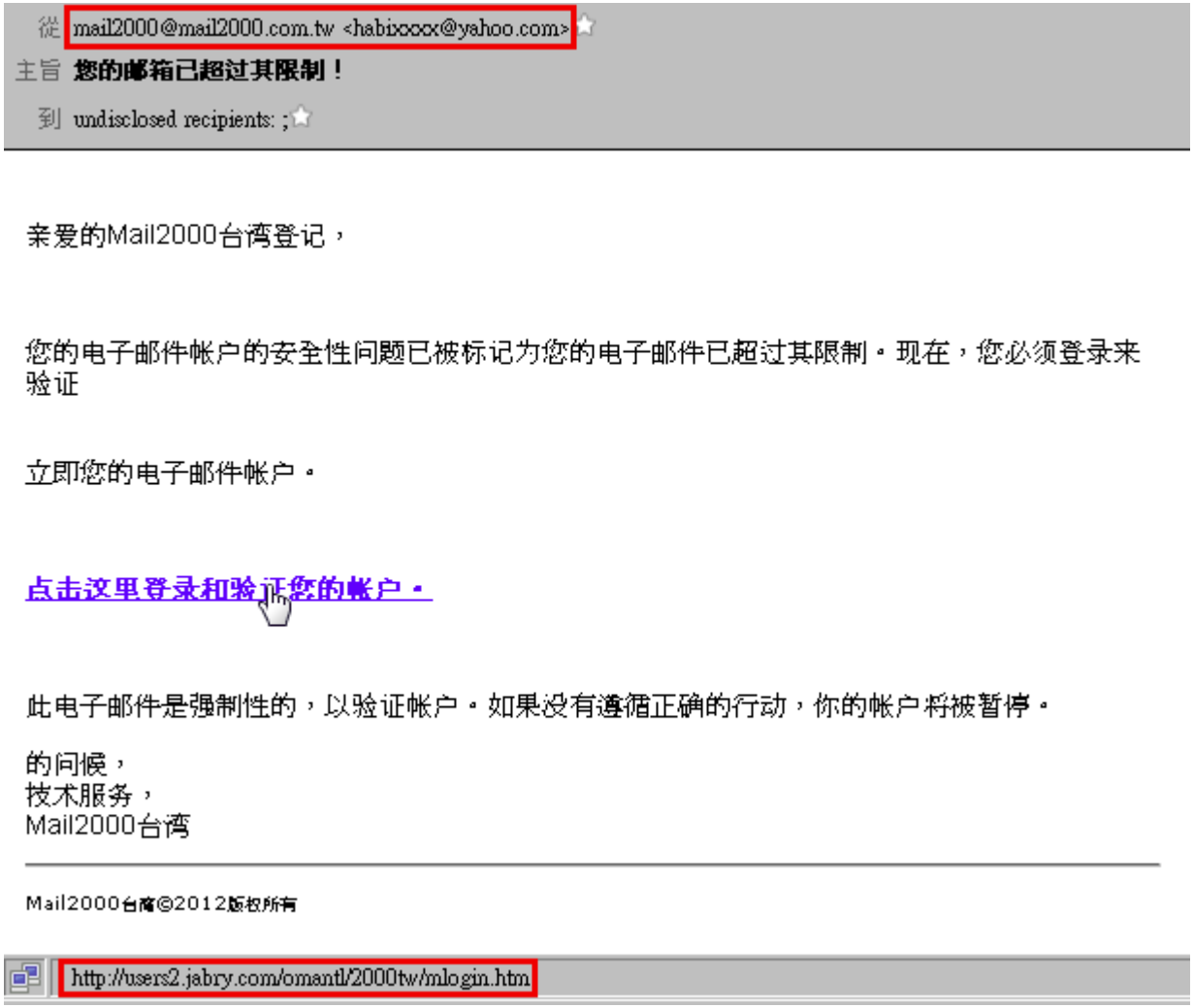
是指攻擊者利用欺騙的受害者到執行操作的方法。通常情況下是利用大眾的疏於防範的小詭計，讓受害者掉入陷阱。該技巧通常以交談、欺騙、假冒或口語用字等方式，從合法用戶中套取用戶系統的秘密，例如：用戶名單、用戶密碼及網路結構。



常見的社交工程攻擊

- 電話佯裝資訊人員
- 偽裝委外廠商
- 電子郵件誘騙使用者登入偽裝之網站
- 電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料
- 利用提供工具、檔案、圖片 為幌子，誘騙使用者下載
- 即時通訊軟體如Facebook, LINE等偽裝

假冒信件



從 mail2000@mail2000.com.tw <habixxxx@yahoo.com>
主旨 **您的邮箱已超过其限制！**
到 undisclosed recipients: ;

亲爱的Mail2000台湾登记，

您的电子邮件帐户的安全性问题已被标记为您的电子邮件已超过其限制。现在，您必须登录来验证

立即您的电子邮件帐户。

点击这里登录和验证您的帐户。

此电子邮件是强制性的，以验证帐户。如果没有遵循正确的行动，你的帐户将被暂停。

的问候，
技术服务，
Mail2000台湾

Mail2000台湾©2012版权所有

http://users2.jabry.com/omantl/2000tw/mlogin.htm

Openfind™
MAIL2000 電子信箱

服務介紹 | 線上訂購 | 常見問題 | 全站搜尋

Openfind.

協科資訊
品質、技術、服務、創新

帳號： @ mail2000.com.tw
密碼： 忘記密碼 登入
SSL ???? SSL ????
邀請您升級 Mail2000 v6

服務公告

精簡

歡迎使用 Mail2000 精簡版首頁
若您覺得新版首頁太複雜或是使用不習慣Mail2000，在此我們提供您精簡版首頁，可加入常用功能使用。[精簡版首頁]
????!????????!?????????????,????...
讚 1,058

????????
Mail2000 ????????????? Mail2000 ??????,???????????...[????]

????????
Mail2000
?????????,???????????????,?????...[????]

功能特色

Mail2000 個人信箱比免費信箱好用在哪裡？價值何在？還有為什麼很多會員，因為親友的推薦，就毫不遲疑的購買使用？Mail2000 個人信箱除了讓您擺脫每天刪廣告信的痛苦，還有許多貼心功能滿足您各式的需求，更有專業的客服提供您使用上的協助...[更多介紹]

立即購買 免費試用

Blog 新訊息

P-Marker Cloud全新登場
自動化清查企業所有個資檔案
Mail2000 v6 新版行事曆
設定手機與行事曆同步

公益專區

網擎資訊推出公益方案，將免費贊助公益團體使用「郵件代管」與「網站代管」，歡迎各界公益團體申請！[瞭解更多]

TOP

Sitemap

產品資訊
Mail2000 信箱
Mail2000 行動簡訊
Mail2000 DVD 備份
Mail2000 禮券

Mail2000 延伸產品
MailCloud 企業郵件代管
Mail2000 企業版
MailGates 郵件防護系統
MailBase 郵件歸檔管理系統

會員服務
Facebook 粉絲團
Mail2000 blog
推薦回饋
白金會員
下載專區
公益計劃

客服中心常見問題
在 iPhone 設定 Mail2000
如何使用拋棄式帳號
訂閱 RSS 使用說明
如何設定外部圖檔封鎖
如何使用虛擬信匣

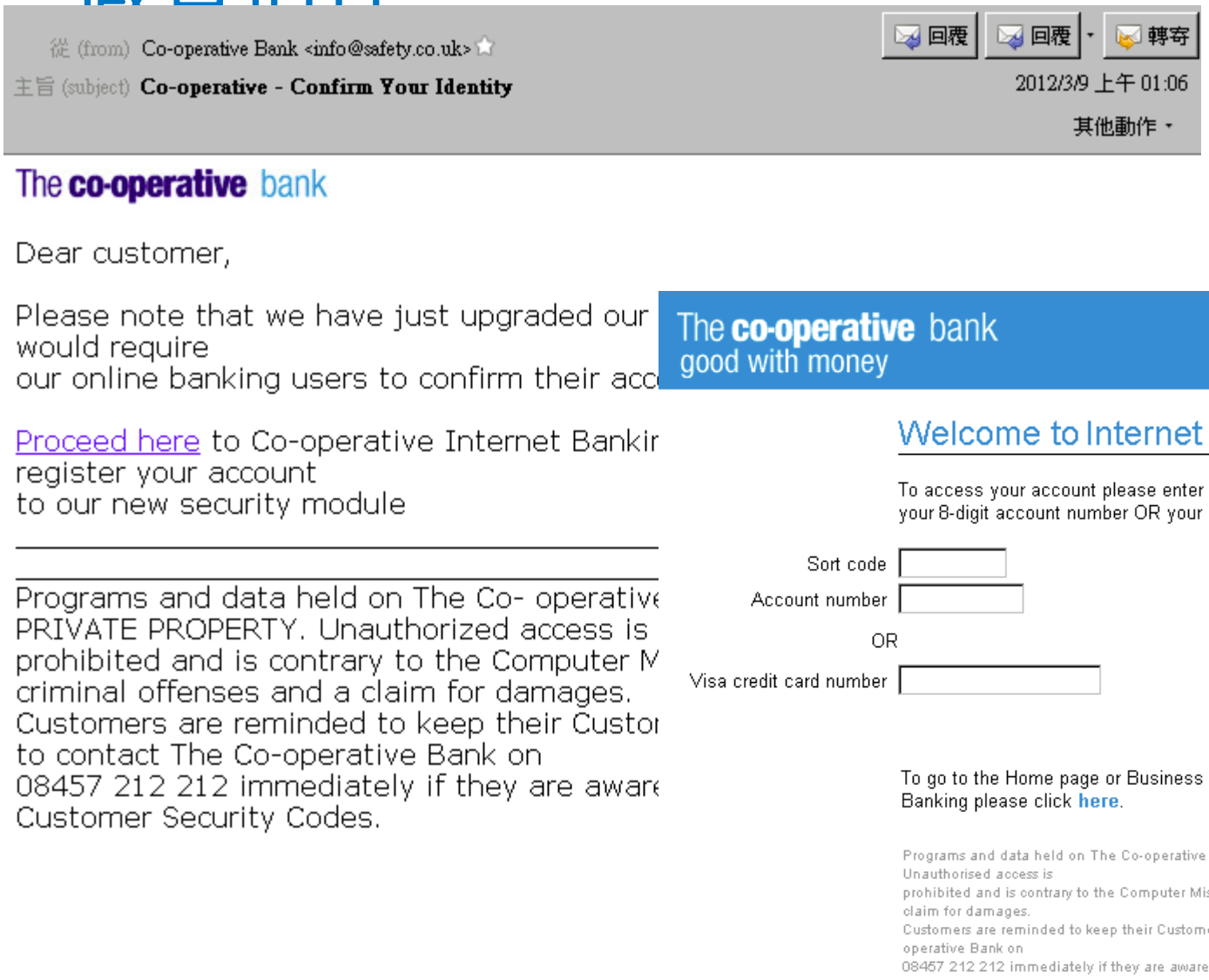
使用條款
信箱使用條款
簡訊使用條款
隱私權政策
交流園地使用規範

立即購買
立即購買

與我們聯絡
客服專線：(02) 2553-7272
客服傳真：(02) 2553-5956
客服信箱：
m2k_adm@mail2000.com.tw
服務時間：
週一至週五 09：00 - 18：00

Openfind.
© 1998 -2012
線上隱私保護政策聲明

假冒信件



從 (from) Co-operative Bank <info@safety.co.uk>
主旨 (subject) **Co-operative - Confirm Your Identity**

回覆 回覆 轉寄
2012/3/9 上午 01:06
其他動作

The co-operative bank

Dear customer,

Please note that we have just upgraded our
would require
our online banking users to confirm their acc

Proceed here to Co-operative Internet Bankir
register your account
to our new security module

Programs and data held on The Co- operative
PRIVATE PROPERTY. Unauthorized access is
prohibited and is contrary to the Computer M
criminal offenses and a claim for damages.
Customers are reminded to keep their Custor
to contact The Co-operative Bank on
08457 212 212 immediately if they are aware
Customer Security Codes.

The co-operative bank
good with money

Welcome to Internet Banking

To access your account please enter your 6-digit sortcode and
your 8-digit account number OR your 16-digit Visa card number.

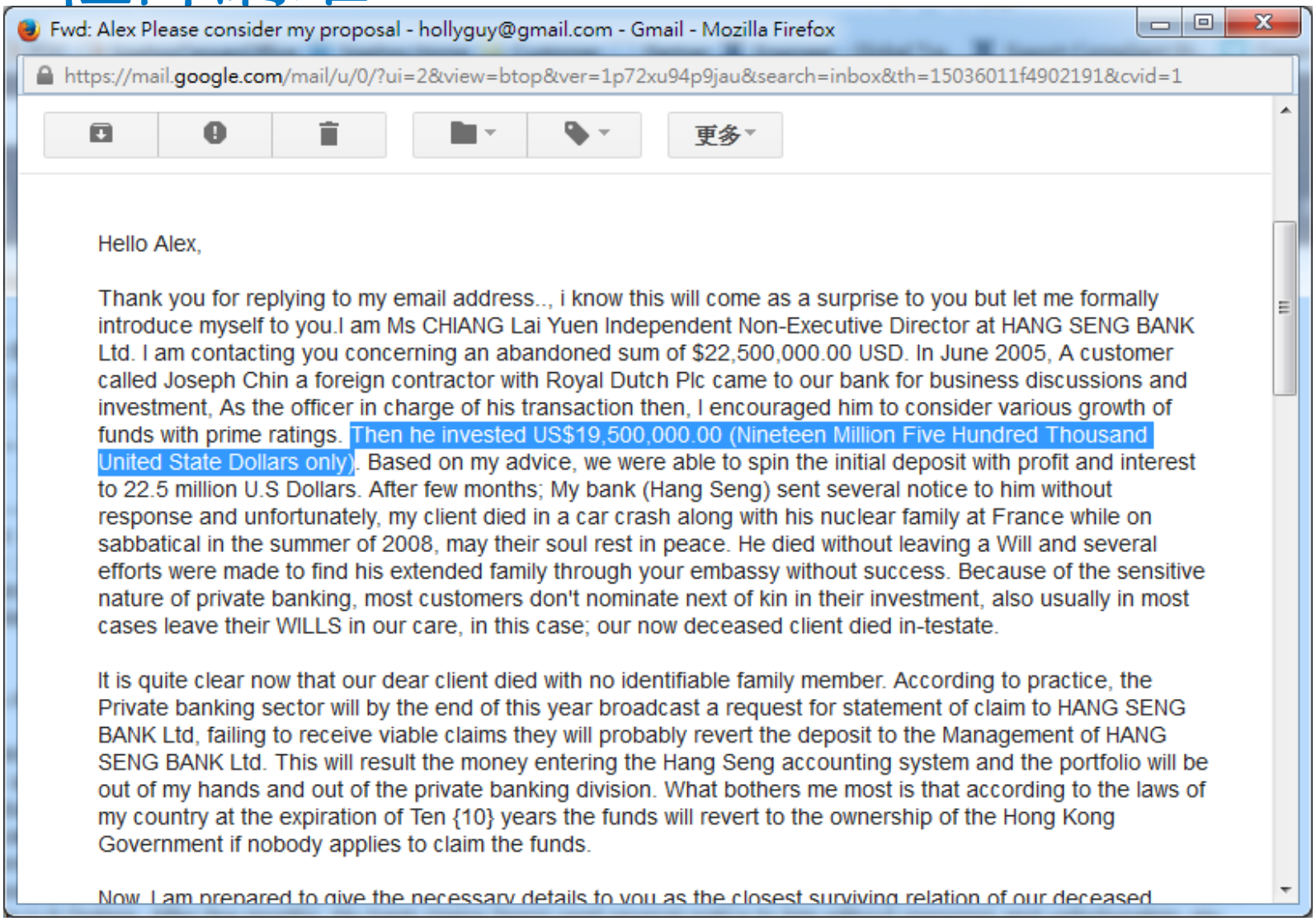
Sort code
Account number
OR
Visa credit card number

OK Clear

To go to the Home page or Business Internet
Banking please click here.

