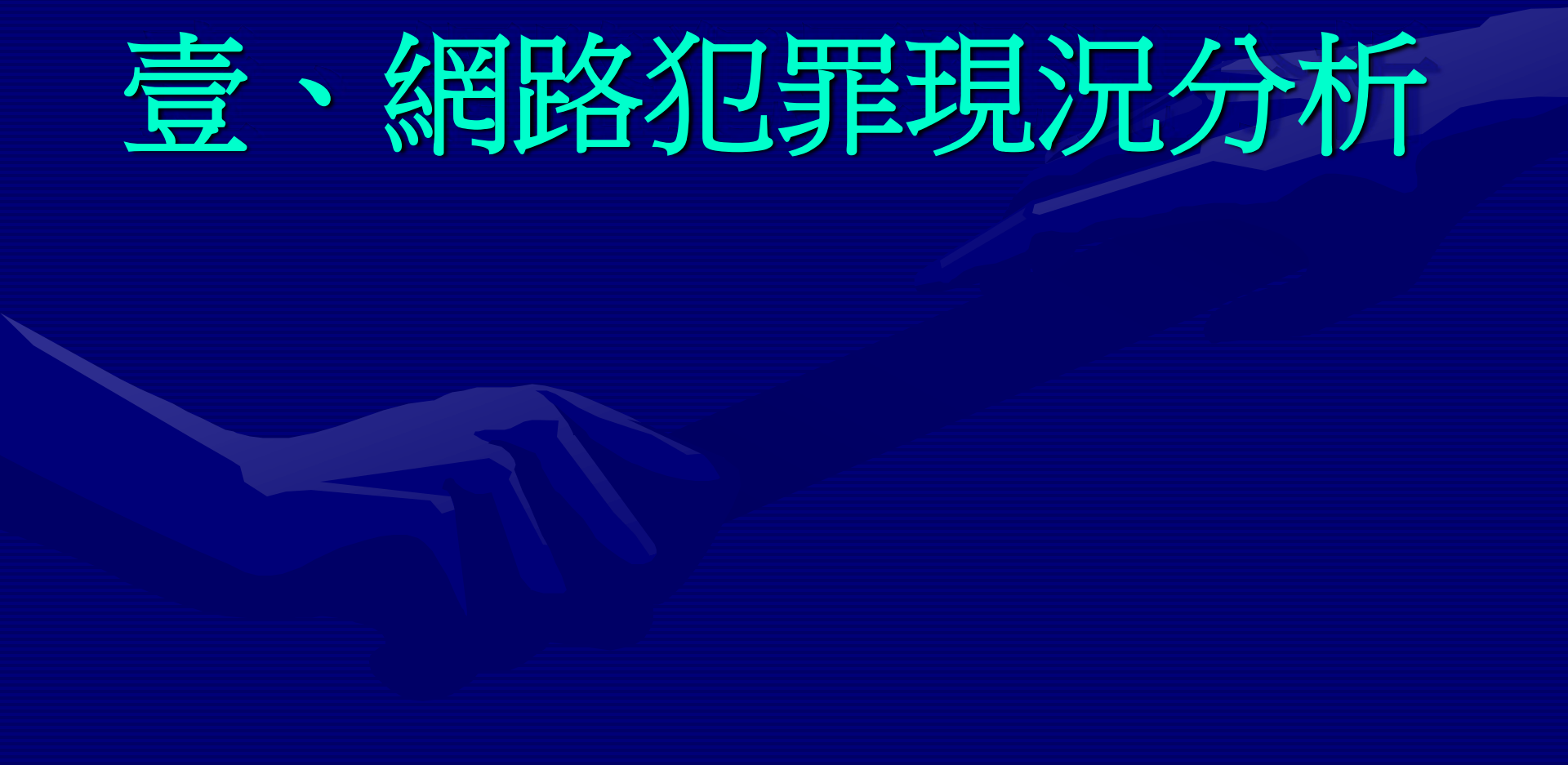


資訊風險 與 網路安全

單位：警政署資訊室
報告人：李相臣

壹、網路犯罪現況分析



- 兒少性交易案件近年來以大陸色情視訊集團以聊天室誘騙台灣被害人加入會員收費，開啟視訊功能互相觀看猥褻動作，並視身份進行恐嚇詐騙。
- 妨害電腦使用多為駭客入侵及線上遊戲犯罪案件，目前線上遊戲案件百分之五十為利用駭客手法進行盜取寶物、天幣等行為，儼然已為駭客練功戰場。

