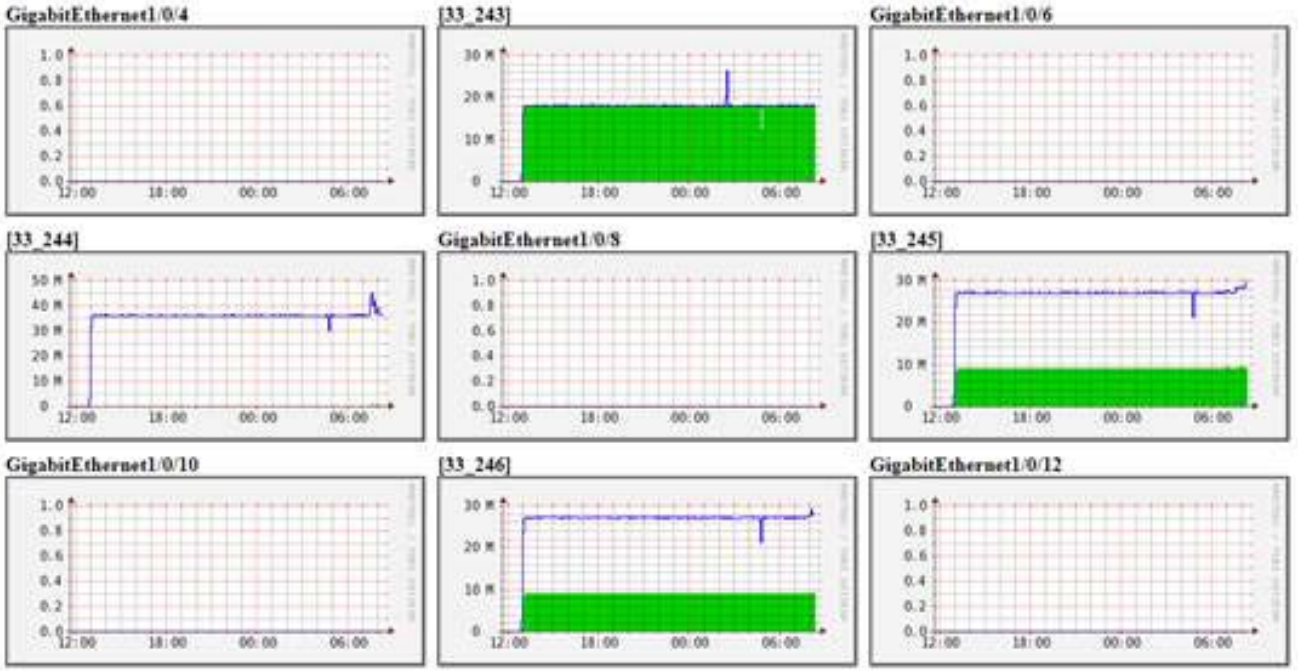
資訊處
National Chung Cheng University
Office of Information Technology

資安事件宣導

無線網路基地台(Wifi AP)攻擊

實際案例分享

- 三月底校內有兩個單位，因自行架設的 Wifi AP 遭受攻擊，大量發送封包，致使整個單位的網路癱瘓，是屬於服務阻斷攻擊的一種。



解決方法

- 將韌體更新至最新版本
  - 無線網路設備應該定期將韌體更新至最新版本，以維持較佳之性能及安全性。
  - 本案例兩個單位所使用的無線網路設備均為同款的D-Link DIR-809，經更新韌體至最新版仍無效。
- 更換無線網路設備
  - 較老舊或安全性不佳的設備，若已更新至最新韌體版本仍無法解決，則應考慮更換較新且安全性較佳之產品。
  - 本案例兩個單位更換無線網路設備後問題已解決。

注意事項

- 有心人士在一定距離內，就可以很容易的對無線網路進行封包的發送或攔截，因此在資安的防護上應該要更加小心，例如：
  - 定期將無線網路設備的韌體更新至最新版本。
  - 管理者密碼一定要更換，切勿使用預設密碼。
  - 加強防火牆設定，只允許相關人員使用。
  - 使用加密的傳輸協定，例如WPA2。
  - 經常檢查所屬區域範圍是否有可疑的 Wifi AP，並予以移除。

資料參考

- 無線網路傳輸風險
  http://download.icst.org.tw/attachfilearticles/無線網路傳輸風險.pdf
- 無線網路安全簡介
  http://www.cc.ntu.edu.tw/chinese/epaper/0003/20071220_3006.htm
- 避免家用Wi-Fi路由器遭駭，你該知道的大小事
  https://www.ithome.com.tw/news/112668