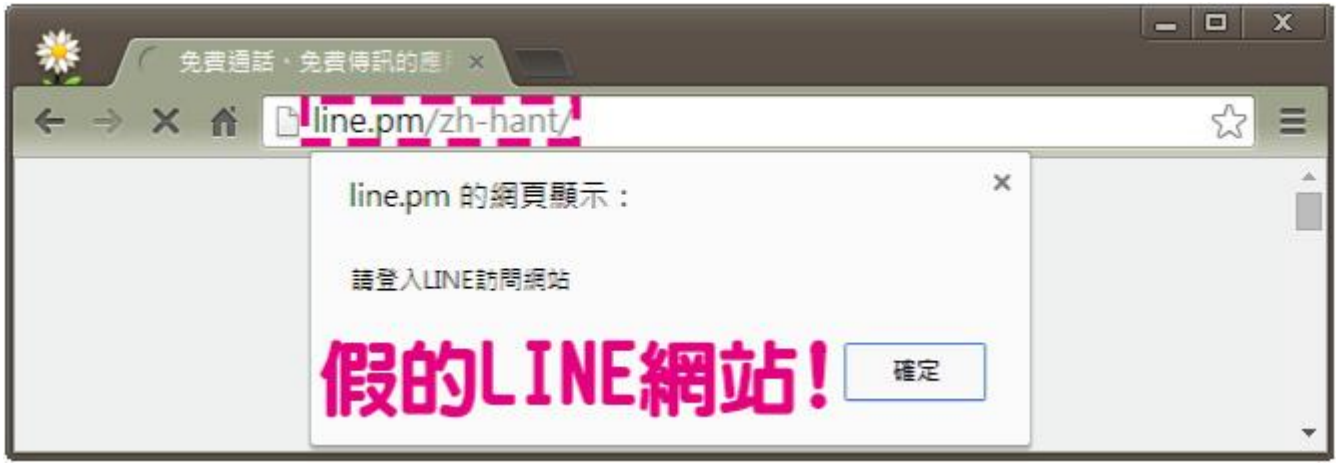
Programs and data held on The Co-operative Bank p.l.c. and smile systems are PRIVATE PROPERTY. Unauthorised access is
prohibited and is contrary to the Computer Misuse Act 1990, which may result in criminal offences and a claim for damages.
Customers are reminded to keep their Customer Security Codes confidential and to contact The Co-operative Bank on
08457 212 212 immediately if they are aware someone else knows their Customer Security Codes.

社群網站 - LinkedIn



假的網站 Fake URL

假的網站 Fake URL



國內案例一

案例一：北部某一從事汽車零件出口之國際貿易公司，貨款均由美國客戶以TT（telegraphic transfer）電匯方式匯至該公司在臺開設之銀行帳戶，雙方並透過E-mail進行聯繫。102年2月底，該公司收到美國客戶以E-mail通知即將匯款美金50萬，數日後竟發現客戶將貨款改匯至一英國銀行帳戶。經向美國客戶查證，美國客戶稱是依照臺灣公司的E-mail指示，臺灣公司始發現雙方往來之E-mail遭駭客入侵。駭客入侵該臺灣公司與美國客戶間之E-mail後，以類似該臺灣公司的E-mail帳號與美國客戶聯絡，致美國客戶陷入錯誤，將貨款改匯至嫌犯指定之英國銀行帳戶，因而遭受巨額金錢損失。

案例二：北部某一工業顧問公司之電子郵件信箱於102年2月遭駭客入侵，直接以該公司之E-mail與美國客戶聯繫，致美國客戶陷入錯誤，將貨款19萬美金匯至嫌犯指定之馬來西亞銀行帳戶，公司因而遭受巨額金錢損失。

國內案例二

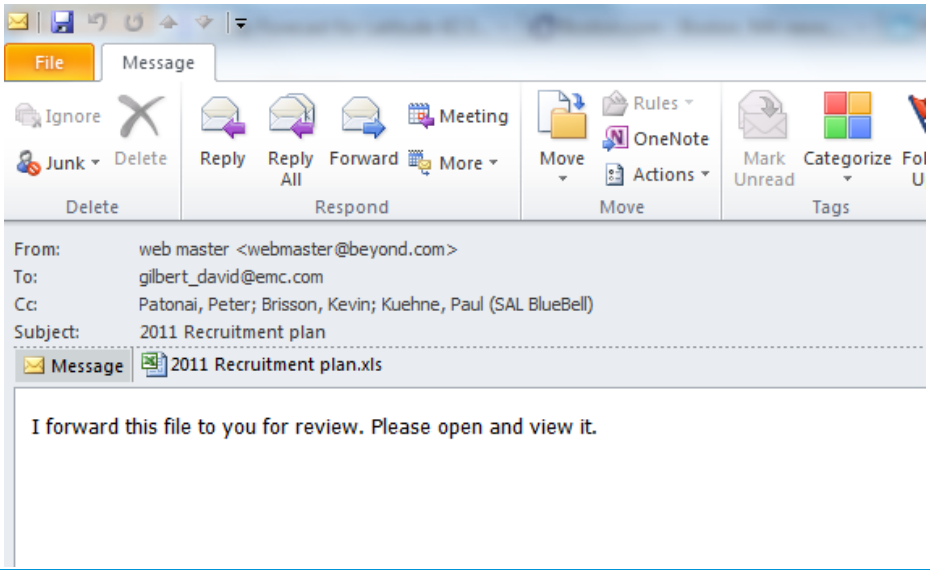
案例二：北部某一工業顧問公司之電子郵件信箱於102年2月遭駭客入侵，直接以該公司之E-mail與美國客戶聯繫，致美國客戶陷入錯誤，將貨款19萬美金匯至嫌犯指定之馬來西亞銀行帳戶，公司因而遭受巨額金錢損失。

國內案例三

案例三：網路駭客攔截某一機械公司所發給客戶的E-mail，郵件尚未到達客戶端前，駭客便直接攔截並竄改郵件內容及匯款帳戶資料。再假借該公司名義，寄件給客戶；幸好客戶端警覺不對，主動聯繫是否有更改銀行帳戶事宜，才免於受騙。

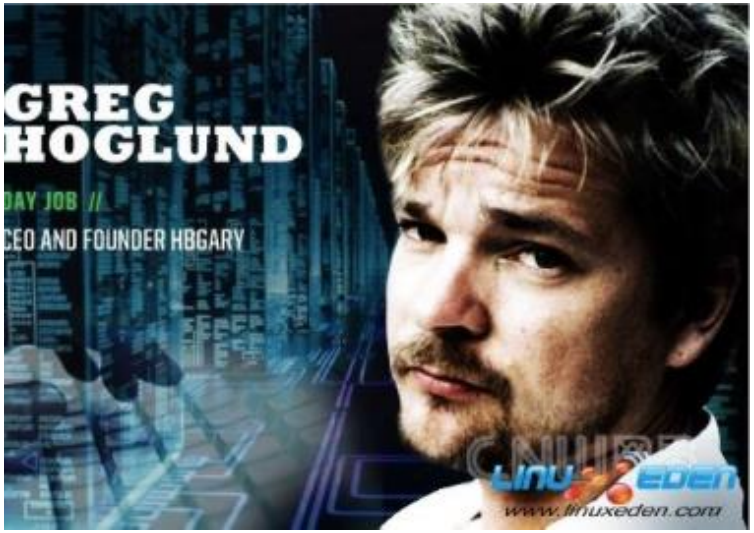
RSA事件

- 2011年3月EMC集團旗下子公司RSA的IT高層主管收到兩封主旨名為「 **2011 Recruitment Plan** 」的電子郵件
- 這兩封信件是駭客精準收集到該IT高層主管的個人背景資訊送出此封電子郵件當**誘餌**
- 結果該收件人打開信件電腦遭到埋入後門由駭客遠端遙控此台電腦**成功竊取到SecureID演算法**



HBGary事件

- CEO email被假冒
- 系統管理員失去警戒心
- 整個公司Email被竊取



From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 1:59 PM
To: jussi <jussij@gmail.com>

im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?
thanks

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:06 PM
To: Greg Hoglund <greg@hbgary.com>

hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 2:08 PM
To: jussi jaakonaho <jussij@gmail.com>

no i dont have the public ip with me at the moment because im ready for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give me public ip and ill ssh in and reset my pw.

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:10 PM
To: Greg Hoglund <greg@hbgary.com>
ok,
takes couple mins, i will mail you when ready. ssh runs on 47152

...a little later:

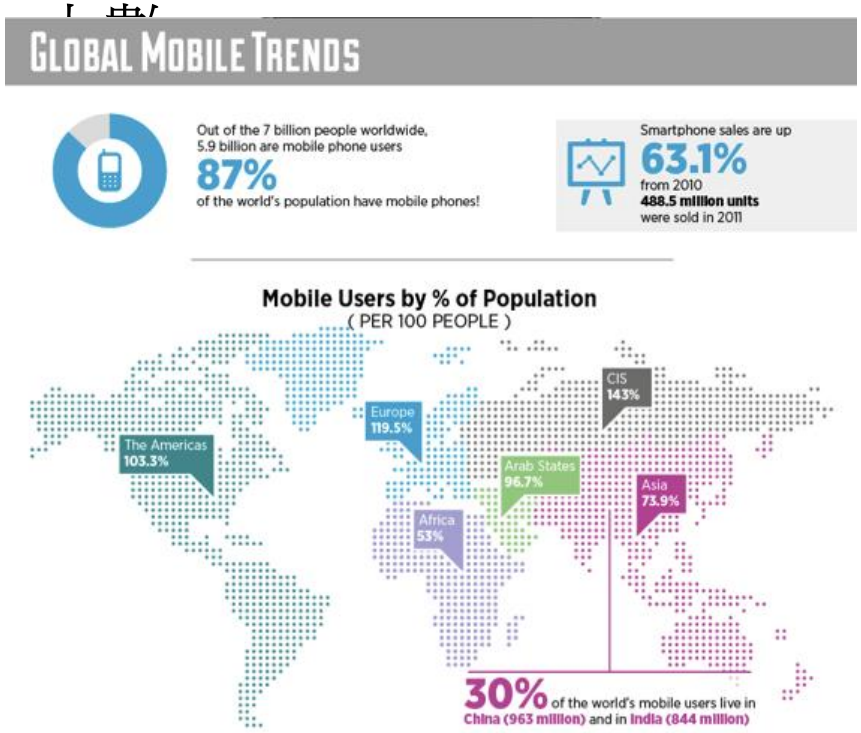
bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]

