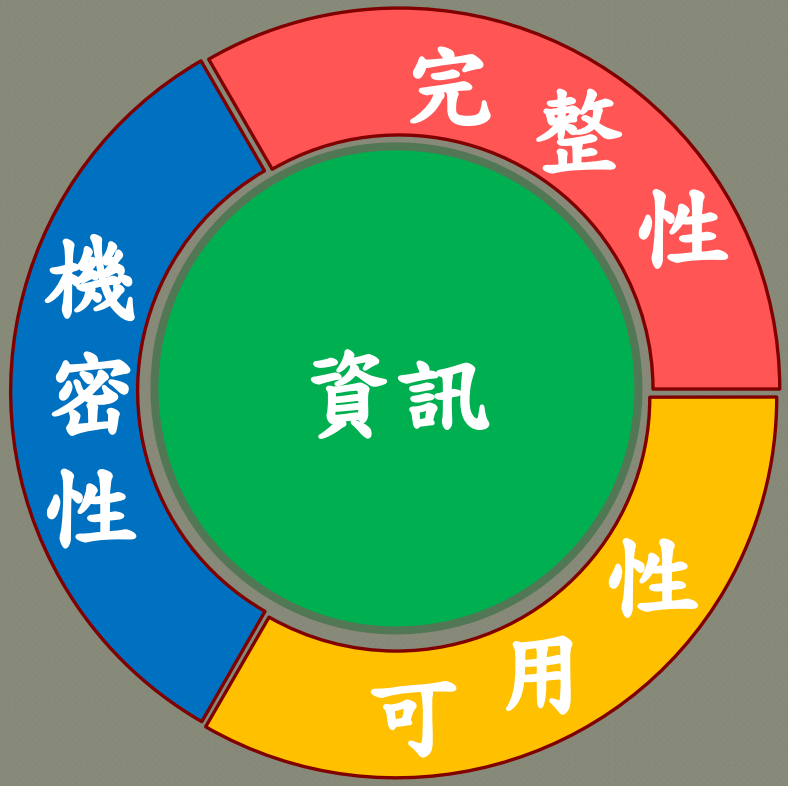
資訊安全防護

圖書資訊館網路通訊組

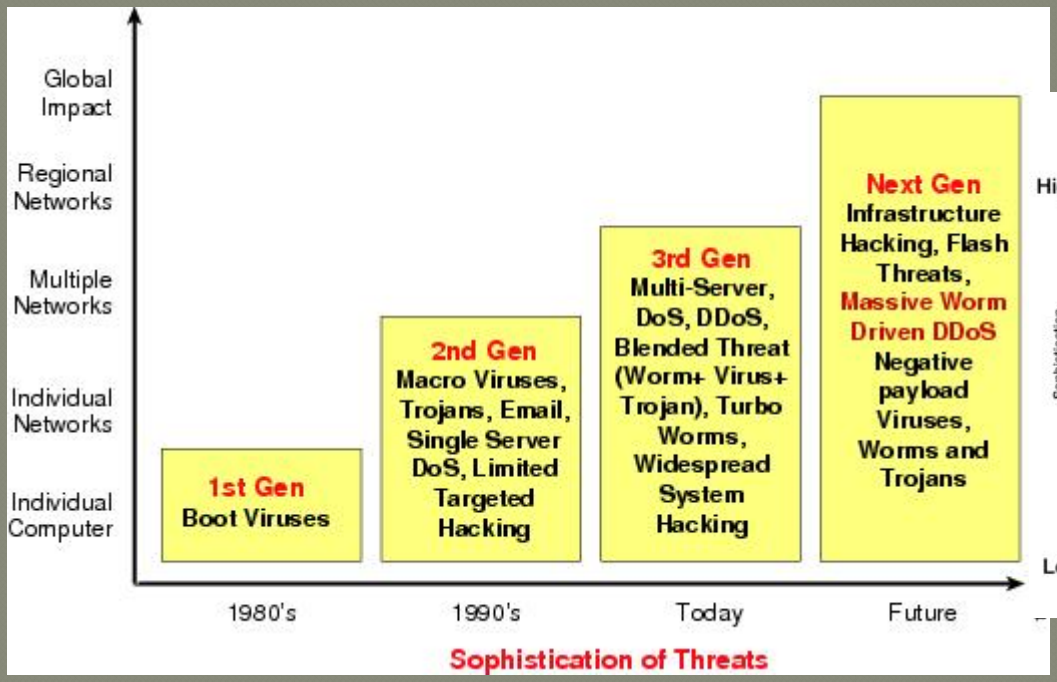
大綱

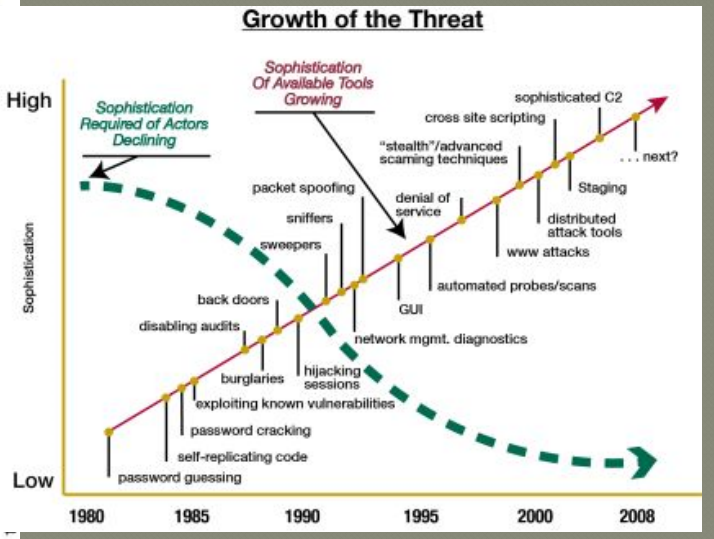
- 資訊安全概念
- 資安趨勢簡介
- 本年度重要資安事件說明

資訊安全概念



資安趨勢


Global Impact
Regional Networks
Multiple Networks
Individual Networks
Individual Computer
1st Gen
Boot Viruses
2nd Gen
Macro Viruses, Trojans, Email, Single Server DoS, Limited Targeted Hacking
3rd Gen
Multi-Server, DoS, DDoS, Blended Threat (Worm+ Virus+ Trojan), Turbo Worms, Widespread System Hacking
Next Gen
Infrastructure Hacking, Flash Threats, Massive Worm Driven DDoS
Negative payload Viruses, Worms and Trojans
1980's
1990's
Today
Future
Sophistication of Threats


Growth of the Threat
Sophistication Required of Actors Declining
Sophistication Of Available Tools Growing
High
Low
Sophistication
password guessing
self-replicating code
password cracking
exploiting known vulnerabilities
burglaries
disabling audits
back doors
hijacking sessions
sweepers
sniffers
packet spoofing
network mgmt. diagnostics
GUI
denial of service
automated probes/scans
www attacks
distributed attack tools
Staging
"stealth"/advanced scaming techniques
cross site scripting
sophisticated C2
. . . next?
1980
1985
1990
1995
2000
2008

