111年度農田水利灌溉管理資訊化推廣與座談

資通安全通報態樣及因應措施

講師：Antonio

個人簡歷

- 專業證照：
  - CEH（Certificated Ethical Hacker）駭客技術專家
  - ISO27001:2013主導稽核員
  - ISO27701個資主導稽核員
- 經歷：
  - 行政院/教育部資安稽核員
  - 台中科技大學-資工系 兼任助理教授
  - 台中教育大學-資統所 兼任助理教授
  - 靜宜大學-國企所 兼任助理教授
  - 工研院/中衛發展中心 工程師/資訊顧問
- 專長：
  - 資訊安全架構認證導入與輔導
  - 資訊安全稽核員
  - 資訊安全教育訓練課程講師

大綱

一. 最近資安入侵攻擊彙整
二. 資通安全通報樣態及因應措施
三. 資訊安全新威脅
四. 安全防護面面觀

8月初網路攻擊樣態

- DDos
- 內容置換
- 網頁內容置換

DDos攻擊

定義DDos攻擊

當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，稱為分散式阻斷服務攻擊（distributed denial-of-service attack，簡稱DDoS攻擊）亦稱洪水攻擊。

DDos攻擊症狀包括：

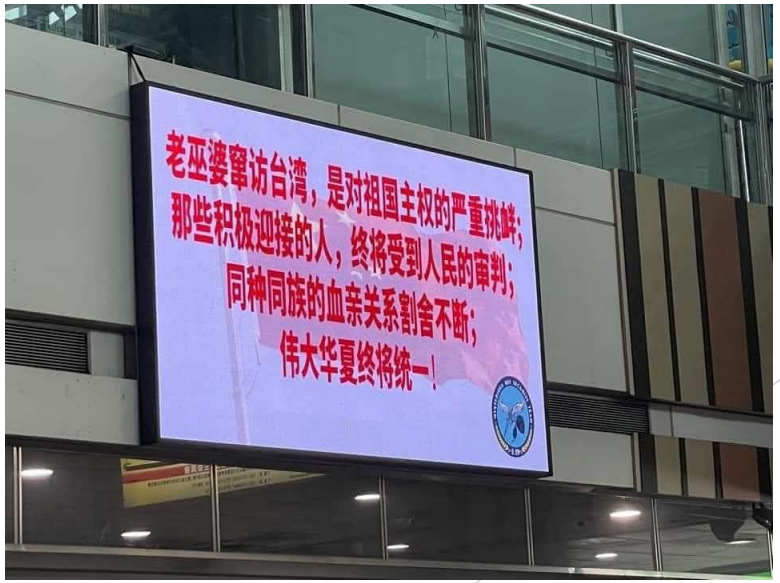
- 網路異常緩慢（打開檔案或存取網站）
- 特定網站無法存取
- 無法存取任何網站
- 垃圾郵件的數量急劇增加[4]
- 無線或有線網路連接異常斷開
- 長時間嘗試存取網站或任何網際網路服務時被拒絕
- 伺服器容易斷線、卡頓、存取延遲

8月初網路攻擊樣態-DDos攻擊

- 總統府證實網站遭DDoS攻擊，疑與美國眾議院議長裴洛西訪臺有關
  - 總統府發言人 張惇涵 8/2晚間表示，當日下午約17:15分起，總統府官網遭受境外DDoS攻擊，攻擊流量為平日的200倍，導致官網一度無法顯示。但經總統府處置後，已於20分鐘內恢復正常運作。張惇涵表示，面對境外勢力持續的複合式資訊作戰，政府各機關會持續加強監控，維護國家資通訊安全，以及各關鍵基礎設施穩定運作。
- 政府入口網站、外交部、國防部與桃園機場網站傳出因遭到DDoS攻擊而無法存取，外交部指出網站收到每分鐘多達850萬次請求
- 行政院政務委員唐鳳表示，8月3日攻擊流量逾15 TB、最高流量為過往的23倍
  - 8月2日至3日間，.tw國家頂級網域DNS最大查詢量每秒約8萬5千餘筆，其中近75% 訊務量為惡意攻擊封包，這些IP位址持有者主要來自美國與中國雲端業者，其中美國雲端業者佔比54.8%，中國業者佔比44.2%。

8月初網路攻擊樣態-內容置換

- 7-11櫃臺後方數位看板的內容遭置換，刑事局調查指出是遭駭客入侵
- 臺鐵新左營車站電子看板疑遭駭客入侵，出現簡體中文恐嚇訊息
  - 從廣告生態系來看，應與超商合作的聯播廣告商其檔案內容被置換，或是數位電子看板的內容管理伺服器（CMR）主機遭入侵？



8月初網路攻擊樣態-網頁內容置換

- 高雄市環保局飲用水網站被置換五星旗
- 臺灣大學部分網頁遭到竄改，圖片皆變為「世界上只有一個中國」的恐嚇訊息
  - 高雄市環保局官網網站被駭13個小時遲遲無法恢復？該單位反映這個網頁是以開放原始碼來操作，開發公司正在了解程式漏洞…

資通安全通報樣態及因應措施

資通安全事件分級

- 依據資通安全事件通報及應變辦法(https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030305)
- 資通安全事件分為四級

第一級

一、非核心業務資訊遭輕微洩漏。
二、非核心業務資訊或非核心資通系統遭輕微竄改。
三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

資通安全事件分級

第二級

一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。
二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。
三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

資通安全事件分級

第三級

一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

資通安全事件分級

第四級

一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。
二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。
三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