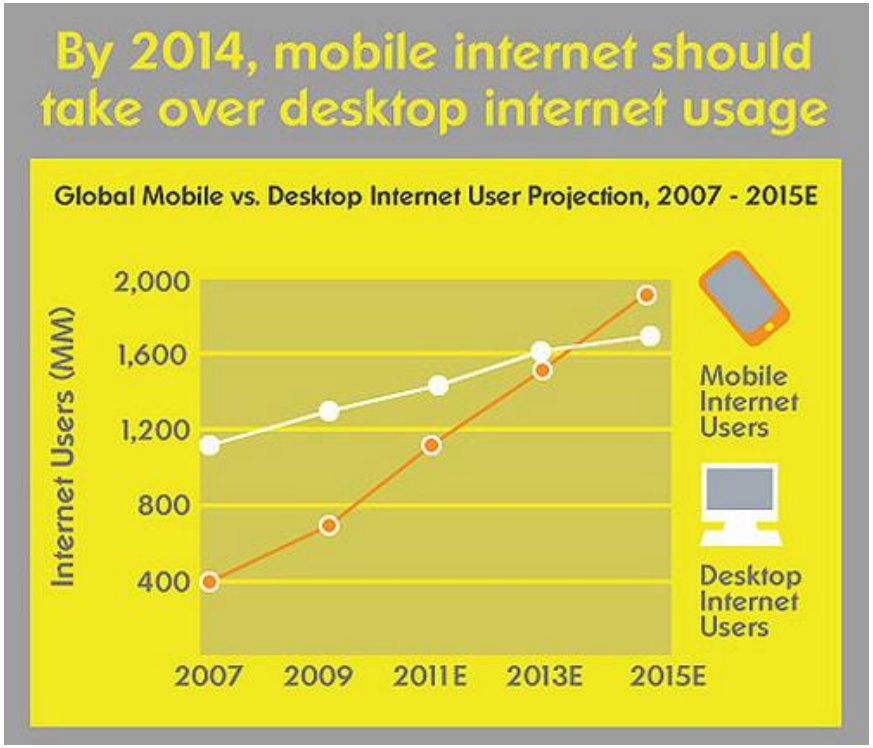
SOPHOS

行動裝置攻擊與日俱增

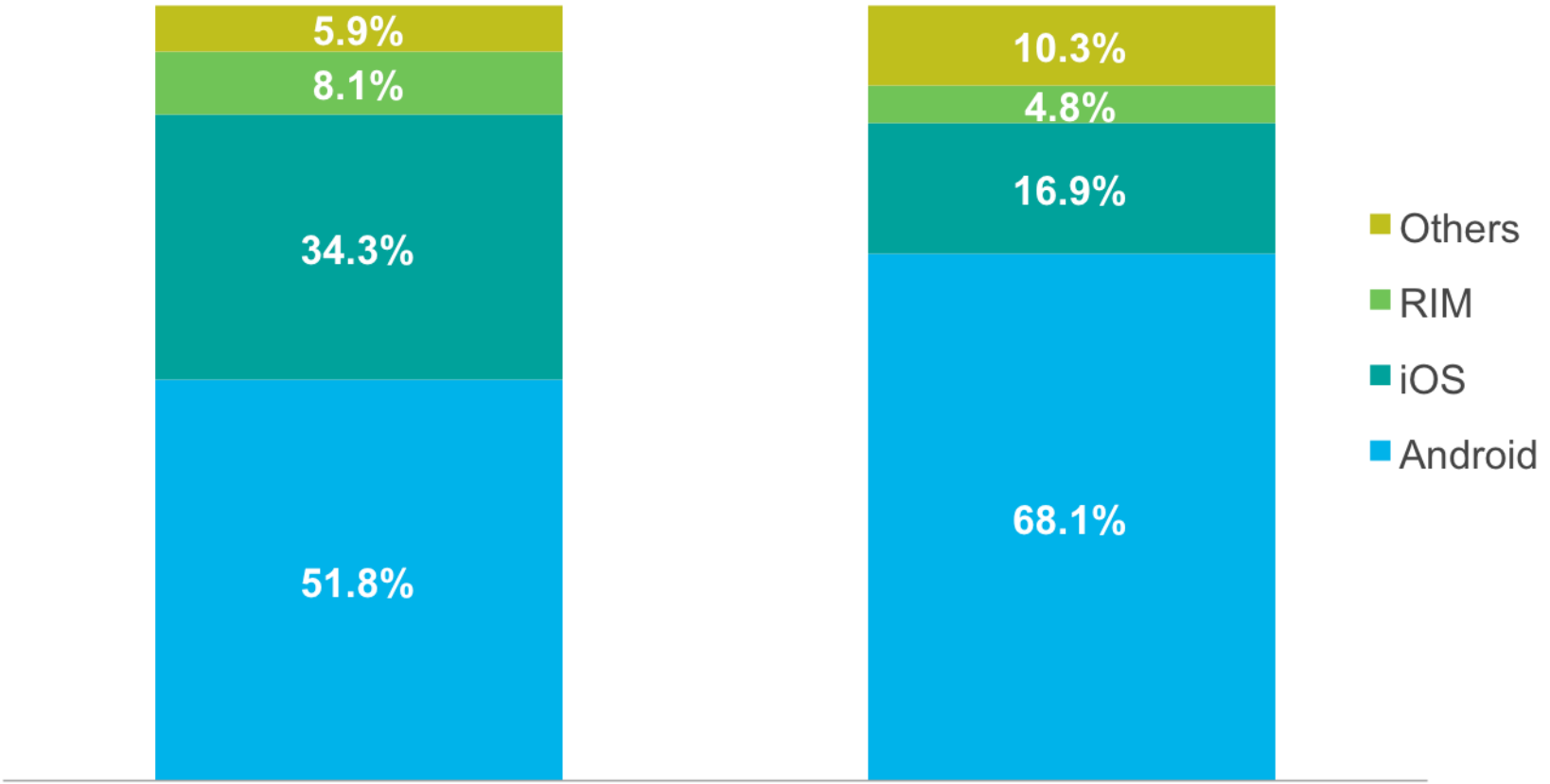
為何是Mobile

- 地球上有87%的人擁有手機
- 2014以後, 使用手機上網的人數會超過使用電腦上網的





為何總是Android



All Smartphone Owners in the US (Source: Nielsen July 2012)

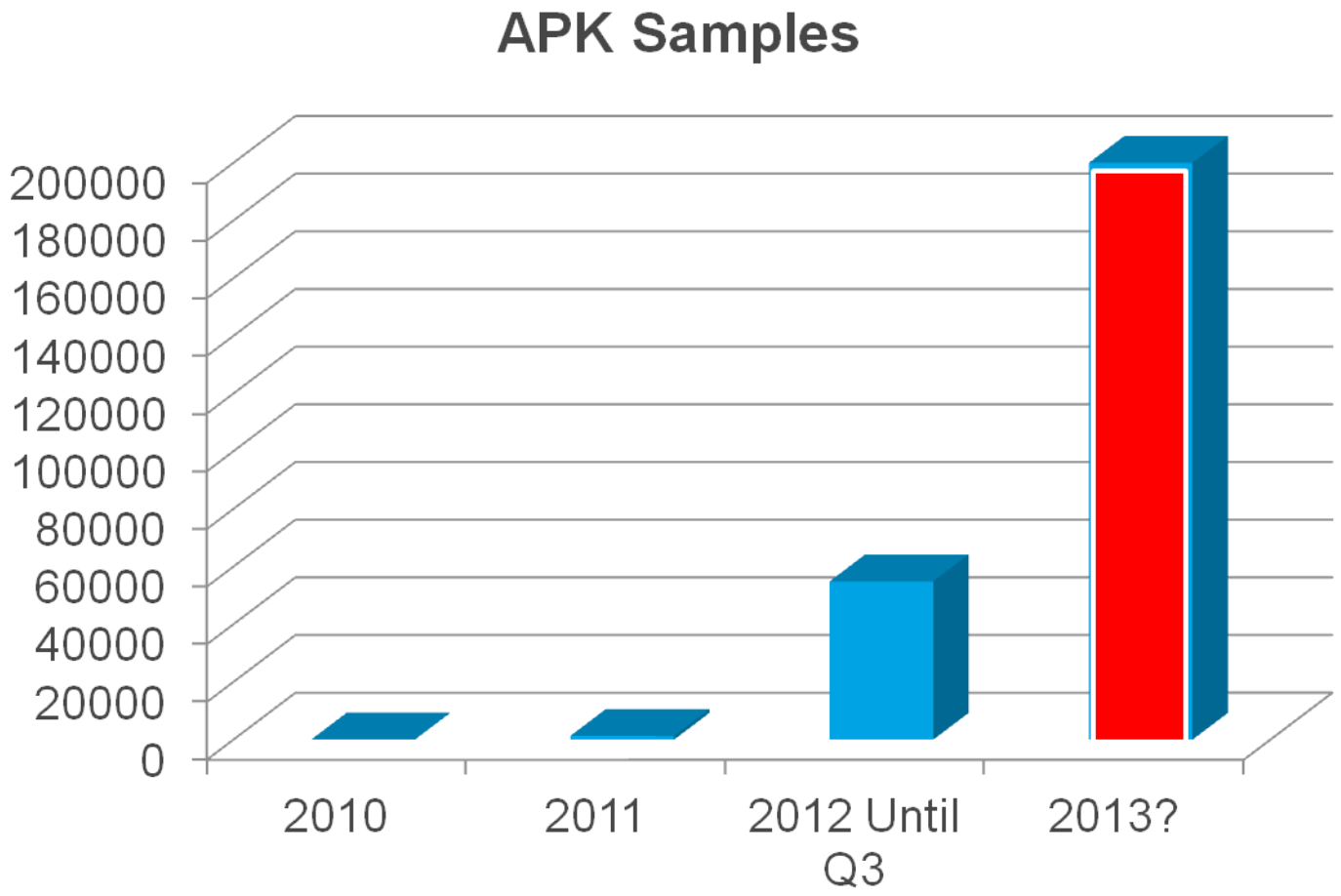
Global Smartphone Shipment in Q2 2012 (Source: Canalys 2012)

Android

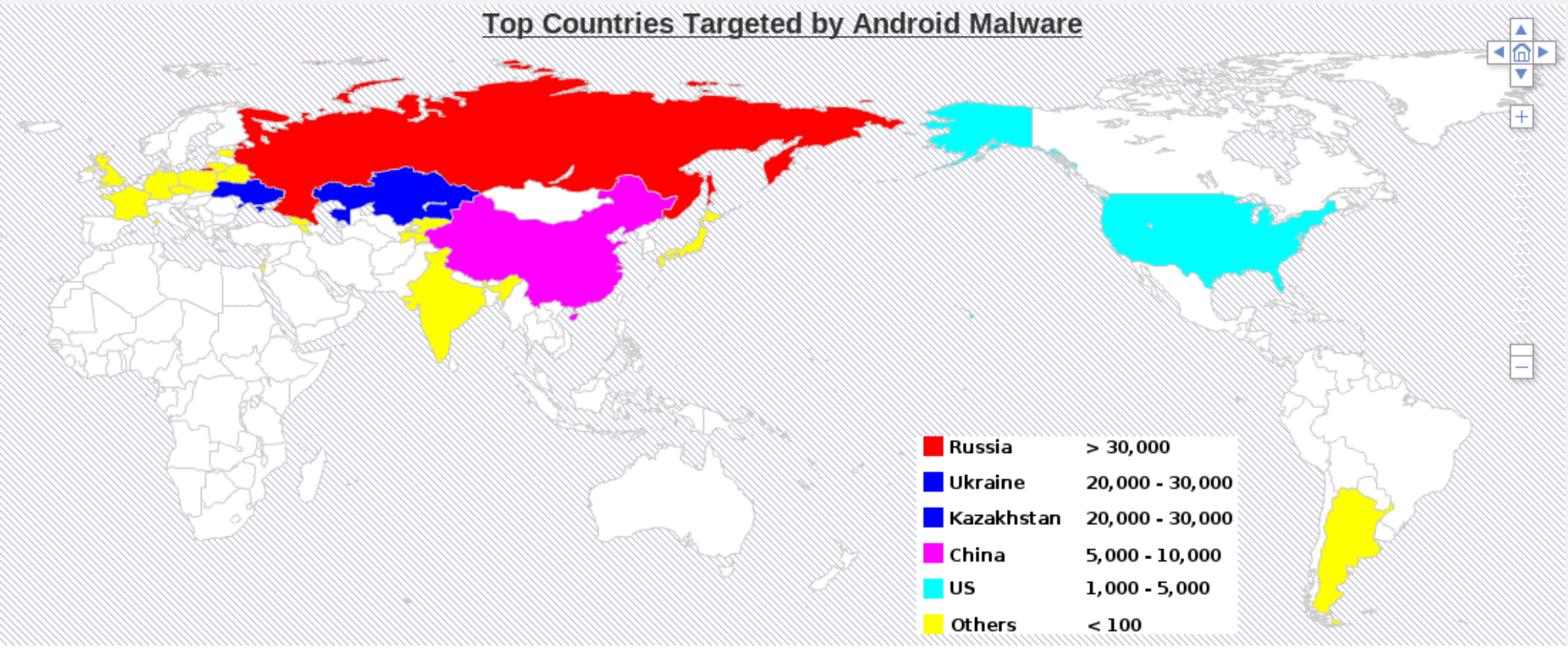
iOS並非不破金身

Find and Call 的應用程式在 App Store 和 Google Play 出現，這個程式會將用戶裝置內的聯絡人資料上載至一個私人伺服器，然後利用用戶的帳戶，向聯絡人發送垃圾 SMS 和電郵。

Android 惡意程式的發展



惡意程式的來源統計


Top Countries Targeted by Android Malware
Russia > 30,000
Ukraine 20,000 - 30,000
Kazakhstan 20,000 - 30,000
China 5,000 - 10,000
US 1,000 - 5,000
Others < 100

惡意APP的目的及分佈比例

- 未經允許秘密自動訂閱付費服務(Premium Service)–48%
- 在手機畫面上持續出現廣告(Adware)–22%
- 竊取個人資料(Data Stealer)–21%
- 未經允許下載惡意程式(Malicious Downloader)–19%
- 入侵手機取得控制權(Rooter)–11%
- 啟動在行動裝置上的點擊付費活動(Click Fraud)–7%
- 記錄使用者行為，傳送給第3方團體(Spying Tools)– 4%

付費簡訊

當心破財 手機不明簡訊 連結別打開

〔記者姚岳宏／台北報導〕手機簡訊暗藏破財陷阱！吳姓男子接到「好友」傳來簡訊，說要分享照片，於是依簡訊指示，下載圖片程式，卻跳出一堆陌生人照片，正感納悶，竟接到小額付費簡訊通知，點一下簡訊竟損失六千元，這才驚覺上了App惡意程式的當。

App惡意程式詐騙網頁

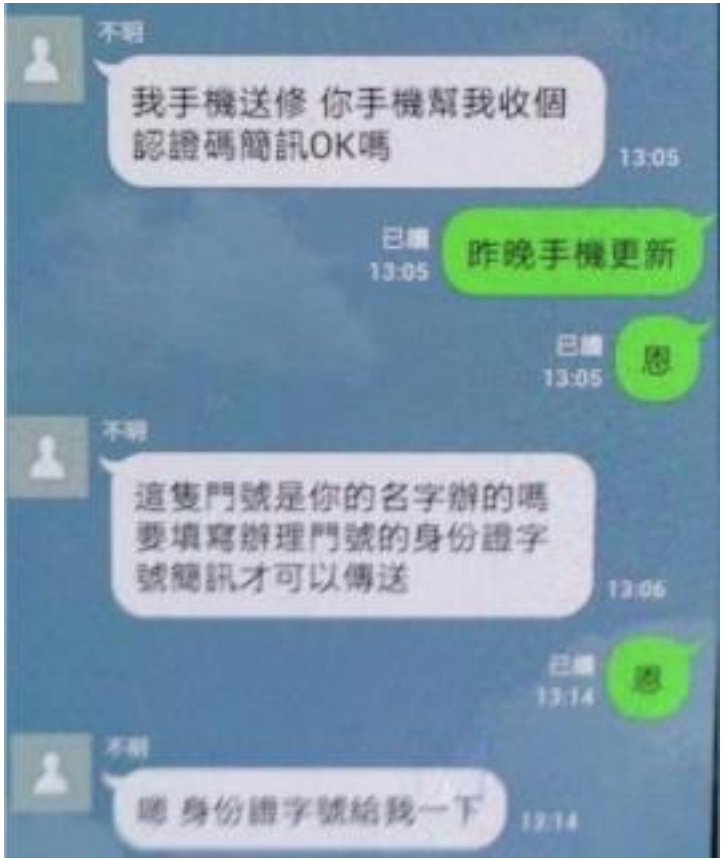
連結App惡意程式

警方表示，桃園縣四十歲吳姓男子，八月接到一封手機簡訊：「是吳某某麼？老同學來看我現在的照片，能想起來我是誰嗎^^」，吳以為是許久不見的朋友傳來，因照片無法顯示，於是點選下載圖片程式，並依網頁指示，下載檔名為.apk的手機應用軟體。