資安趨勢

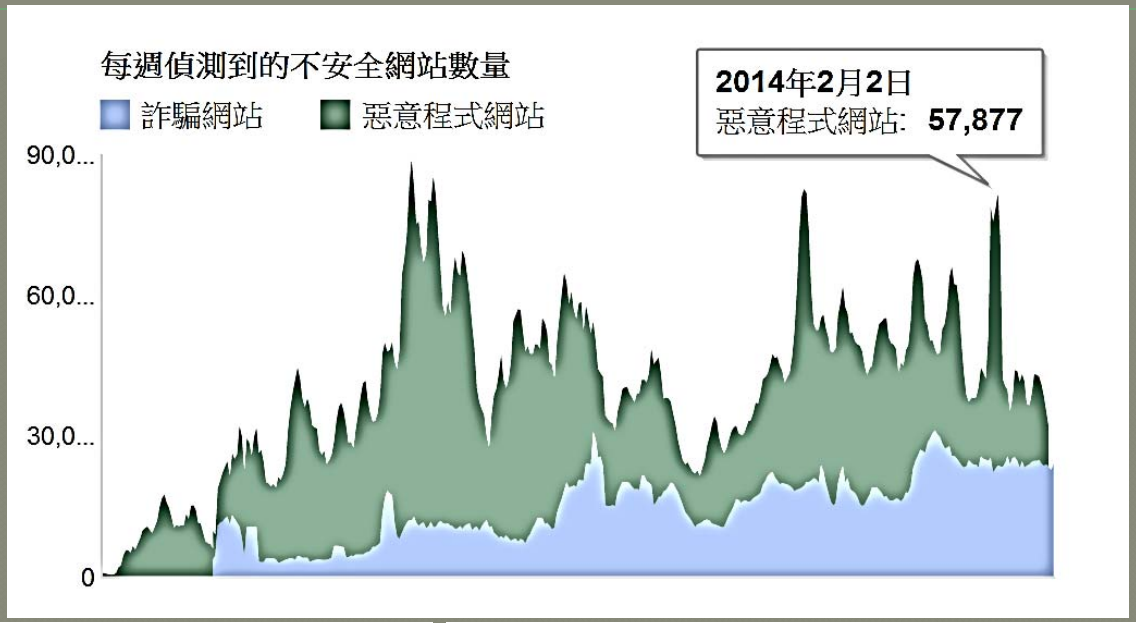
資料來源：國家資通安全會報技術服務中心

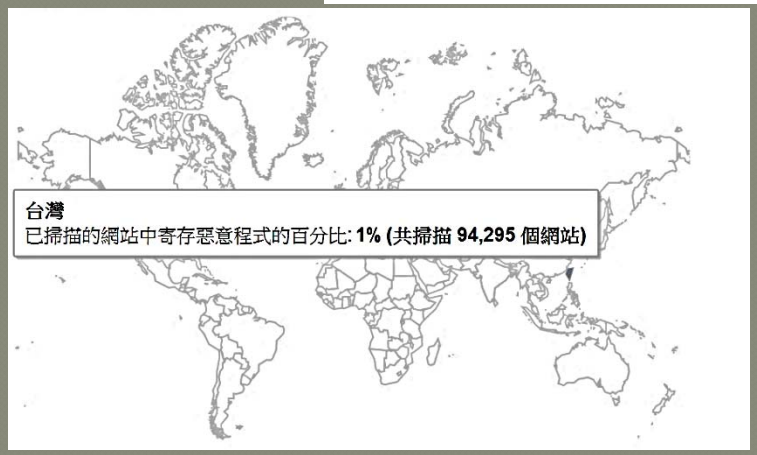
資安趨勢

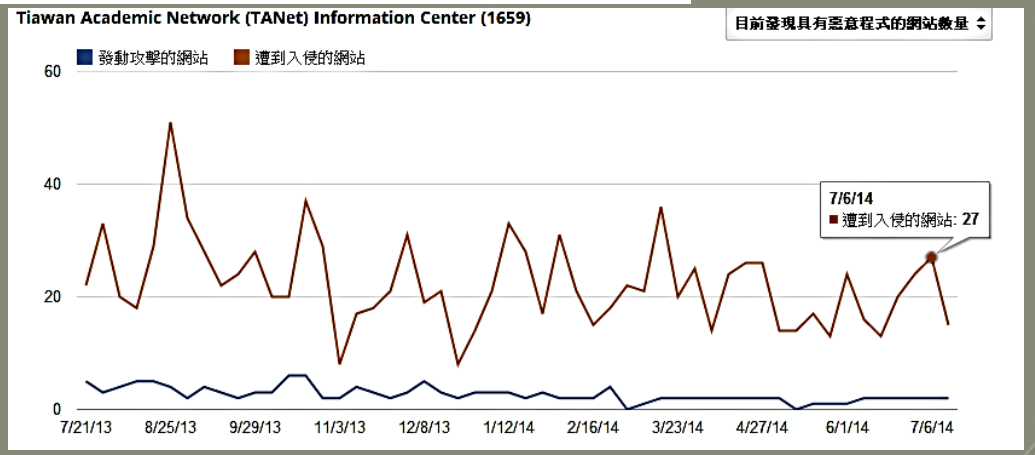
- 賽門鐵克2013年網路安全威脅研究報告
  http://bcove.me/yttsz4ar
- AKAMAI發布2013 Q4全球網路狀態報告