一、網路特性

◎無距離國界限制

◎極易隱匿、偽冒

◎系統漏洞層出不窮

◎科技發展迅速，功能眾多，技術規格不一，難以破解

二、困難

- 犯罪網址（網站、郵件、...）
設於國外
- 網咖或公共區域上網
- 業者未保留使用記錄
- 身份盜用或使用假資料
- 無線上網

貳、網路犯罪類型

架構



* 距離 台北=紐約=巴黎=高雄
路徑 台北 → 東京 → 紐約 → 巴黎 → 台北

功 能

1、WWW

(全球資訊網)

2、E-mail

(電子郵件)

3、BBS

(電子佈告欄)

4、ICQ

(線上交談)

5、NEWS

(新聞群組)

6、Telnet

(遠端登入)

7、FTP

(檔案傳送)

8、I-Phone

(網路電話)

9、Message

(網路簡訊)

⋮

網站

- 色情
- 盜版
- 偽（禁）藥
- 投顧
- 詐騙（假網站，
中獎）
- 超連結
- 惡意網站
- 情報傳遞
- 訊息交換
- 密語

BBS、NEWS

- 妨害名譽
- 援交
- 詐騙
- 販賣盜版工具軟體

E-MAIL

- 販賣違禁品
- 詐騙
- 網路釣魚（騙取資料）
- 惡意程式

P2P

- 交換違法檔案
- 惡意程式

VOIP

- 犯罪聯絡
- 詐騙

Telnet

- 遠端入侵

FTP

- 傳遞大量違法檔案

財	電話詐騙	人	MSN
	人性(貪念、恐懼)		人性(都會寂寞24hr)
	隨機		隨機
	無法查證		無法查證
	即時		即時
	取得信任		取得信任
	失財		失身

美國線上交友付費網路比率最高

Malicious code

- 竊取檔案（密碼）
- 刪改資料
- 遙控電腦
- 癱瘓電腦（恐嚇）
- 勒贖資料（電腦）



惡意(木馬)程式植入方式

一、駭客手法（SQL漏洞）

二、MSN、E-MAIL之傳遞

三、FTP之共享程式

四、P 2 P

五、瀏覽網頁

六、檔案分享

七、線上遊戲

電子商務詐欺

- 冒用帳戶
- 買空賣空
- 偽卡
- 哄抬價格
- 截標



僵尸電腦（Botnet、Zombie）

電腦遭控制被利用為跳板或攻擊他人之系統。由於傳輸封包極少，不易發現，本局正調查二起事件，已知被害電腦難以估計。



網路釣魚（Phishing）

偽冒他人電子郵件帳號或以網頁誘騙使用者開啟，以騙取帳號密碼或植入木馬。

打造線上交易安全從釣魚網站開始

原始	偽冒
MySpace	Myspacce
Icbc	1cbc
Paypal	Paypa1
網路釣客跳板	VOIP、簡訊



病毒(Virus)

◎刪除檔案

◎電腦當機



部落格 (BLOG、V-BLOG)

- 妨害名譽
- 傳遞情報
- 大陸緊縮部落格
- 藝人部落格真假難辨
- MIS對抗垃圾Blog

參、網路犯罪趨勢研析



1. Phishing 變化迅速

- 聳動主題
- 偽造寄件者
- 類似網址
- 假造URL

2. 無線上網難以追蹤

- 溢波盜用
- 攔截封包
- DOS
- 偽冒基地台

3. 跨國分工累犯增加
→ 大陸

4. 科技傳統犯罪結合
→ 駭客特質

5. 專業數位(電腦)鑑識工作
→ 保存現場

6.P2P應用擴增

SKype

◎P2P

◎寬頻

◎便宜

◎特殊壓縮封包

◎專門攻擊skype病毒出現

P2P 軟體可能影響網路安全的問題

- P2P工具包，可能被惡意人員放置木馬後門程式，與病毒蠕蟲。（日本真實案例）
- P2P軟體本身的漏洞，造成駭客入侵。
- 使用P2P軟體時，誤將本機目錄開放共享。
- 使用P2P下載影音檔案，多半為mp3與mpeg, avi等等檔案，可能造成侵權行為。
- 使用P2P下載色情影片，影響正常工作與政府形象。

防範P2P工具漏洞的注意事項

- 公務網路應嚴禁P2P軟體工具。
- 出差或返家，不應私人電腦下載P2P檔案。
- 下載任何工具軟體，要從原廠官方網站取得。
- 使用P2P工具，要縮短暴露在網際網路的時間。
- 使用任何網路工具(包括P2P檔案下載工具)，不應侵害他人權益，入侵他人電腦或是侵犯著作權。
- P2P技術是技術潮流，我們不是反對P2P發展，而是『反對在辦公室，使用P2P檔案下載』。