誤載被騙小額付費

MSN/LINE詐騙

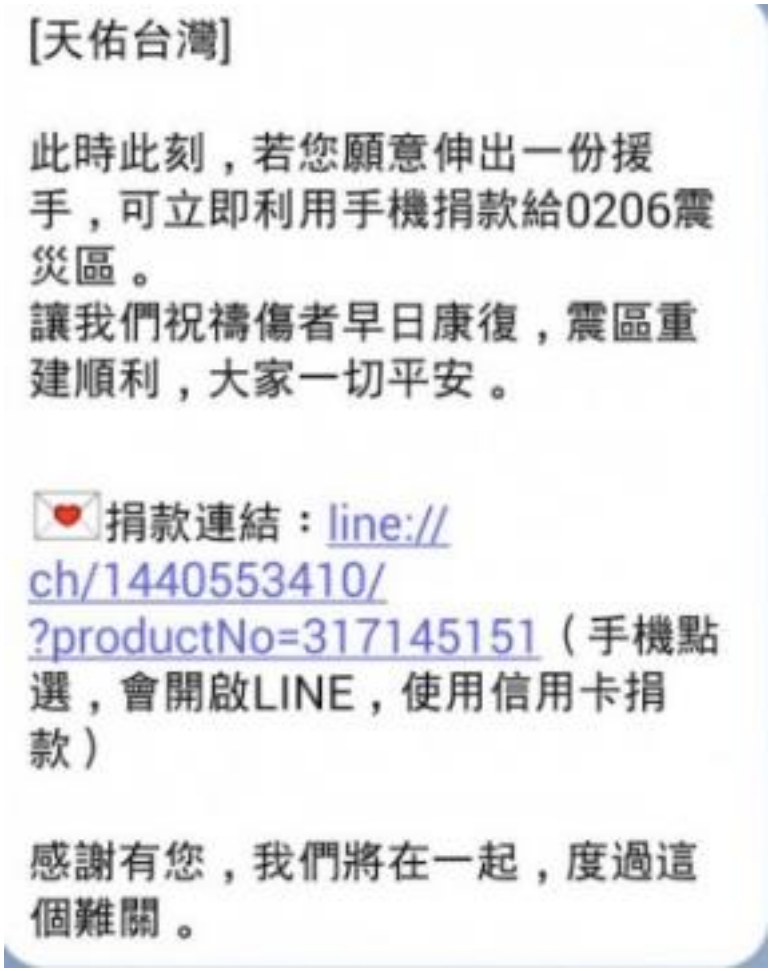
- 利用信任關係
- 手機門號小額付款
- 假貼圖真釣魚



簡訊詐騙

- 短網址
- 簡訊驗證碼

結合時事


[天佑台灣]

此時此刻，若您願意伸出一份援手，可立即利用手機捐款給0206震災區。
讓我們祝禱傷者早日康復，震區重建順利，大家一切平安。

捐款連結：line://ch/1440553410/?productNo=317145151（手機點選，會開啟LINE，使用信用卡捐款）

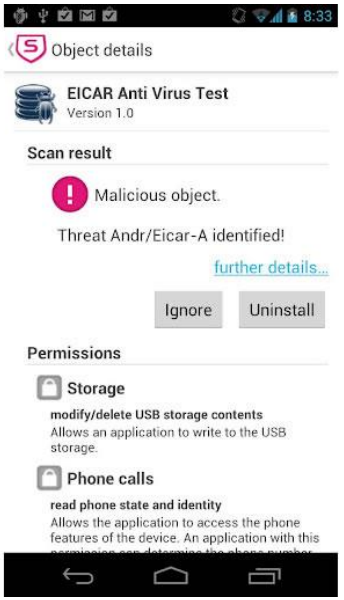
感謝有您，我們將在一起，度過這個難關。

盡量在APP Store安裝軟體

官方本身的 APP 下載平台，具有審核機制以確保安全性

盡量少安裝破解的APP

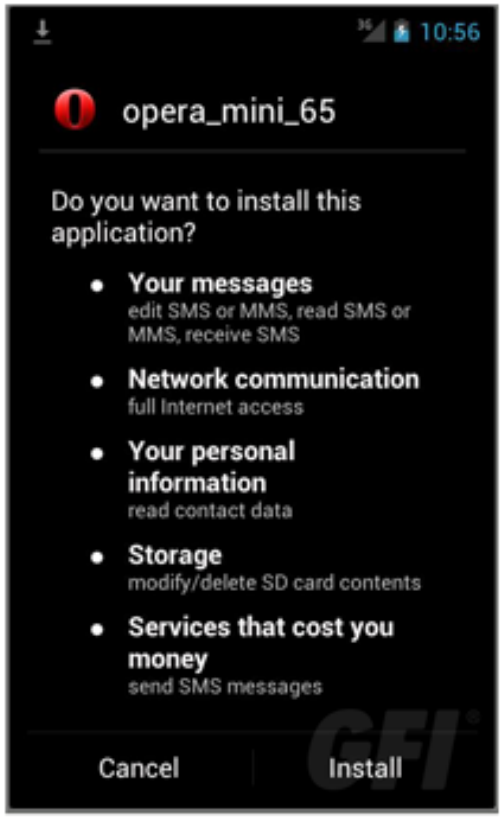
如果還是需要安裝非官方來源的APP, 建議安裝第三方的防毒軟體來確保APP的安全性



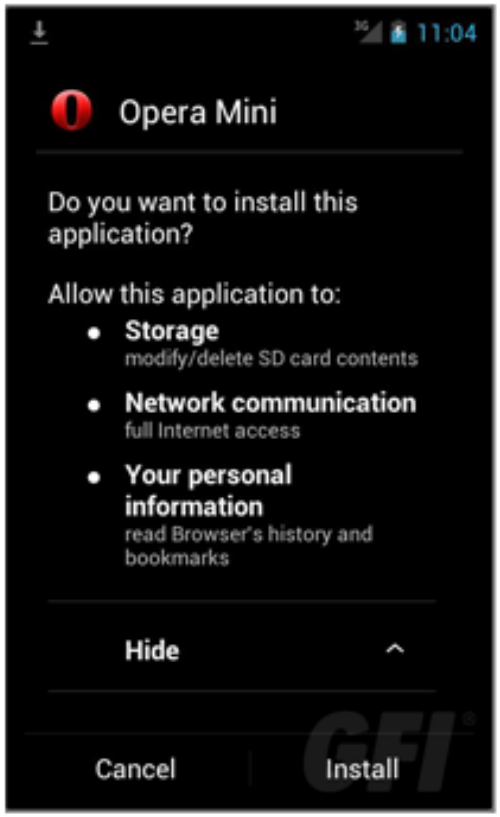
安裝 APP 之前查看要求授權內容

在安裝的過程中，至少都一定會跳出這樣的畫面，告訴你會需要哪些權限，取得你的個人資訊或是相關控制等等。

魔鬼總是藏在細節裡



Malware Permissions Screen (First Screen)

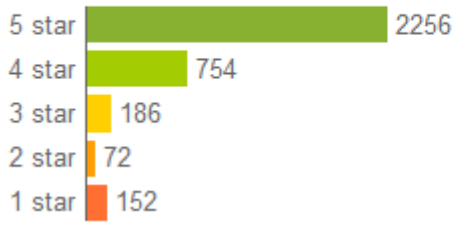


Opera Mini Permissions Screen (Second Screen)

大部份人在安裝時並不會去注意這件事情

注意評等數及使用者評論

使用者評論



平均評分：

4.4

★★★★½

3,329

總覽 | 使用者評論 (9) | 新功能 | 權限

It's cool.

★★★★★ by solar – 2011年4月5日

很棒的界面，不過pro版的功能比免費的還少，而且還竟錯字，但如果可以有清除查詢歷史資料的功能那就更完美了!

★★★★★ by Kevin – 2011年5月23日

在高鐵上只能顯示到238km/h, 再快就不會更高，請改善

★★★☆☆ by Adiemue – 2011年5月13日

Good performance! Quick response to speed change! No ads

★★★★★ by Terence – 2011年4月5日

多方參考意見可尋到蛛絲馬跡

來路不明連結不要輕易點選

收到簡訊或流行的Line/Whatsapp好友訊息，最號請與傳送者確認是否安全才點選。

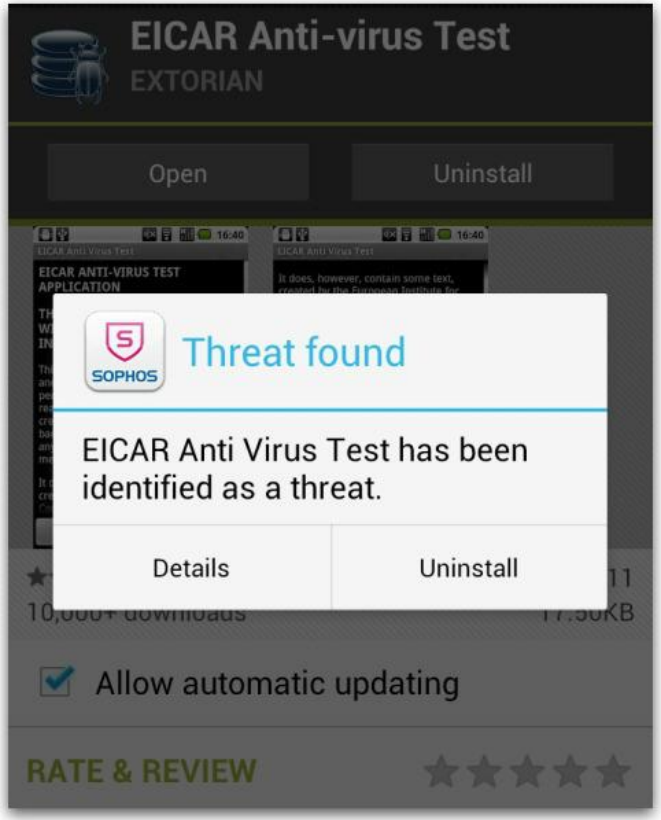
原文網址: 太熱心就上當！LINE好友傳萌犬比賽討讚　戳一下錢沒了 | ETtoday生活新聞 | ETtoday 新聞雲 http://www.ettoday.net/news/20131122/299205.htm#ixzz2ldR1KDLq
Follow us: @ETtodaynet on Twitter | ETtoday on Facebook

太熱心就上當！LINE好友傳萌犬比賽討讚　戳一下錢沒了
www.ettoday.net

前陣子會陌生的LINE帳號傳送「照片上的人是你嗎？」等口語化訊息，讓人失去戒心點開網址；現在又有駭客盜用使用者帳號，傳給其好友「我朋友的狗狗參加比賽，一定幫忙讚一個哦，感

提高設備安全性

✓Android手機：Menu->設定->安全性->裝置管理，確認<u>未知的來源</u>沒有勾起。

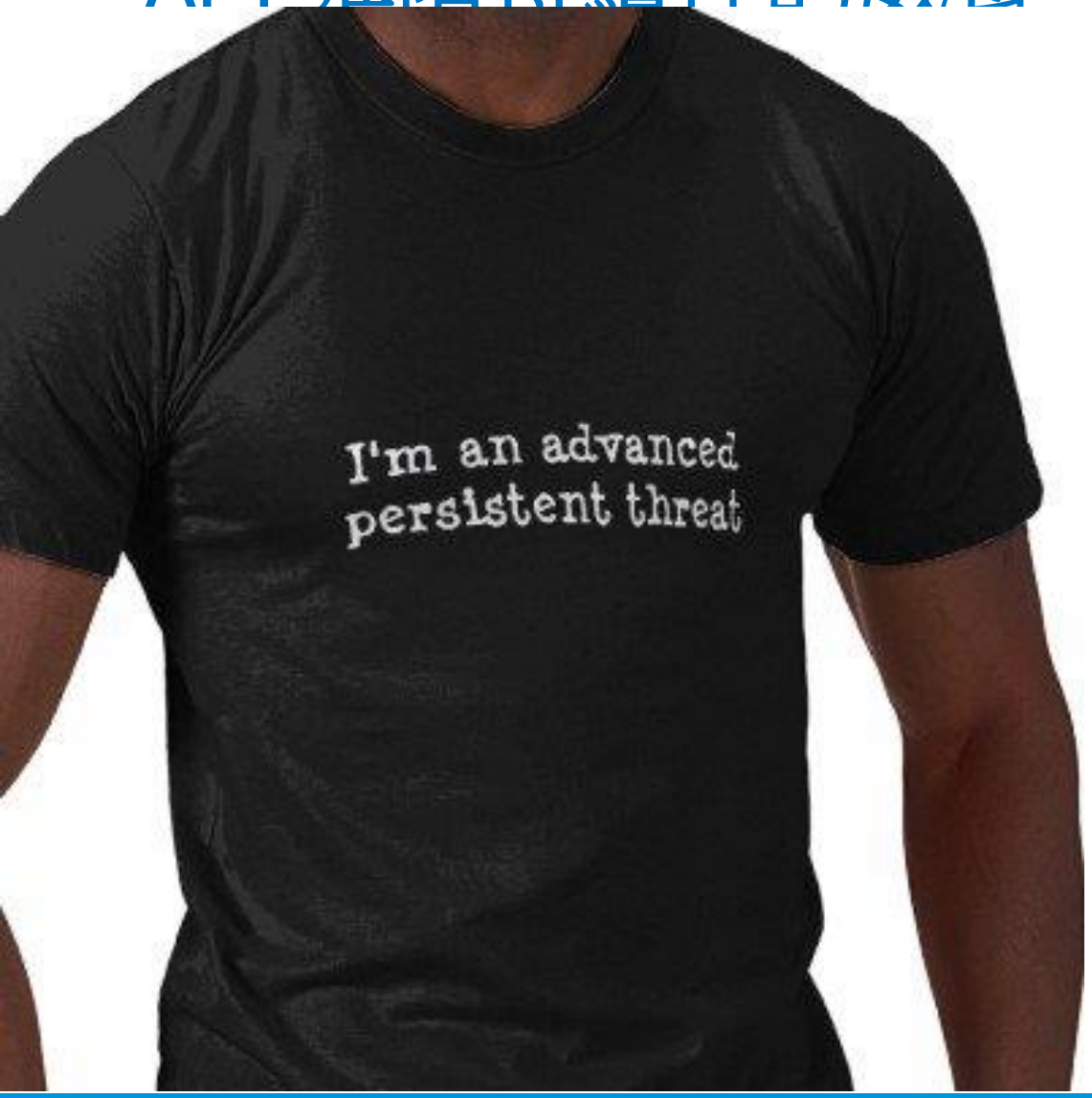


✓安裝防毒軟體

SOPHOS

APT攻擊的威脅

APT 進階持續性的威脅



是一種具策略性新型態攻擊方式，此類攻擊者通常都非常有耐性，不再為了蠅頭小利或一時的虛名而行，他們能為了一個終極目標持續幾天、幾週、幾個月，甚至更久。

APT攻擊的特性

- 低調/持續進行
- 未達目標絕不放棄
- 結合客製化惡意程式
- 運用社交工程
- 精準攻擊


www.china-defense-mashup.com

Step 1：Collect Personal Information

www.samehsvpost.org

SOCIETY OF AMERICAN MILITARY ENGINEERS

Huntsville, AL Post
PO Box 1600
Huntsville, AL 35807-3401

DEDICATED TO NATIONAL DEFENSE

Quick Launch

(HOME)

