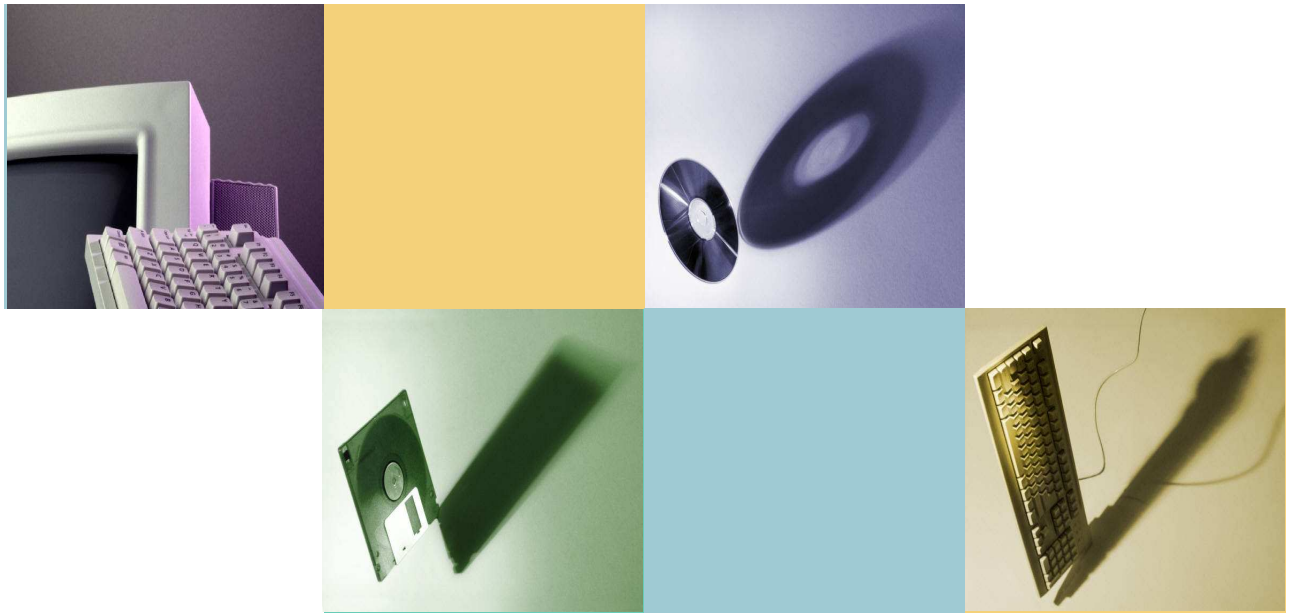
資安事件通報程序

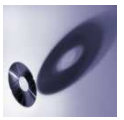
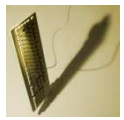


Wednesday, Jun 20 2012

曾國旭

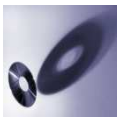
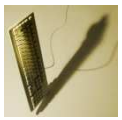
資安事件分級

- **依影響程度分成4個等級**，說明如下：
- 符合下列任一情形者，屬4級事件
  - 國家機密資料遭洩漏
  - 國家重要資訊基礎建設系統或資料遭竄改
  - 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作
- 符合下列任一情形者，屬3級事件
  - 密級或敏感公務資料遭洩漏
  - 核心業務系統或資料遭嚴重竄改
  - 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作

資安事件分級(續)

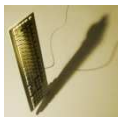
- 符合下列任一情形者，屬2級事件
  - 非屬密級或敏感之核心業務資料遭洩漏
  - 核心業務系統或資料遭輕微竄改
  - 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作
- 符合下列任一情形者，屬1級事件
  - 非核心業務資料遭洩漏
  - 非核心業務系統或資料遭竄改
  - 非核心業務運作遭影響或短暫停頓
- 資安事件於**發生後1小時內須通報**，**1、2 級事件需於72 小時內處理完成**並結案(包括通報與應變)，**3、4 級事件需於36 小時內完成**。