Region	% Attack Traffic	Unique IP Addresses	Avg. Connection Speed (Mbps)	Peak Connection Speed (Mbps)	% Above 10 Mbps	% Above 4 Mbps
Australia	0.1%	8,726,302	5.8	35.2	9.7%	54%
China	43%	120,626,188	3.4	13.8	1.8%	29%
Hong Kong	0.3%	3,062,575	12.2	68.0	37%	81%
India	0.7%	17,844,839	1.5	10.9	0.4%	3.6%
Indonesia	5.7%	7,225,893	1.6	12.5	0.1%	1.8%
Japan	0.4%	40,370,608	12.8	53.7	47%	83%
Malaysia	0.1%	2,136,588	3.0	30.0	1.7%	25%
New Zealand	<0.1%	2,139,109	5.3	21.6	6.7%	55%
Singapore	0.1%	1,563,139	7.9	59.1	19%	67%
South Korea	0.6%	20,382,592	21.9	64.4	71%	94%
Taiwan	3.4%	11,001,109	8.3	50.9	23%	68%
Vietnam	0.3%	5,985,212	1.8	12.6	0.1%	2.7%

資安趨勢


每週偵測到的不安全網站數量
詐騙網站
惡意程式網站
2014年2月2日
惡意程式網站: 57,877
90,0...
60,0...
30,0...
0


台灣
已掃描的網站中寄存惡意程式的百分比: 1% (共掃描 94,295 個網站)


Tiawan Academic Network (TANet) Information Center (1659)
目前發現具有惡意程式的網站數量
發動攻擊的網站
遭到入侵的網站
60
40
20
0
7/6/14
遭到入侵的網站: 27
7/21/13
8/25/13
9/29/13
11/3/13
12/8/13
1/12/14
2/16/14
3/23/14
4/27/14
6/1/14
7/6/14

本年度重要資安事件說明

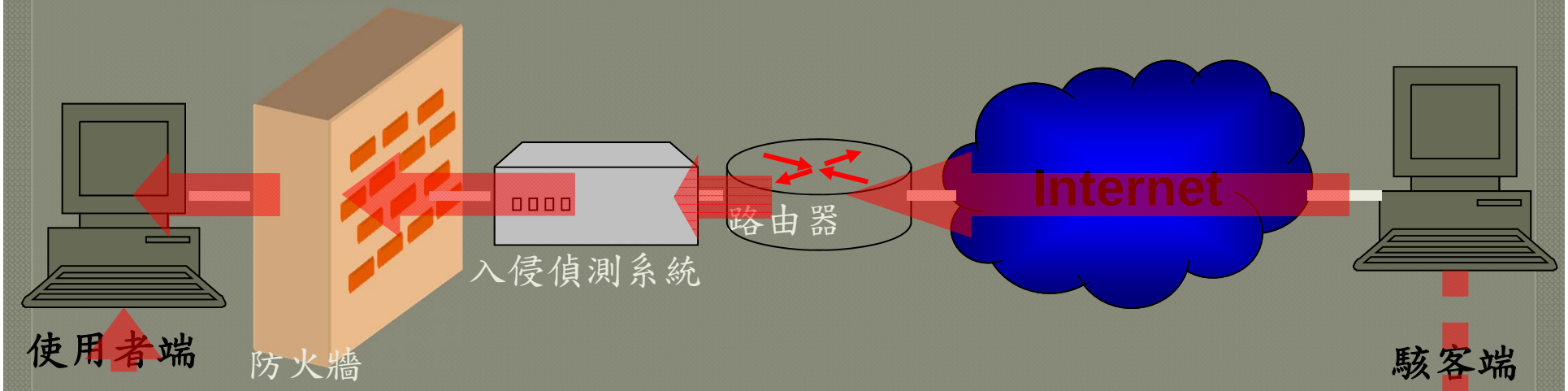
- 電子郵件社交工程
- OpenSSL漏洞(heartbleed)
- Windows XP停止支援因應
- 行動裝置小額詐騙因應