- *Post Officers, Board Members, & Committee Chairpersons*
- *SAME State of the Post - 2011*
- *Huntsville Post Newsletters*
- *Board Minutes*
- *Sustaining Members*
- *Constitution & Bylaws*
- *Scholarships*
- *Photo from 2011 Golf Tournament*
- *Recent Presentations*
- *Photos from Meetings*
- *Awards*
- *PDH Certificates and Attendees*
- *SAME National Link*
- *External Link: Engineering and Construction Camps*
- *Contact Us*

DIRECTORS				
Director (odd year)	Dennis Bacon	(256) 830-1031 X125		dbacon@shearerassociates.u
Director (odd year)	Charlie Joyner	(256) 799-3292		Cjoyner@csc.com
Director (even year)	John Rivenburgh	(256) 705-8564		jdjriven@comcast.net
Director (even year)	COL Nello Tortora	(256) 895-1300		Nello.Tortora@usace.army.m
COMMITTEES				
Awards	Margaret Zaice	(256) 217-2563		Margaret.Zaice@parsons.cor
Membership	Lael Feist, P.E.	(256) 837-5844		LaelRuth.Feist@CH2M.com
Sustaining Membership	James Kling	(205) 595-8188 EXT 803		JKling@onestopenv.com
Constitution & ByLaws	Harry Spear	(256) 313-9495		Harry.Spear@mda.mil
Programs	Roger Young	(256) 382-9728		roger.young@ipc-us.com
Publicity	Judy Wilson	(256) 777-0570		JudyOK@aol.com
Golf Tournament	Jeff Jones	(256) 551-1968	(256) 503-4183	jeffrey.jones@tetratech.com
Mail/Listserver	Deborah Walker	(256) 895-1796		Deborah.D.Walker@usace.ar

Step 2：Customize Malware

精心設計的腳本，難以分辨真偽

malware.pdf - Adobe Reader

File Edit View Document Tools Window Help

1 / 1 61.8% Find

"25th" Annual Huntsville Post SAME Golf Tournament

ENTRY RESERVED FOR FIRST 128 GOLFERS

Thursday, OCTOBER 6, 2011

Rain date: Friday October 7, 2011

SUNSET LANDING GOLF COURSE

(at the Huntsville International Airport)

To benefit the Huntsville Post SAME Scholarship Fund

1030 AM CHECK-IN & LUNCHEON

12:00 PM SHOTGUN START

POST TOURNAMENT AWARDS

Come out and join us for a four-person scramble. The cost is $55 per person and includes green fees, cart, range balls, lunch and after tournament awards. You do not have to be an SAME member to play.

HOW TO BE A SPONSOR

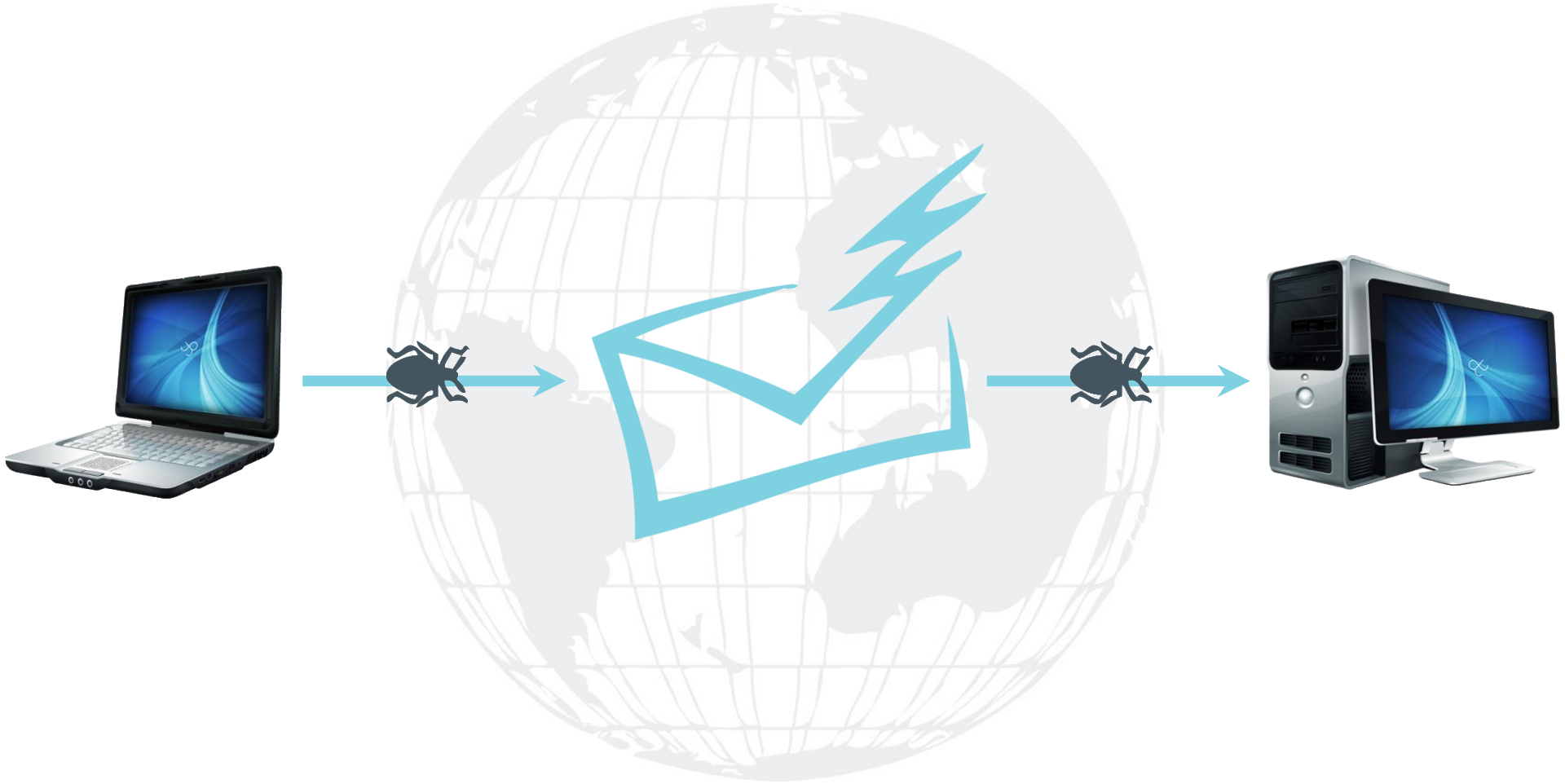
- Title Sponsor - $2,000, includes two, four person teams (call or email Jeff Jones for additional details)
- Lunch Sponsor - $1,000, includes one, four person team (call or email Jeff Jones for additional details) Businesses may get a Team Sponsor Package for $500 Sponsor a hole and get a four person team (Save $70!)
- Raffle Prize Sponsor - $500
- Businesses may sponsor a hole for $350
- Donate Door Prizes or Awards for the Post Tournament Awards
- Donate golf paraphernalia or other company logo items for the "goodie bags"

Please send payment and entry forms no later than close of business **Monday, September 19, 2011**. Call Jeff Jones (jeffrey.jones@tetratech.com) at 256-503-4183 or Phil Loftis at 256-217-2532 if you have any questions.

TEAM CAPTAIN _____

COMPANY

Step 4：Send Email

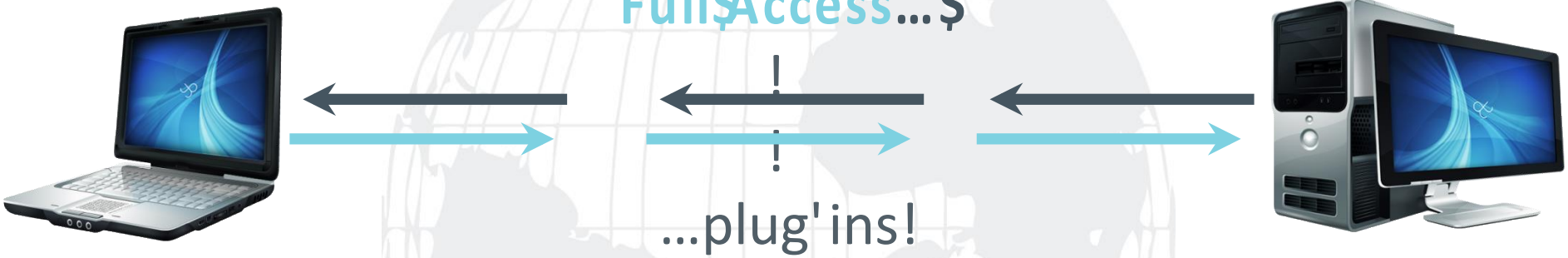


74%$
FAIL$

McAfee®

KASPERSKY ANTI •VIRUS

Step 5：Full Control



without!files!!

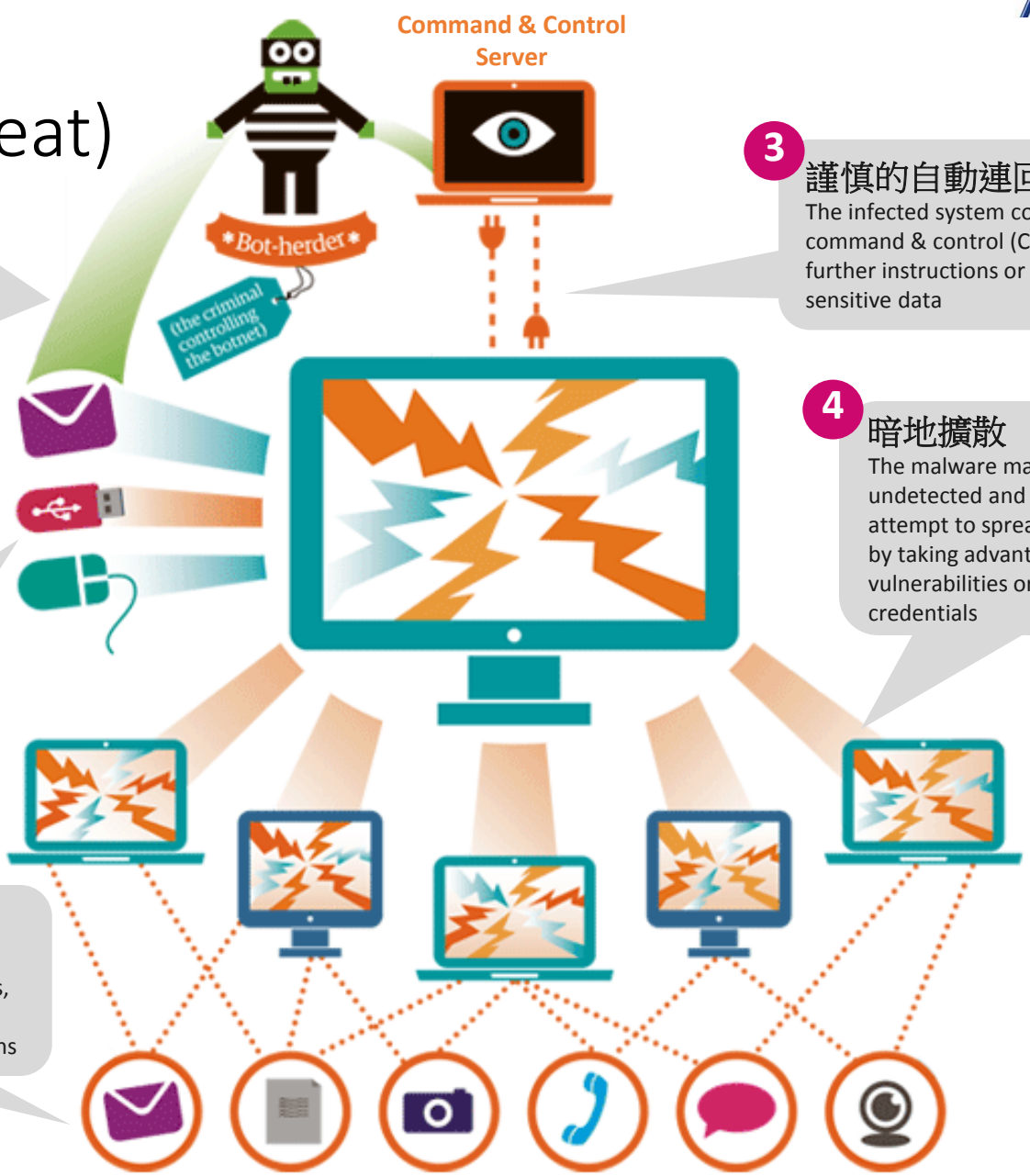
!

!