7.PROXY與大樓伺服器增加

→ 月租

8.BOTNET、SPAM

→ 跨國

9. Zero-day attack

2004年惡意程式17000

百分之55%木馬

漏洞	誘騙
NIMDA	NET Sky
SQL Slammer	My Doom
BLAST	BAGLE

10. VOIP

- 電信 + 網路 (電話VS電腦)
- 轉接

11. 手機惡意程式 (圖片、簡訊)

- 病毒 (當機)
- 木馬 (竊取資料)
- 傳聞大陸已破解Skype
(reverse engineer)

- 手機病毒

- 食人魚病蟲cabir

- 武士 CommWarrior

- 骷髏頭Skulls

已超過百種

- 手機o.s

- Symbian

- Window Mobile5.0

- Linux

12. 電腦資料勒索

→ 竊取

→ 刪除

→ 加密

13. 針對USB、磁片、光碟

→ 木馬出現

14. USB成最大傳播幫兇

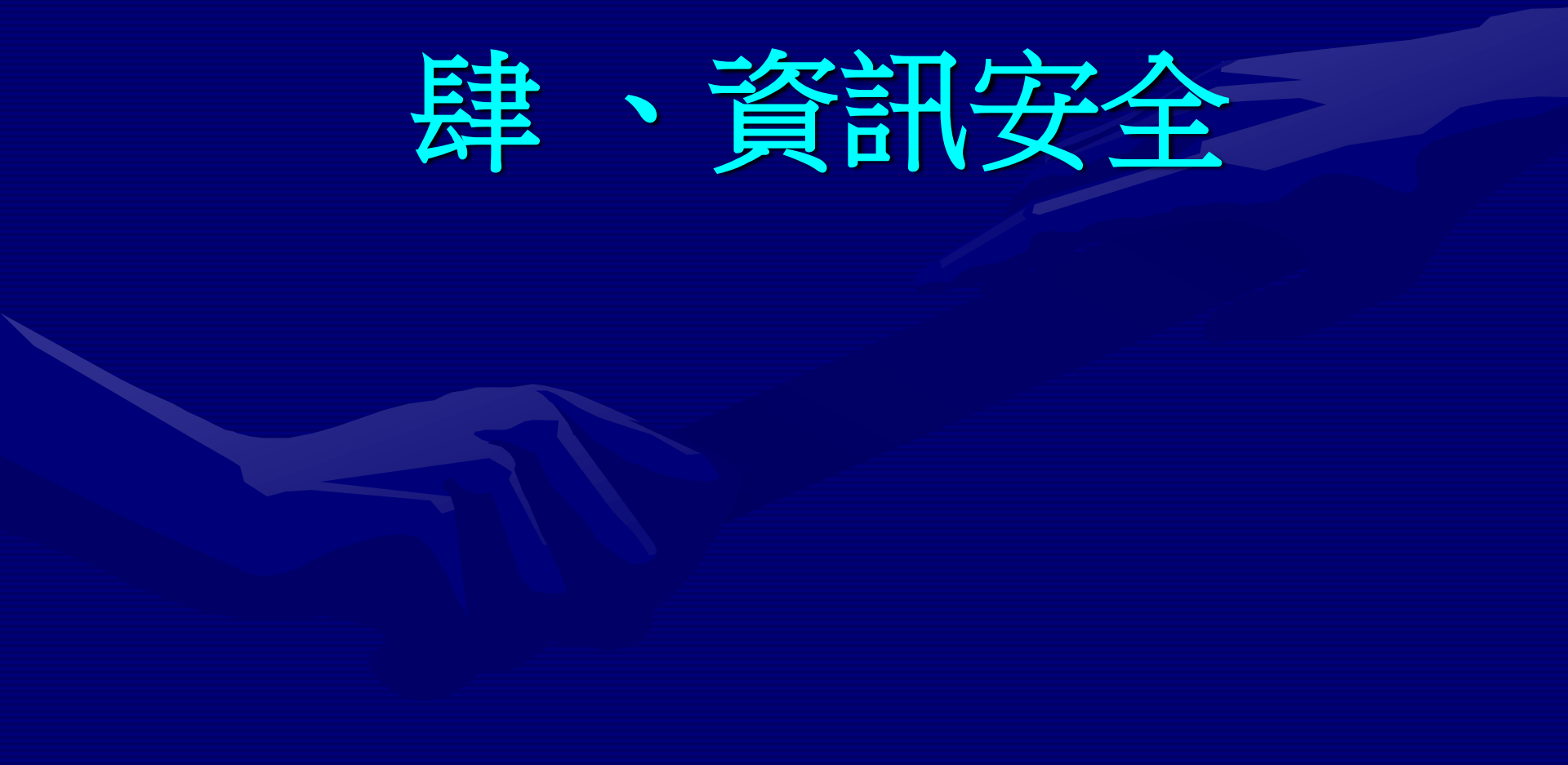
15.資料庫大量流失

- 民眾使用同一帳號密碼
- 外洩資訊整合交流
- 受害單位不願面對
- 駭客受僱或出賣資料

國內駭客團體增加，威脅資訊安全

Google進階功能即可發現有漏洞的網站

肆、資訊安全



主管（官）

- 1、查核資安計畫
- 2、支持有效資安預算
- 3、成立資安小組，定期召開會議

政風人員

- 1、會同資訊人員查核資安報表
- 2、熟悉資安硬體功能
 - * 防毒（駭）軟體
 - * 防火牆
 - * 各種稽核檔
 - * sniff
- 3、會同資訊人員查核電腦不當使用情形

資訊人員

- 1、建構資安軟、硬體防線
- 2、紀錄完整資安報表
- 3、建立警示檔
- 4、安裝”掃惡”軟體
- 5、分析封包
- 6、資安教育訓練

防火牆

- 通訊埠
- IP位址

入侵偵測

1、特徵比對

- * 後門
- * DDOS
- * 猜密碼
- * 惡意掃描
- * 溢位攻擊

2、通訊協定分析

- * 長度
- * 檔頭

3、行為模式

- * Database
- * learning

使用人員

- 1、節制功能
- 2、注意免費資訊