電子郵件社交工程

- 電子郵件社交工程簡介
- 惡意電子郵件特性
- 電子郵件社交工程郵件內容範例
- 本年實例
- 防範建議

電子郵件社交工程簡介

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法
- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)



1.駭客設計攻擊陷阱程式(如特殊word檔案或外部惡意連結。

2.將攻擊程式置入電子郵件中。

3.寄發電子郵件給特定(或不特定)目標。

4.受害者開啟電子郵件。

5.啟動駭客設計的陷阱，將被植入後門程式。

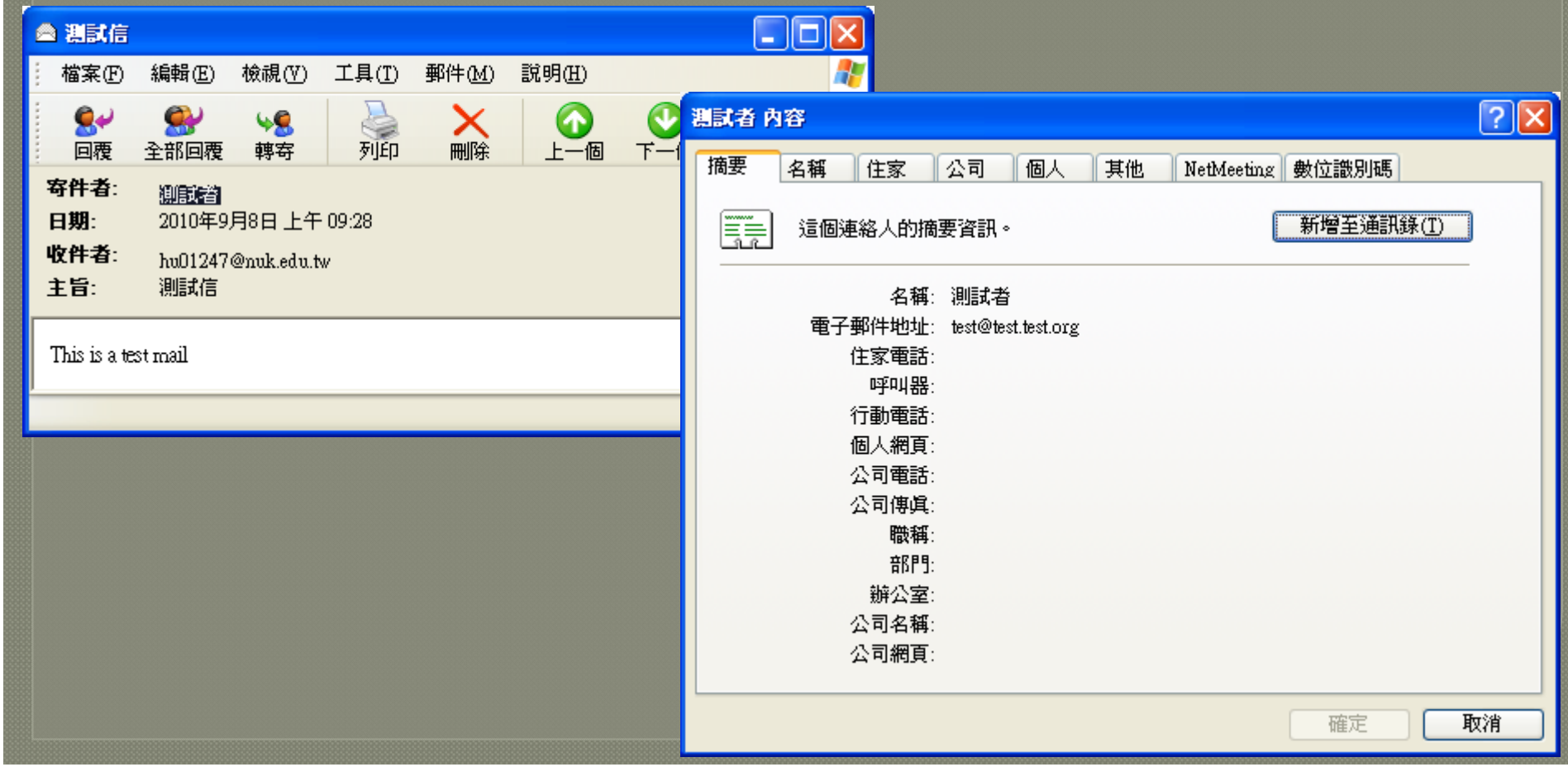
6.後門程式逆向連接，向遠端駭客報到。

惡意電子郵件特性

- 假冒寄件者
- 使用讓人感興趣的主題及內容
- 含有惡意程式的附件(或外部連結網址、圖)
- 利用零時差攻擊

特性一：假冒寄件者

- 駭客會假冒使用者信任的人，讓使用者相信電子郵件的內容，進而去開啟這些附件或超連結，並暗中啟動木馬程式。



特性二：使用讓人感興趣的主題及內容

- 駭客會使用收信者有興趣的主旨，甚至會配合目前最熱門的新聞事件，來吸引收信者開啟郵件
- 如教育部電子郵件社交工程演練的信件主旨
  - 帶鹹味的繽紛，探索克里米亞腐海之美
  - 鼎王認錯補償 打8折送鍋底
  - 「奈米」即將改變你的世界