敵人躲在自家城牆內


殭屍電腦
殭屍電腦
中繼站
駭客

進階的威脅 (Advance Threat)



1 針對性的攻擊
Advanced Persistent Threats (APTs) are usually targeted at specific industries, organizations, or even individuals and may involve significant research into personnel, offices, IT practices, operations, and much more to help gain a foot-hold

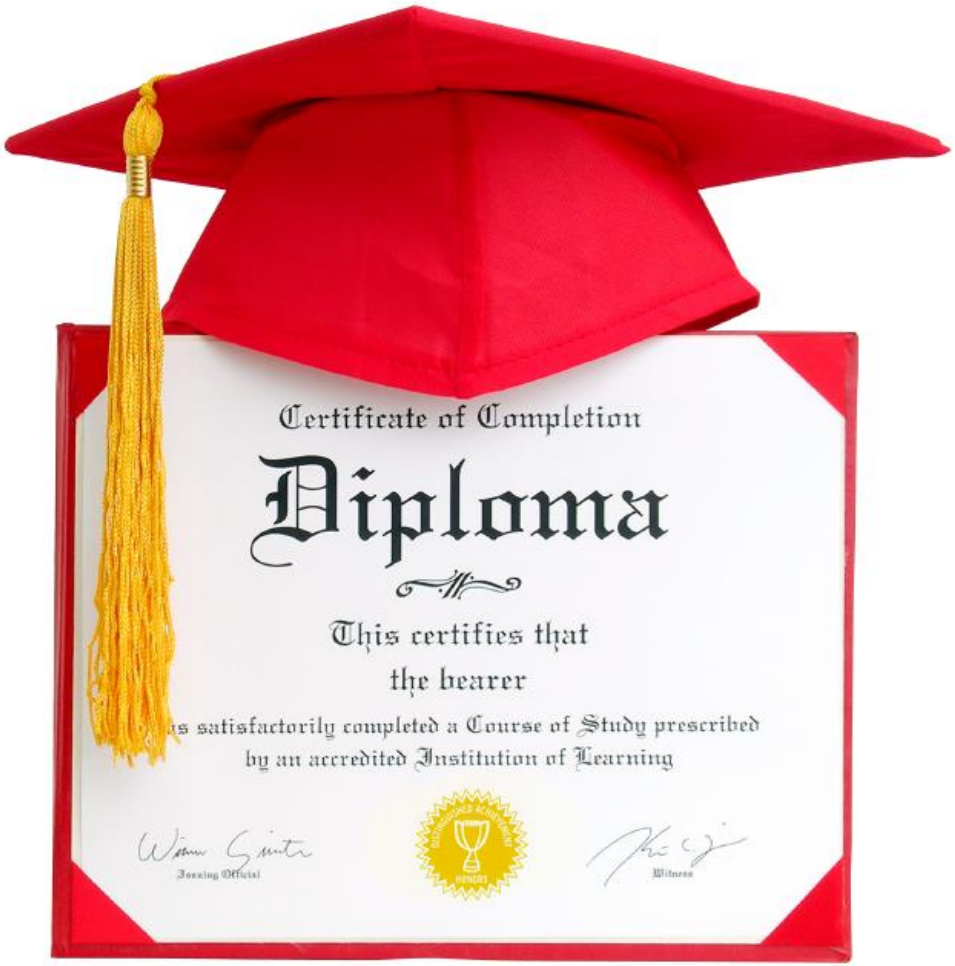
2 進入點
Targeted or not, the initial system is usually infected by either:
- Visiting an infected website
- Opening an email attachment
- Plugging-in a USB stick

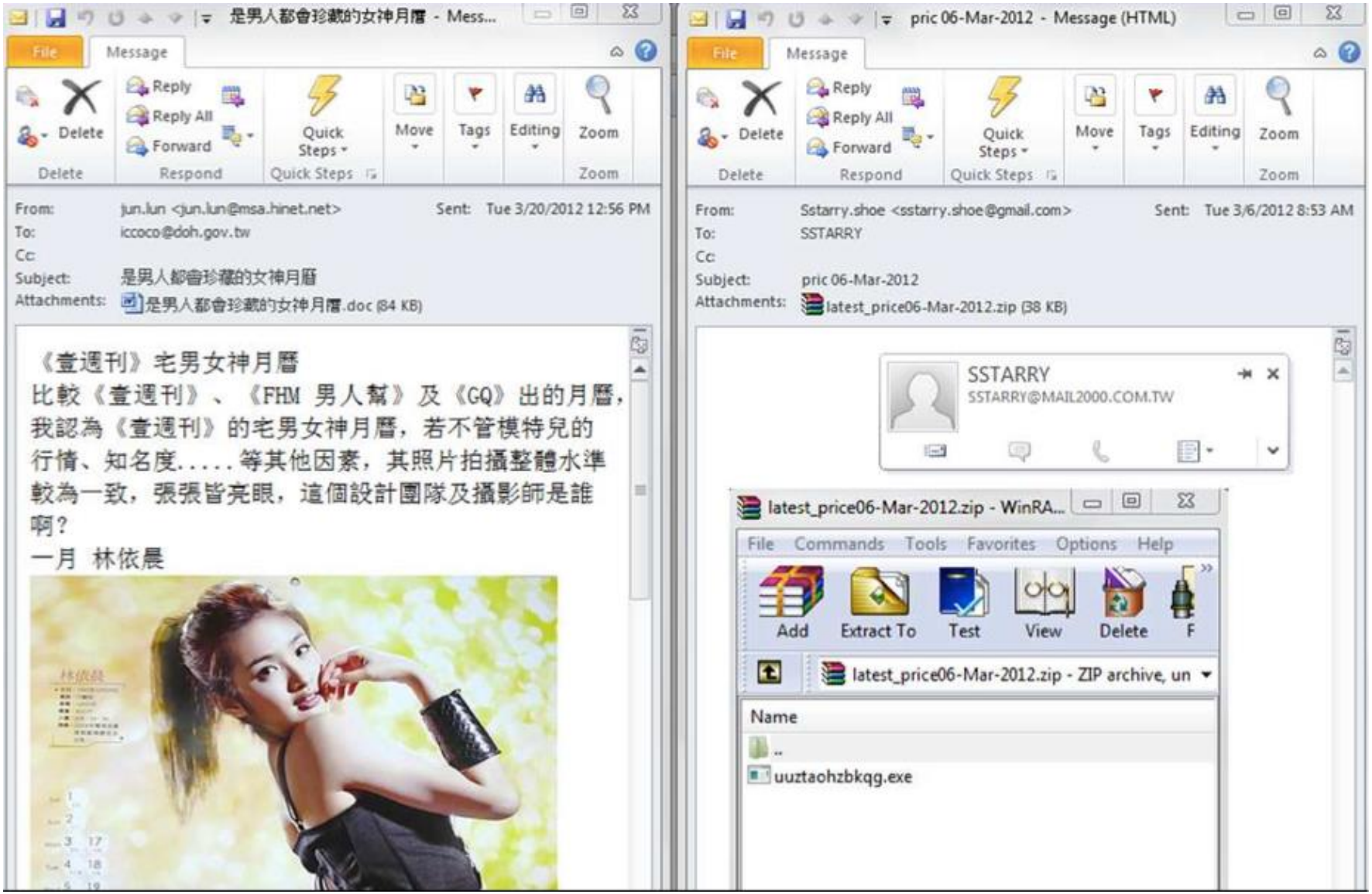
3 謹慎的自動連回特定位置
The infected system connects to the command & control (C&C) server for further instructions or to start passing sensitive data

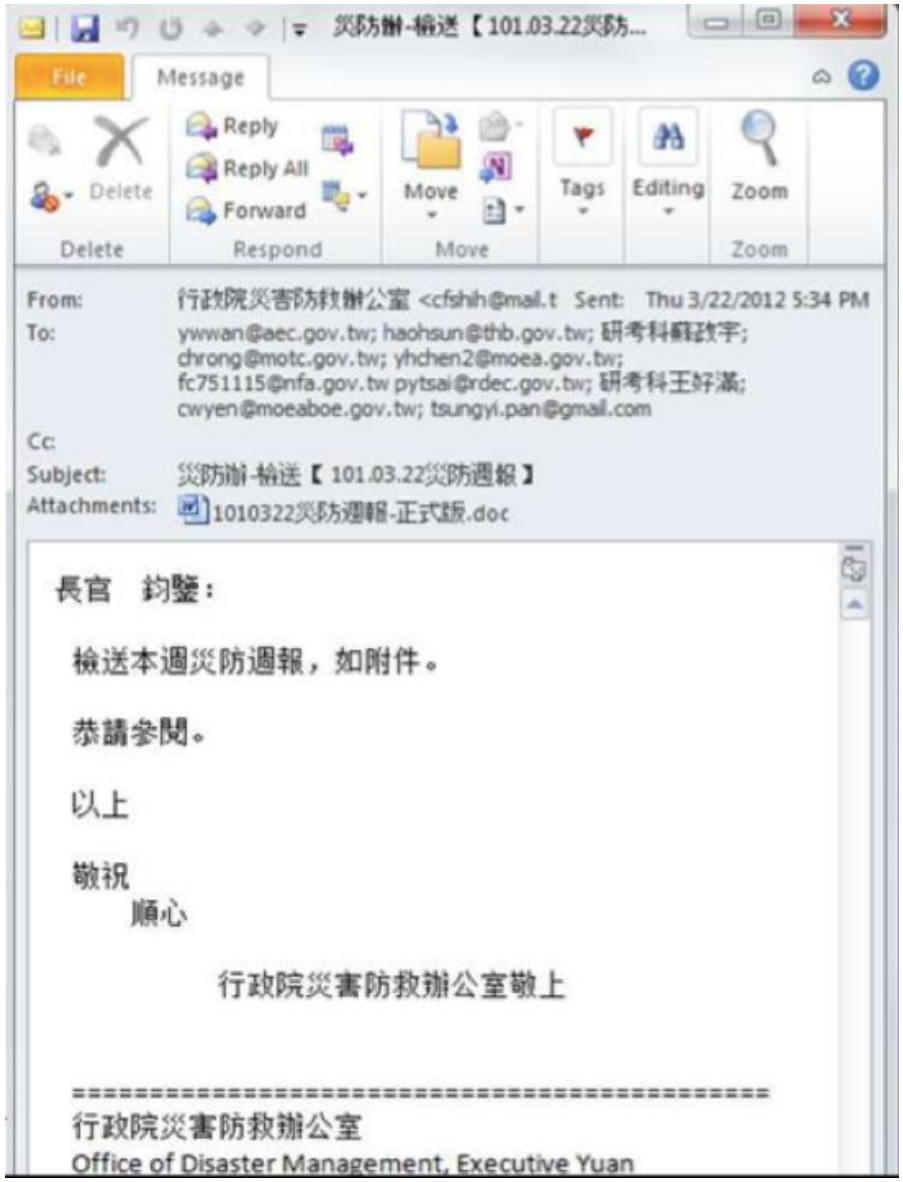
4 暗地擴散
The malware may choose to remain undetected and move slowly or it may attempt to spread to other systems by taking advantage of unpatched vulnerabilities or using hijacked credentials

5 低調的洩漏資料
The malware may attempt to steal information from emails, documents, Skype or IM conversations, or even webcams depending on it's intentions

Congratulations




是男人都會珍藏的女神月曆 - Mess...
File
Message
Reply
Reply All
Forward
Delete
Quick Steps
Move
Tags
Editing
Zoom
Delete
Respond
Quick Steps
Zoom
From: jun.lun <jun.lun@msa.hinet.net>
Sent: Tue 3/20/2012 12:56 PM
To: iccoco@doh.gov.tw
Cc:
Subject: 是男人都會珍藏的女神月曆
Attachments: 是男人都會珍藏的女神月曆.doc (84 KB)
《壹週刊》宅男女神月曆
比較《壹週刊》、《FHM 男人幫》及《GQ》出的月曆，我認為《壹週刊》的宅男女神月曆，若不管模特兒的行情、知名度.....等其他因素，其照片拍攝整體水準較為一致，張張皆亮眼，這個設計團隊及攝影師是誰啊？
一月 林依晨
pric 06-Mar-2012 - Message (HTML)
From: Sstarry.shoe <sstarry.shoe@gmail.com>
Sent: Tue 3/6/2012 8:53 AM
To: SSTARRY
Cc:
Subject: pric 06-Mar-2012
Attachments: latest_price06-Mar-2012.zip (38 KB)
SSTARRY
SSTARRY@MAIL2000.COM.TW
latest_price06-Mar-2012.zip - WinRA...
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
latest_price06-Mar-2012.zip - ZIP archive, un
Name
..
uuztaohzbkqg.exe


災防辦-輸送【101.03.22災防...
File
Message
Reply
Reply All
Forward
Delete
Move
Tags
Editing
Zoom
Delete
Respond
Move
Zoom
From: 行政院災害防救辦公室 <cfshih@mail.t Sent: Thu 3/22/2012 5:34 PM
To: ywwan@aec.gov.tw; haohsun@thb.gov.tw; 研考科蘇致宇;
chrong@motc.gov.tw; yhchen2@moea.gov.tw;
fc751115@nfa.gov.tw pytsai@rdec.gov.tw; 研考科王妤潔;
cwyen@moeaboe.gov.tw; tsungyi.pan@gmail.com
Cc:
Subject: 災防辦-輸送【101.03.22災防週報】
Attachments: 1010322災防週報-正式版.doc
長官 鈞鑒：
檢送本週災防週報，如附件。
恭請參閱。
以上
敬祝
順心
行政院災害防救辦公室敬上
==========
行政院災害防救辦公室
Office of Disaster Management, Executive Yuan

水坑式攻擊

全國公文系統被駭

- 2013年5月發現
- 全國7千多個機關受害
- 動員百人耗時3個月恢復正常

電子公文交換系統受駭，超過7千個機關受影響

全臺公務機關傳遞各式電子公文的行政院電子公文交換網路系統於5月初發現遭駭，負責電子公文交換的終端軟體eClient，在提供該軟體直接下載的網站中，eClient 的執行檔被置換成一個惡意程式，對外連線到不明的中繼網站。行政院資通安全辦公室預估，全臺超過7,000個政府機關受到影響，包括中央機關、地方機關、市政公所、醫院、中小學校等。

行政院資通安全辦公室也發出聲明稿表示，近年來政府各機關逐步建立的網路監控機制收到成效，5月初主動偵測到公文電子交換網路系統（eClient）在機關外端有異常行為，經追查確認係遭新型態惡意攻擊植入惡意程式。

經行政院資通安全辦公室召開多次專案會議，決定重建受駭的公文交換系統，以避免殘留惡意程式。該聲明稿中指出，目前中控端已完成重建，行政院檔案管理局於5月22日邀集各機關說明eClient更版程序及注意事項等，預計可於5月底前完成外端掃毒及更新。

通報中也要求政府各單位將已經發現的中繼站名單，更新到各單位的防火牆規則中，監控內部公務電腦是否連線到這些中繼站，判斷是否被入侵。

據了解，這起資安事件被發現的原因是，5月初時，有一個政府單位負責電子公文交換系統的人員，下載了電子公文官網上提供的新版eClient更新程式，下載並安裝後到電腦上以後，電腦上的防毒軟體卻跳出警告，通知使用者這是一個惡意程式。這位公務員將此狀況通報資通安全辦公室後，才發現這起資安事件。

行政院資通安全辦公室當時就要求，負責協助監控臺灣各個政府部門主要的4大SOC中心（包括中華電信、宏碁、數聯資安及關貿網路）和相關合作的資安廠商，來協助各個政府部門徹底檢查電子公文交換系統是否同樣遭駭。

行政院資通安全辦公室主任蕭秀琴表示，目前政府已經掌握新攻擊手法的模式，因為其複雜與精密程度是過去所罕見，應該是駭客長期埋伏且是有組織、有系統的行為。

蕭秀琴說，目前政府部門最要緊的是復原系統、清查到底「掉了什麼」？原因是什麼？以及如何才能避免再發生類似資安漏洞。而行政院資通安全辦公室為求徹底防範，除了將這次資安事件，列為次嚴重的第三級資安事件外，也全面更新七千多部的電腦eClient軟體。**全國有6成電子公文有外洩風險**

行政院電子公文交換系統受駭，受影響的範圍深遠。行政院國家檔案管理局副局長林秋燕表示，全臺有7,303個機關都使用eClient做為電子公文交換，包括中央各部會、地方政府各機關，如鄉鎮市公所、醫院與國高中、國小等各級學校等，也都在此次受影響的範圍內。

- 2013/3/20 PM2:00 3大電視台，銀行/ATM大當機
- ATM採Window平台並安裝南韓自有品牌防毒軟體
- 惡意程式早已滲透進入南韓防毒廠商更新伺服器