教育機構資安通報平台

⇨https://info.cert.tanet.edu.tw/

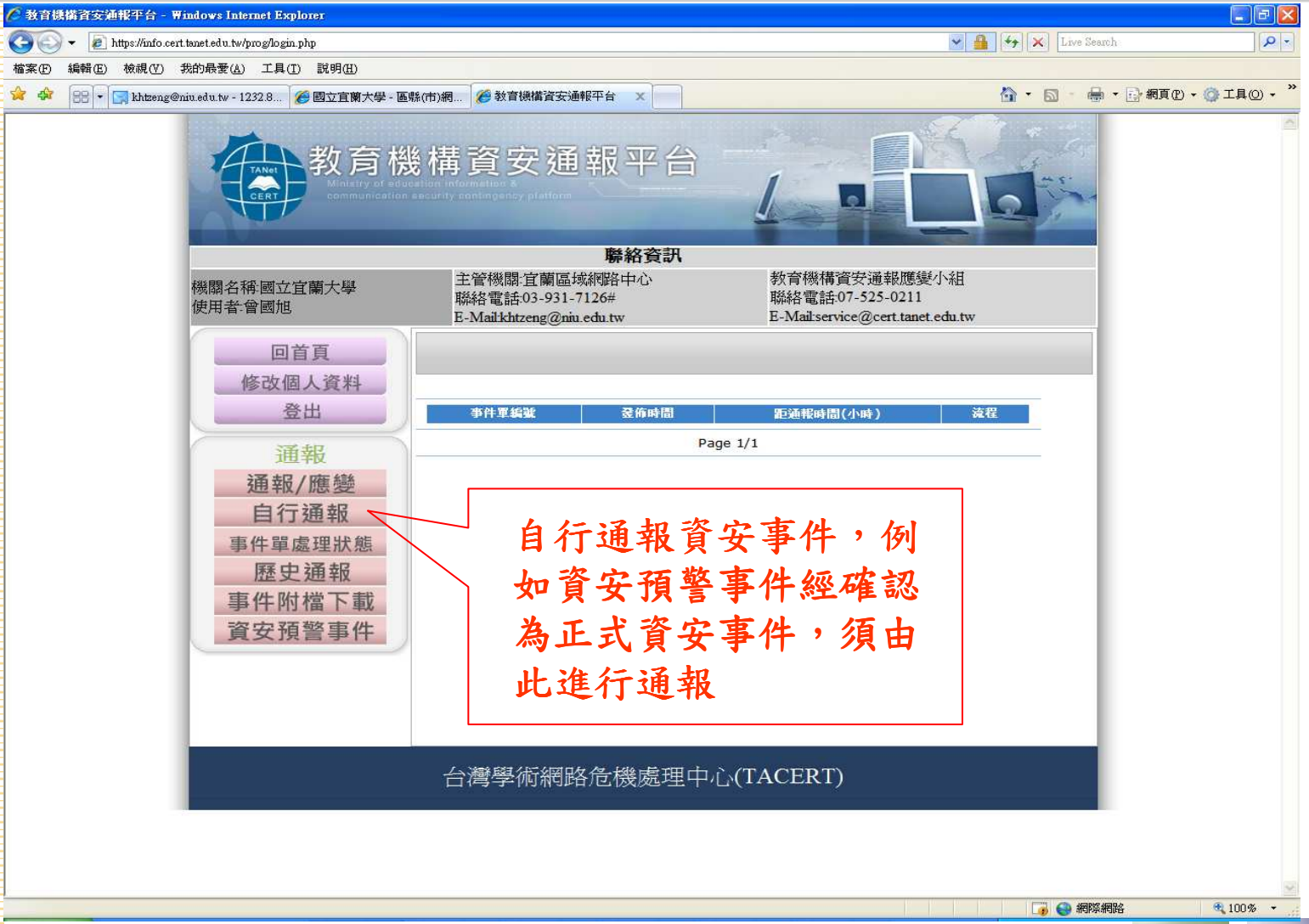




教育機構資安通報平台(續)