  - 打造千頌伊美鼻 醫師：微整注射不宜超過2次
  - …

特性三：含有惡意程式附件

- 駭客在電子郵件附帶一個含有惡意程式的檔案，這個檔案不一定是執行檔，可能是各種類型的應用程式，甚至是壓縮檔。駭客會夾帶任何在應用程式上有弱點的文件檔案類型，並想辦法誘騙使用者開啟附件，藉以啟動安裝木馬程式。例如：
  - 含有惡意程式的影片檔（wmv）
  - 含有惡意程式的Office文件（doc）
  - 含有惡意程式的圖檔（jpg）
  - 含有惡意程式的壓縮檔（zip）

含有惡意程式之附件

- 附件檔案型態不一定是執行檔(.exe)，可能是各種類型的檔案(.doc、.ppt、.mdb等)，甚至是壓縮檔(.rar)
- .exe .com .scr
  .pif .bat .cmd
  .doc .xls .pps/ppt
  .reg .lnk .hta
  .zip .rar .swf
  .html .pdf .mdb

工學院某老師

- 釣魚信件騙取密碼

寄件者：supportt@nuk.edu.tw
主旨：重要提示：親愛的電子郵件帳戶的用戶
內容：
您的郵箱已超過管理員設置的默認存儲限制，
您目前正在運行的低，你可能無法發送或接收新郵件，
直到您重新驗證您的郵箱。
重新驗證您的郵箱，請點擊下面的鏈接，
並正確填寫所需的所有信息：
http://redcliffebedandbreakfast.com/wp-info/webmail.h
謝謝
系統管理員