Sony Picture事件

- 2014/11/24 員工收到來自GoP組織在電腦上視窗的警告
- 辦公室的電腦/伺服器全部停擺，員工被迫回家工作
- 洩漏資料：
  - 商業影片檔
  - 員工個資/薪資
- 公司市值蒸發600億

APT Events Sample

Host

Remote network

Advanced Threat Protection: Recent Events

Total Events: 208

	User/Host	Threat Name	Destination	Events	Origin	
1	192.168.107.90	C2/Generic-A	tv.shipinjiandu.com	2	AFCd	+
2	192.168.20.188	C2/Generic-A	down.395tian.com	1	AFCd	+
3	192.168.20.188	C2/Generic-A	ftp170685.host307.web538.com	2	AFCd	+
4	192.168.43.135	C2/Generic-A	click.leimg8.com	1	AFCd	+
5	192.168.20.145	C2/Generic-A	www.zxckkk.com	1	AFCd	+
6	192.168.20.145	C2/Generic-A	www.go2apx.com	5	AFCd	+
7	192.168.20.188	C2/Generic-A	www.go2apx.com	5	AFCd	+
8	192.168.20.188	C2/Generic-A	www.zxckkk.com	5	AFCd	+
9	192.168.20.145	C2/Generic-A	forum.l2gangstarr.com	2	AFCd	+
10	192.168.20.188	C2/Generic-A	forum.l2gangstarr.com	2	AFCd	+

IPS：排名靠前的阻止的攻击

没有可供此报告使用的数据

IPS：排名靠前的攻击者

没有可供此报告使用的数据

APT Events Sample

Botnet downloading additional malware

```
2014:03:03-00:29:56 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?guangdong.fushan" action="drop"
2014:03:03-00:37:53 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?guangdong.fushan" action="drop"
2014:03:03-00:38:22 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="223.6.250.180" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="www.go2apx.com" url="/mv_110_5601.exe" action="drop"
2014:03:03-00:54:52 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?yunnan.zhaotong.chuzhou" action="drop"
2014:03:03-00:55:17 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?yunnan.zhaotong.chuzhou" action="drop"
2014:03:03-00:55:23 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?yunnan.zhaotong.chuzhou" action="drop"
2014:03:03-00:55:30 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?yunnan.zhaotong.chuzhou" action="drop"
2014:03:03-00:56:40 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?yunnan.zhaotong.chuzhou" action="drop"
2014:03:03-00:57:01 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?yunnan.zhaotong.chuzhou" action="drop"
2014:03:03-00:57:08 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?yunnan.zhaotong.chuzhou" action="drop"
2014:03:03-00:57:13 testDevice afcd[25628]: id="2022" severity="warn" sys="SecureNet" sub="packetfilter" name="Packet dropped (ATP)" srcip="192.168.20.188"
dstip="119.84.119.219" fwrule="63001" proto="6" threatname="C2/Generic-A" status="1" host="q.hr44.com" url="/dt.asp?yunnan.zhaotong.chuzhou" action="drop"
```

SOPHOS

日益猖獗的勒索病毒


CryptoLocker
请注意!
我们将使用病毒Crypt0L0cker为您的所有文档加密。
单击此处可付款还原文档。
常见问题
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
10/9/2013
4:25 PM
Time left
95 : 56 : 35
Next >>

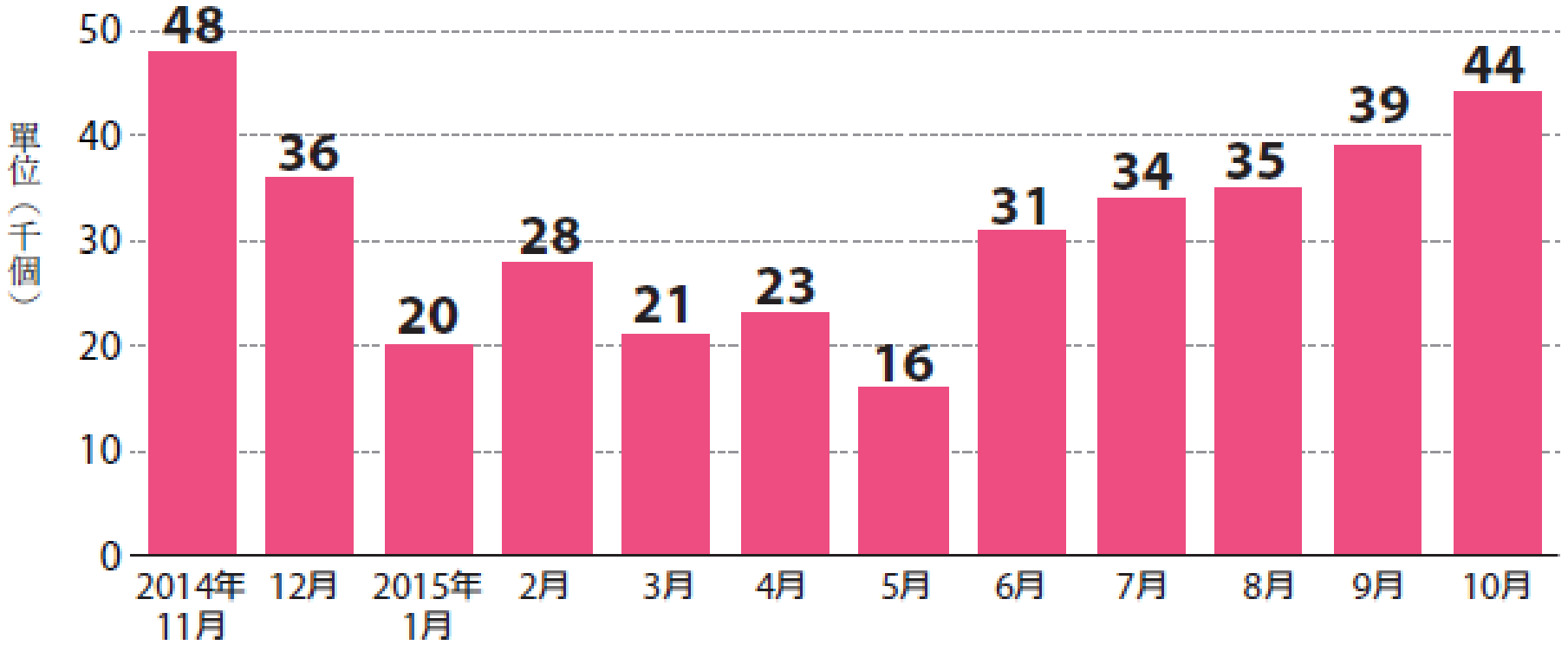
FIGURE 2: Attempted Infections of CW3. Source: Cyber Threat Alliance

最壞勒索軟體CryptoWall 3已造成3.25億美元損失

美國洛杉磯醫院電腦遭駭客挾持勒索360萬美元

最強大勒索軟體

CryptoWall進化到4.0版，更難偵測，連檔名都加密！


單位（千個）
50
40
30
20
10
0
48
36
20
28
21
23
16
31
34
35
39
44
2014年 11月
12月
2015年 1月
2月
3月
4月
5月
6月
7月
8月
9月
10月

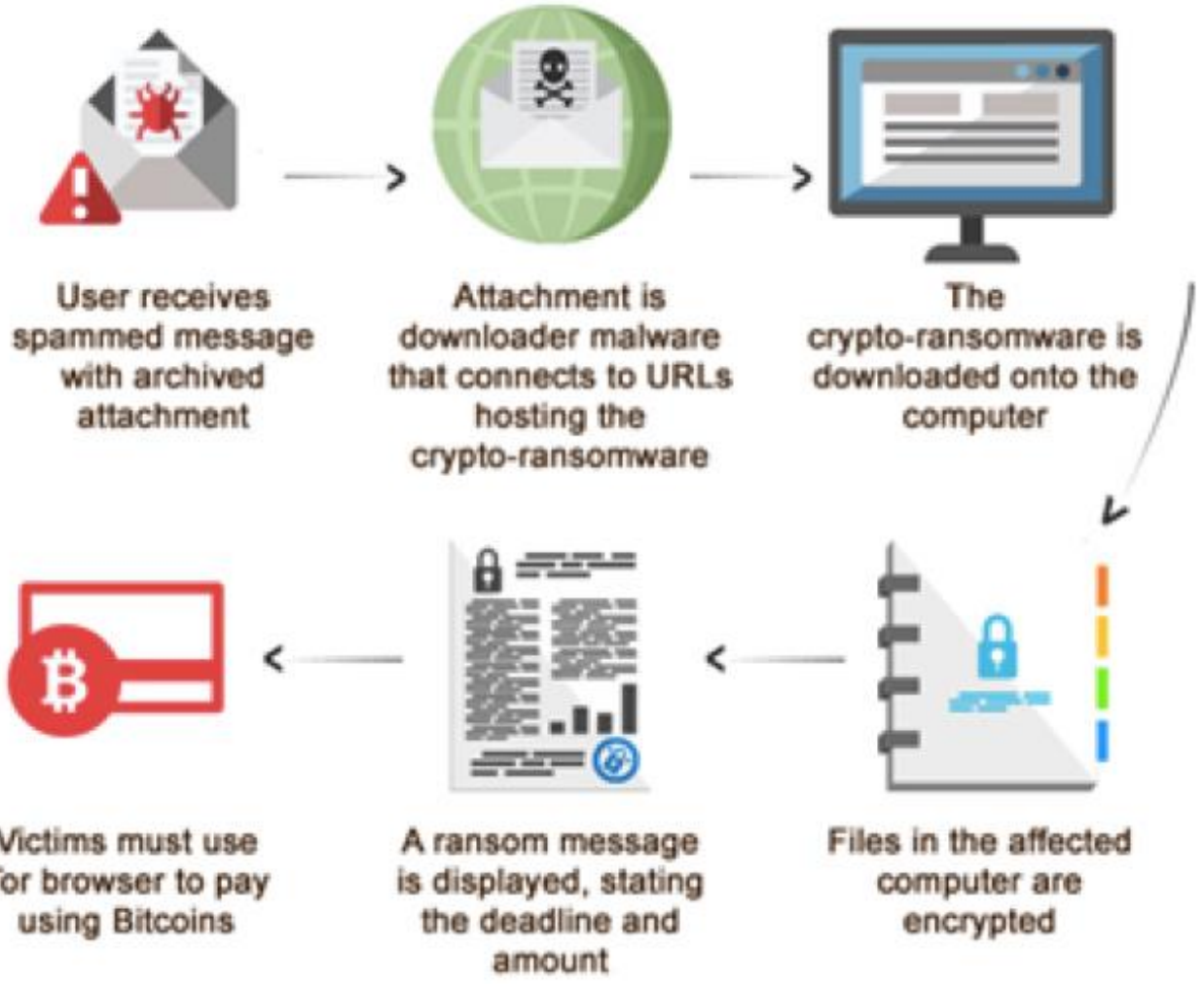
- 偽裝成快遞信件...
- 附件夾帶隱藏的惡意程式
- 回報惡意中站,下載金鑰
- 將Pdf / Word / Excel / PowerPoint .... 檔案加密
- 跳出付款解鎖警訊，需要金鑰才可以解開

假 Windows 10 更新連結暗藏勒索軟體

- 勒索軟體 Ransomware
- 假冒各種形式
  - Windows 10 update
  - 防毒軟體
  - 解毒軟體
  - …

假冒免費 Windows 10 更新通知信件暗藏勒索軟體

不給錢，手機變磚頭


User receives spammed message with archived attachment
Attachment is downloader malware that connects to URLs hosting the crypto-ransomware
The crypto-ransomware is downloaded onto the computer
Files in the affected computer are encrypted
A ransom message is displayed, stating the deadline and amount
Victims must use Tor browser to pay using Bitcoins