- 3、勿攜回家（檔案、電腦）
- 4、勿改設定
- 5、日日更新
- 6、更改密碼

作業規定

- 一、明訂保密協定與權利義務
- 二、隱私權之規定
- 三、密碼帳號使用管理
- 四、檔案使用管理
- 五、上線使用時間管理
- 六、使用權限管理
- 七、使用記錄安全管理
- 八、連線IP管理
- 九、修補程式管理

伍、案例檢討與建議

1. 植入木馬方式係以電子郵件聳動標題，誘騙使用人開啟。
2. 網路芳鄰未設密碼，擴散迅速。
3. 資訊室未發現連線 I P 異常，且未分析對外流量封包。
4. 未使用分段網路，致全單位均可能遭感染。
5. 未使用 V P N 阻擋對外異常連線。
6. 建置系統驗收後，應先將預設密碼刪除。
7. 使用者密碼應慎選，至少設定六位數以上，並避免僅使用英、數字。

8. 備份資料及備援系統之安全
9. 針對維護廠商與委外建檔公司加強防制作為
10. 應指定業務單位審核上網資料。
11. 避免「資訊拼圖」。
12. 應指派專人時時瞭解最新漏洞，並立即修補（每日工作）。
13. 網站主機應與內部資料庫切離，避免遭入侵。
14. 資訊人員考核亦須重視。

陸、網路安全概念

1. 防止惡意程式軟體已由套裝改成線上服務
(無版本之分)
2. 跨Window 及 Unix異質作業平台病毒出現
(Bi)
3. Window WGA偵測盜版軟體及Mac都有回
傳功能
4. Blue Pill 稱可躲過所有偵測軟體

5. PC或NB電腦遺失或遭竊損失很大
6. 軟體業者委託代工應注意植入木馬
7. 惡意程式，質降量增
8. IP Phone較一般電話更不安全，可入侵電腦故內容猶須加密。

9. 線上販售網路釣魚工具。

10. 3.5G(HSDPA，高速下行網路封包存取)可上網又使用Skype無法監聽。

11. 資訊管理

- 可否上網
- 上網行為
- 使用資訊內容

柒、資訊安全注意事項

一	慎灌軟體
二	慎用超連結
三	勿將公事檔案下載回家
四	注意防毒軟體更新
五	勿用通用密碼
六	使用U S B應注意安全

七	注意假網頁
八	慎點選廣告首頁
九	勿於非交易平台私下交易
十	晶片卡及自然人憑證移除
十一	勿存重要資料
十二	手機病毒防範
十三	P2P軟體很多被植入木馬
十四	時時自我檢測電腦

報告完畢
敬請指教