駭客

利用盜取之帳號密碼

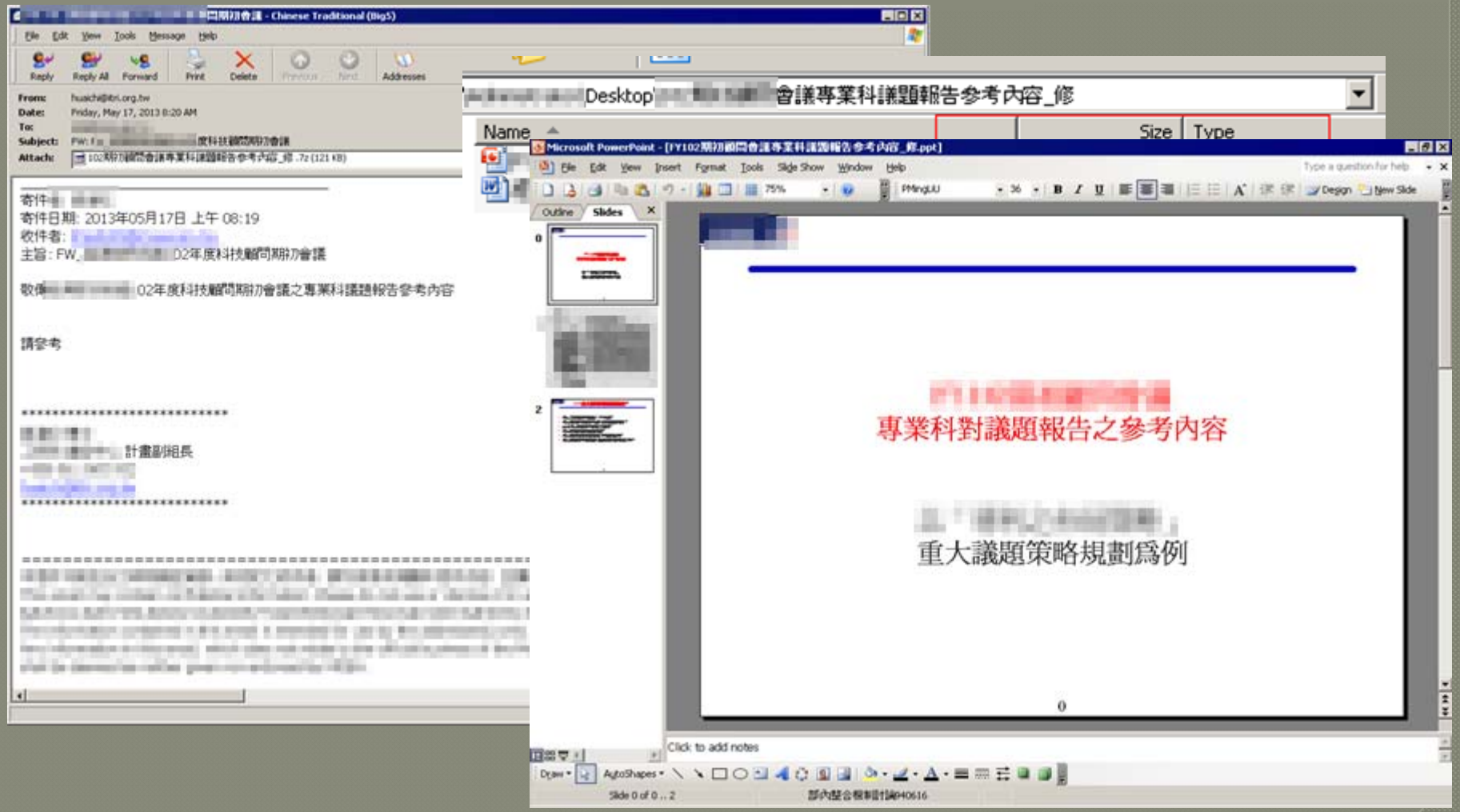
學校郵件主機
名譽評等降級
寄外信件遭退

請點擊”鏈接”

重新驗證畫面

帳號密碼取得

政府部門資安案例


Reply
Reply All
Forward
Print
Delete
Addresses
From:
Date: Friday, May 17, 2013 8:20 AM
To:
Subject:
Attach:
寄件日期: 2013年05月17日 上午 08:19
主旨: FW:
02年度科技顧問期初會議
02年度科技顧問期初會議之專業科議題報告參考內容
請參考
計畫副組長
Desktop
會議專業科議題報告參考內容_修
Name
Size
Type
Outline
Slides
專業科對議題報告之參考內容
重大議題策略規劃爲例
Click to add notes

防範建議

- 關閉預覽窗格
- 設定純文字讀取模式
- 避免開啟內容之超連結
- 確認信件來源
  - 不要開啟可疑電子郵件
    - 聳動的主旨、不正常的發信時間、陌生或少來往的對象、要求輸入機密資料
- 避免開啟可疑的附件檔案
  - Exe、dll、src、bat、pif、com、vbs…
- 避免開啟與公務無關的電子郵件
- 避免在不安全的網站留下個人資料