勒索病毒感染途徑

- 電子郵件
  - 包含惡意程式的附件或連結
- 惡意網站
  - 包含惡意連結或廣告

進化中的勒索病毒

- 檔案名稱加密
- 預設金鑰
- 植入網頁中(JavaScript)，瀏覽就中標
- 跨平台，勒索病毒不再侷限於 Windows 平台

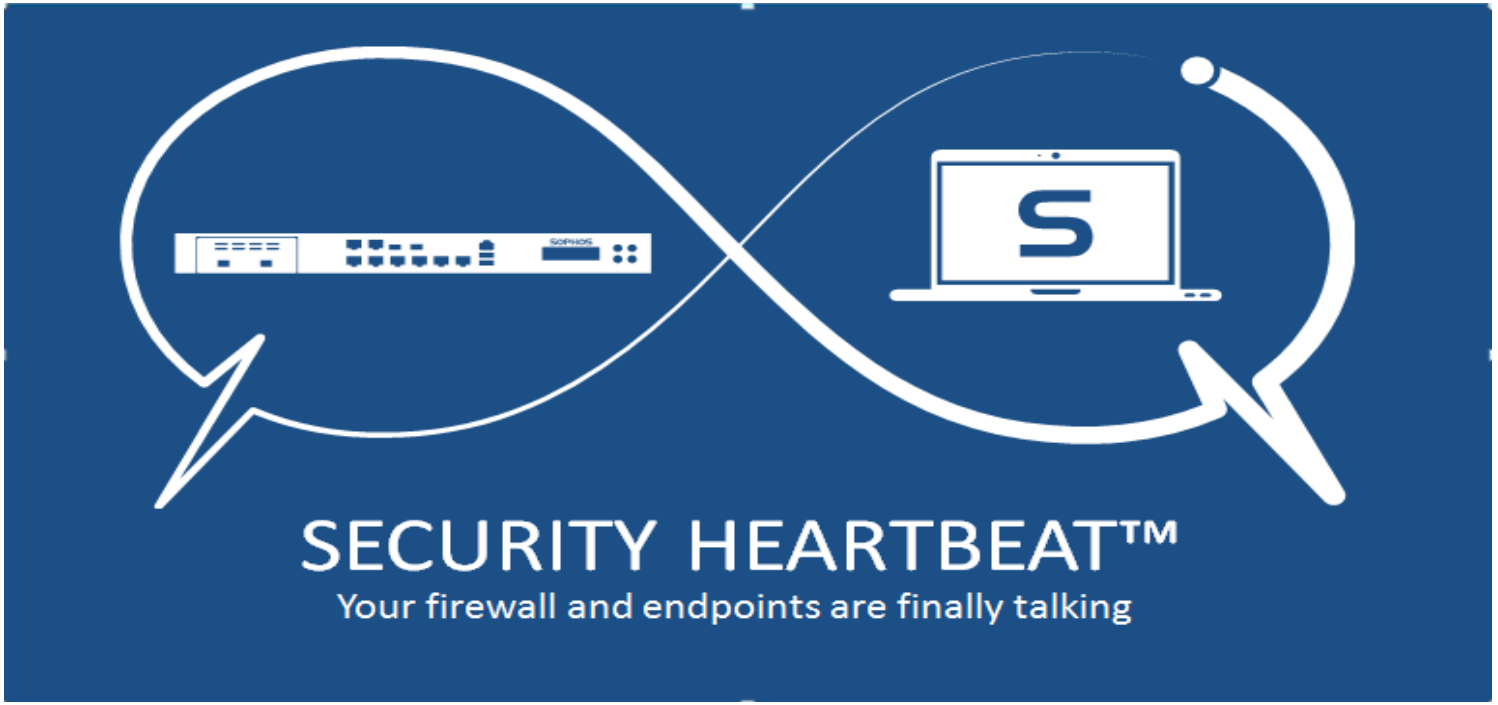
Ras

SOPHOS

聯合防禦解決方案

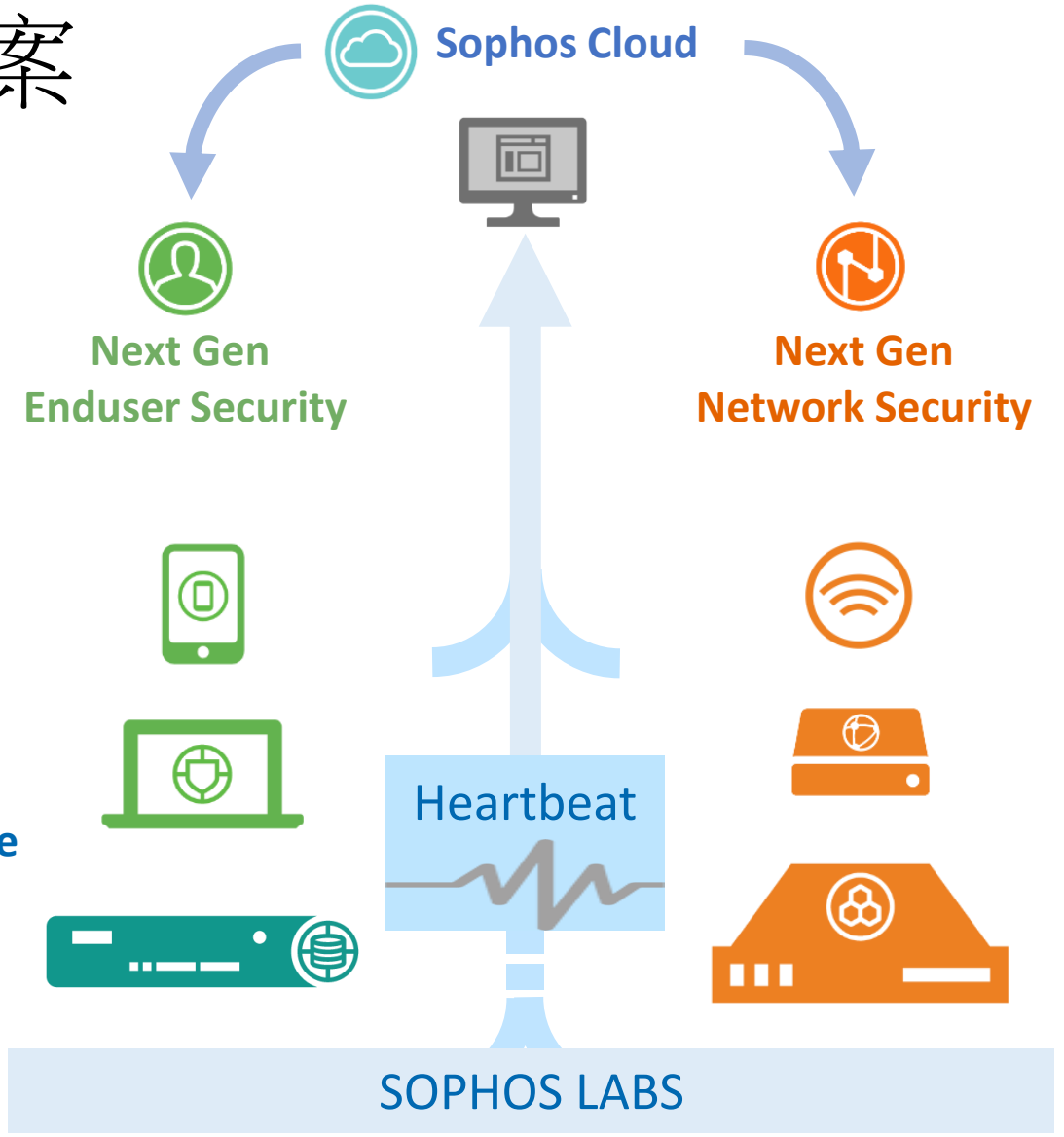
如何防禦日趨複雜的資安環境

- 強化資安架構(縱深與聯防)
  - 聯合閘道安全設備與端點防護

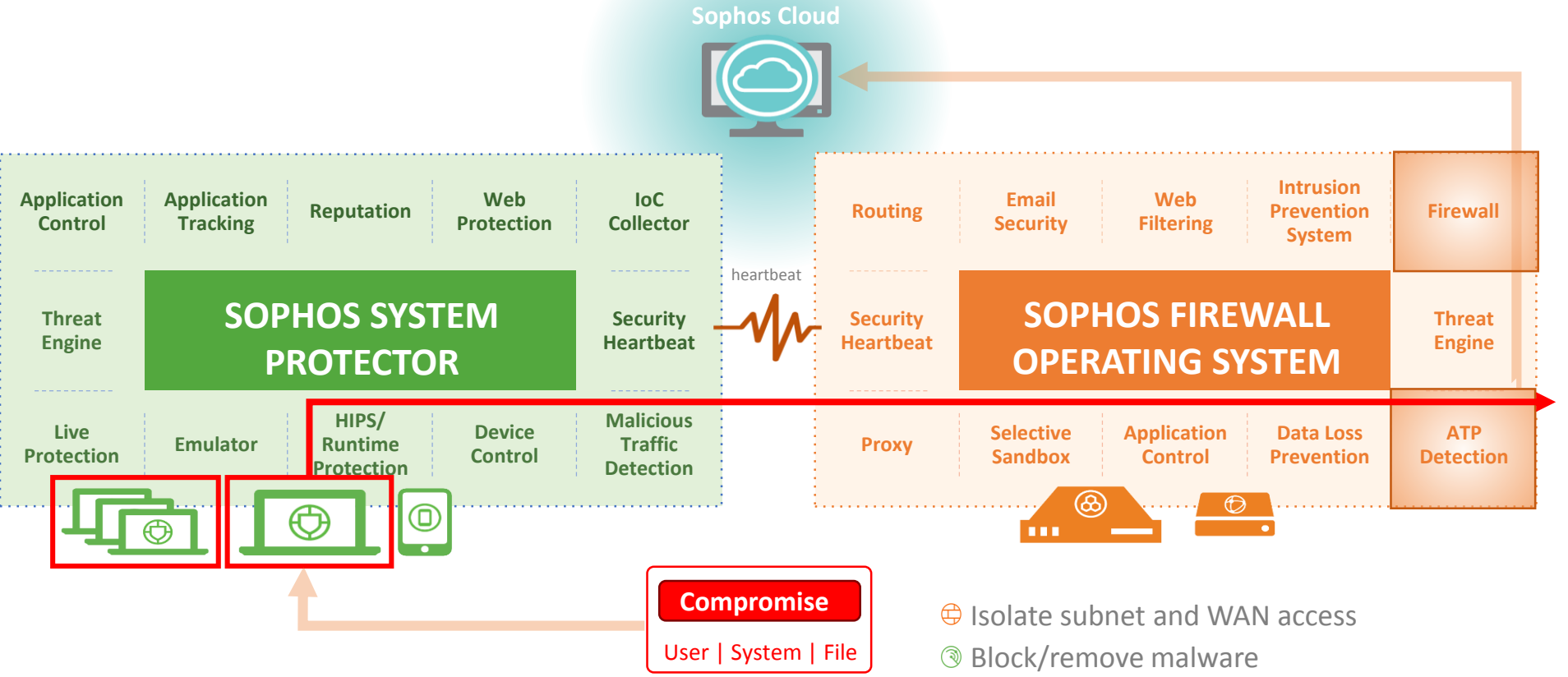


Sophos解決方案

- **Accelerated Threat Discovery**
- **Active Source Identification**
- **Automated Incident Response**



Synchronized Security: Next Generation Threat Detection



聯合防禦，提升資安事件能見度與即時反應

Sophos XG Security Gateway

+

Sophos Cloud Enduser Protection

唯一網路與端點安全領導廠商

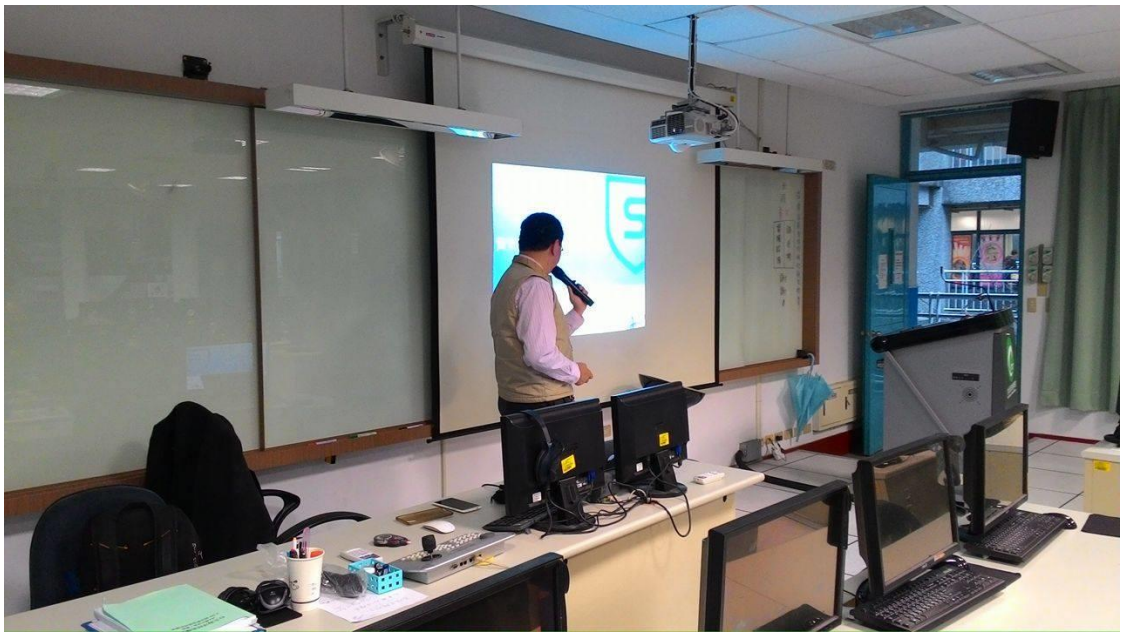
Gartner Magic Quadrant
ENDPOINT PROTECTION

Gartner Magic Quadrant
UNIFIED THREAT MANAGEMENT


?
Q
&
&
A
!

SOPHOS

活動寫真




德語
GERMANY
日語
JAPAN
西班牙語
SPAIN
泰語
THAILAND

104 學年度資訊安全認知暨網頁製作研習營 淡水場-1

時間：105 年 3 月 11 日（星期五）、~~105 年 4 月 8 日（星期五）~~ 上午 9 時 00 分至下午5點

地點：淡水校區 A202、~~士林校區 國際第一會議廳~~

出席人員：~~全體教職員~~ 共602

單位	姓名	簽到	單位	姓名	簽到
秘書室	郭展銓		時尚系	許煌珠	許煌珠
文書組	白書伃	白書伃	時尚系	徐珮清	
人事室	邵彥芬		時尚系	芮巧徽	芮巧徽
人事室	吳建忠	吳建忠	時尚系	洪于雯	洪于雯
總務處	高佩侑		時尚系	王宥婷	王宥婷
營繕組	張莉娟	張莉娟	時尚系	王立鳳	王立鳳
事務組	鄧惠貞	鄧惠貞	時尚系	黃酈淨	黃酈淨
通識中心	郭正中	郭正中	視傳系	劉東弦	
教發中心	張詠晴		食品系	林雪良	林雪良
課註組	王奕然	王奕然	食品系	林圳德	
課註組	楊喻涵		餐管系	謝宜芳	謝宜芳
衛保組	王歆婷	王歆婷	資通系	陳士孝	
圖資中心	郭子傑	郭子傑	資通系	楊連富	楊連富
圖資中心	張哲偉	張哲偉	資通系	陳建彘	陳建彘
數遊系	嚴本嘉	嚴本嘉	資通系	林慧菁	林慧菁
數遊系	蔡慧貞	蔡慧貞	教資系	陳家琪	陳家琪
銀髮系	任曉晶	任曉晶	時尚系	涂雅婷	涂雅婷
銀髮系	方佩欣	方佩欣	時尚系	陳嫚君	陳嫚君
銀髮系	宋貞儀	宋貞儀	時尚系	郭展銓	郭展銓
銀髮系	黃秀媚	黃秀媚	視傳	呂延倚	呂延倚
海觀系	余瑞軒	余瑞軒	圖資中心	黃彥志	黃彥志

104學年度資訊安全認知暨網頁製作研習營 淡水場-2

時間:105年3月11日(星期五)、~~105年4月8日(星期五)~~ 上午9點至下午5點 ~~上午9時00分~~

地點: 淡水校區A202、~~士林校區 國際第一會議廳~~

出席人員:~~全體教職員~~ 共60人

單位	姓名	簽到	單位	姓名	簽到
招生組	吳玉梅	吳玉梅	通識教發	王柏鈞	王柏鈞
招生組	余慶豐	余慶豐	教發	王文智	王文智
招生組	蔡旻娟	蔡旻娟	教發	蔡佩珊	蔡佩珊
招生組	梁雨薇	梁雨薇	教發	張詠晴	張詠晴
課註組	楊紋熙	楊紋熙	資通	陳俊銘	陳俊銘
課註組	楊喻淞	楊喻淞	財金系	許珊珊	許珊珊
課註組	李鳳	李鳳	通空系	李欣芳	李欣芳
課註組	李瑜	李瑜	航海系	高嬿祖	高嬿祖
課註組	洪嘉穗	洪嘉穗	教發	~~陳宥瑜~~	~~陳宥瑜~~
表藝系	[illegible]	[illegible]			
數遊系	[illegible]	[illegible]			
數遊系	鄭靜怡	鄭靜怡			
數遊系	[illegible]	[illegible]			
視傳系	林學志	林學志			
通識中心	吳依蓉	吳依蓉			
航運	謝榮發	[illegible]			
航運	許慧娟	許慧娟			
資通	陳士彥	陳士彥			
總務處	胡振瑜	胡振瑜			
時尚	~~王宏偉~~	~~王宏偉~~			
時尚	~~王瑞章~~	~~王瑞章~~			