教育機構資安通報平台(續)

教育機構資安通報平台(續)



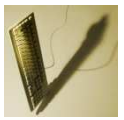
教育機構資安通報平台(續)

教育機構資安通報平台(續)

教育機構資安通報平台(續)

教育機構資安通報平台(續)





教育機構資安通報平台(續)

close or Esc Key

措施	2.利用工具程式於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。
參考資訊	本攻擊相關資訊可於下列網址 http://www.iss.net/security_center/reference/vuln/WINS_UDP_Pointer_Code_Exec.htm內查詢

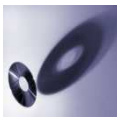
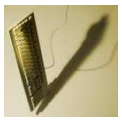
EWA事件單狀態

- ◉ 誤判
- ○ 確實事件　　事件單編號
- ○ 無法判斷

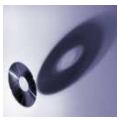
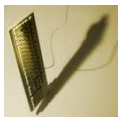
原因

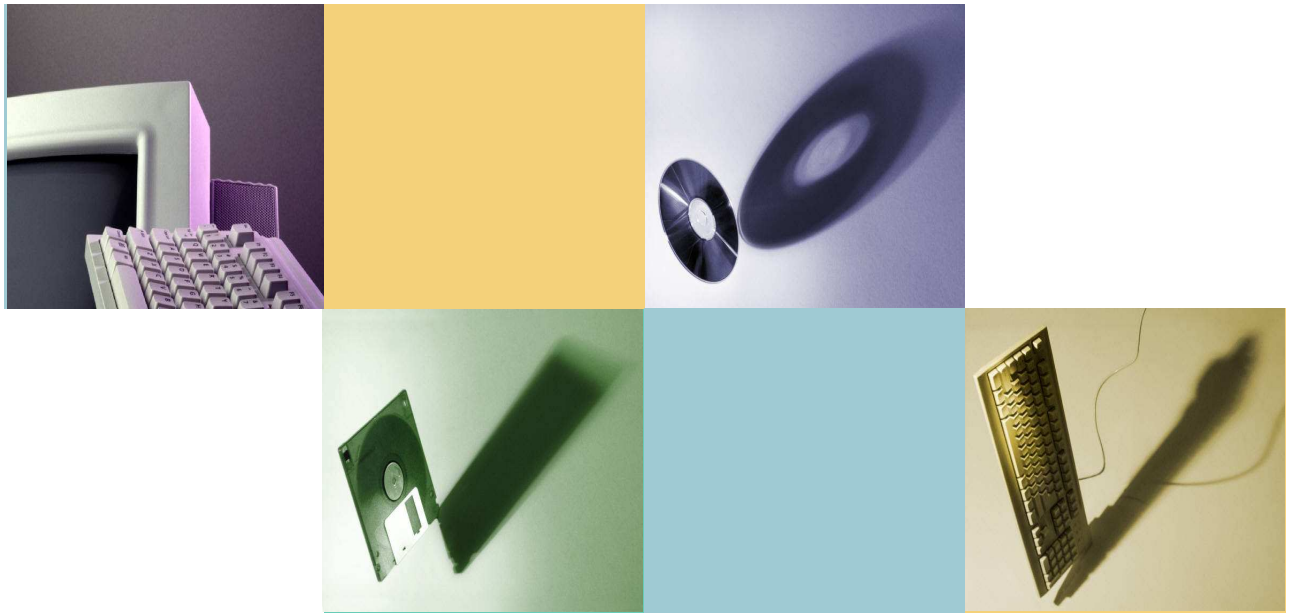
經比對防火牆紀錄，乃是使用teamviewer軟體，並非攻擊事件

送出

Q and A



THANKS !