OpenSSL漏洞(heartbleed)

- Security Socket Layer (SSL)簡介
- HeartBleed弱點運作說明
- 防範建議

Security Socket Layer (SSL)簡介

Security Socket Layer (SSL)簡介

HeartBleed弱點運作說明

- OpenSSL於103/4/9公告存在高風險漏洞，編號為CVE-2014-0160。OpenSSL漏洞也稱為Heartbleed漏洞
- 攻擊者利用該漏洞無需通過權限或身份驗證，即可讀取伺服器記憶體， 竊取SSL 私密金鑰、Session Cookie、使用者帳號密碼等
- 攻擊者可對由OpenSSL 保護的網路通信進行解密、偽冒或進行中間人攻擊，竊取E-mail、文件及通訊內容等，導致伺服器遭到入侵而取得機敏資訊

防範建議

- 確認常用網站是否存有Heartbleed漏洞
  - –可利用簡易外部OpenSSL檢測工具確認網站是否具Heartbleed漏洞
    - Heartbleed-Ext (Firefox瀏覽器附加元件)
    - Chromebleed (Chrome 瀏覽器擴充套件)
- 變更常用網站帳號密碼
  - –先確認網站已無Heartbleed漏洞再變更帳密
- 瀏覽的網站如果存有Heartbleed漏洞
  - –通知管理者儘快修補漏洞
  - –儘速離開網站

Windows XP停止支援因應

- 事件說明
- 衝擊影響
- 建議作為

資料來源：國家資通安全會報技術服務中心

事件說明

- 微軟2001年推出Windows XP，雖然歷經Windows Vista、Windows 7到現在的Windows 8.1，至今仍為微軟公司使用期間最長的作業系統
- 自2008/6/30起停售XP後，隨著時間的演進，已進入產品生命週期末端，將於2014/4/8終止支援(End of Support，簡稱EOS)，不再針對XP提供下述支援服務：
  - – 安全性系統更新檔
  - – 非安全性系統更新檔
  - – 修補程式協議支援(付費服務)
  - – 按事件處理的付費支援服務
  - – 產品線上支援及線上技術內容更新服務

衝擊影響

- 1. XP作業系統相關應用軟體弱點已無法確保可取得更新的修補程式
  - –XP作業系統上所安裝之IE瀏覽器於2014/4/8後也將無法取得新的修補程式
  - –微軟應用程式開發與執行環境(runtime) 的支援平台也會調整(如.NET framework 與DirectX)，相對應在XP 上的安全性更新也不再支援
  - –微軟於5/1破例修補XP版IE漏洞(MS14-021)

衝擊影響

- 2. XP作業系統已發現弱點數量多，遭攻擊風險高
  - 根據CVE Details弱點資料庫統計數據顯示，XP作業系統
  - 已被發現弱點數量達721個，明顯高於Win7與Win8

衝擊影響

- 3. XP作業系統惡意程式感染率高
  - – 根據微軟第十五期資訊安全情報報告，平均每1000台XP電腦掃描結果含有惡意程式的電腦數量達9.1台(0.91%)，遠高於Win7與Win8
  - – 微軟可信賴運算部門總監Tim Rains表示，微軟停止支援XP更新修補程式後，惡意程式感染率預期大幅攀升至66%

建議作為

- 1. 加速XP升級至Windows新版作業系統
- 2. 強化XP電腦資安防護
  - –帳戶權限設定
  - –軟體防護
  - –監控防禦
- 3. 保留XP映像檔與使用還原卡
- 4. 透過網路區隔加強管理使用XP電腦

請參考103.4.18電子郵件：
[圖書資訊館]有關「微軟公司windows XP作業系統終止支援服務之相關資安因應防護措施」，請 查照。

行動裝置小額詐騙因應

- 手機小額詐騙手法分析與教戰守則懶人包
  www.cib.gov.tw/Upload/Files/5178.pdf

結語