資通安全通報分級

<table>
<tr><th colspan="3">判斷因素</th><th>第一級</th><th colspan="3">第二級</th><th colspan="4">第三級</th><th colspan="2">第四級</th></tr>
<tr><td colspan="3">資訊洩漏(機密性)</td><td>非核心業務</td><td colspan="3">•核心業務
•關鍵基礎設施非核心業務</td><td colspan="4">•一般公務機密
•敏感資訊
•關鍵基礎設施核心業務</td><td colspan="2">國家機密</td></tr>
<tr><td rowspan="4">資訊/資通系統遭竄改狀況(完整性)</td><td rowspan="2">資訊竄改</td><td>資訊別</td><td>非核心業務</td><td>非核心業務</td><td>核心業務</td><td>關鍵基礎設施非核心業務</td><td>核心業務</td><td>•一般公務機密
•敏感資訊</td><td colspan="2">關鍵基礎設施</td><td>關鍵基礎設施核心業務</td><td>國家機密</td></tr>
<tr><td>嚴重程度</td><td>輕微</td><td>嚴重</td><td>輕微</td><td>輕微</td><td>嚴重</td><td>—</td><td>嚴重</td><td>輕微</td><td>嚴重</td><td>—</td></tr>
<tr><td rowspan="2">系統竄改</td><td>資通系統別</td><td>非核心</td><td>非核心</td><td>核心</td><td>處理關鍵基礎設施非核心業務</td><td colspan="2">核心</td><td colspan="2">處理關鍵基礎設施</td><td colspan="2">處理關鍵基礎設施核心業務</td></tr>
<tr><td>嚴重程度</td><td>輕微</td><td>嚴重</td><td>輕微</td><td>輕微</td><td colspan="2">嚴重</td><td>嚴重</td><td>輕微</td><td colspan="2">嚴重</td></tr>
<tr><td rowspan="2">受影響於容忍時間回復與否(可用性)</td><td colspan="2">業務/資通系統別</td><td>非核心</td><td>非核心</td><td>核心</td><td>關鍵基礎設施非核心業務</td><td colspan="2">核心</td><td colspan="2">關鍵基礎設施</td><td colspan="2">關鍵基礎設施核心業務</td></tr>
<tr><td colspan="2">可否回復</td><td>可</td><td>否</td><td>可</td><td>可</td><td colspan="2">否</td><td>否</td><td>可</td><td colspan="2">否</td></tr>
</table>

資安攻擊樣態

一.網頁攻擊

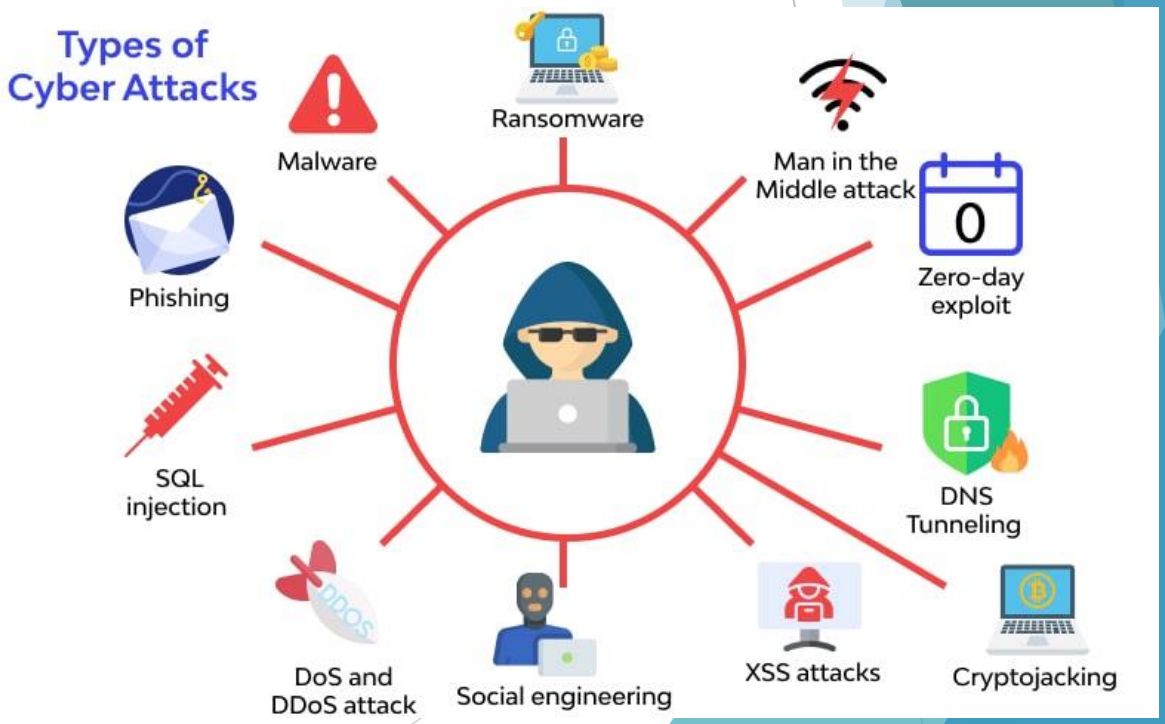
二.非法入侵

三.阻斷服務

四.設備問題

攻擊樣態-網頁攻擊

- 網頁置換
- 惡意留言
- 惡意網頁
- 釣魚網頁
- 網頁木馬
- 網站個資外洩

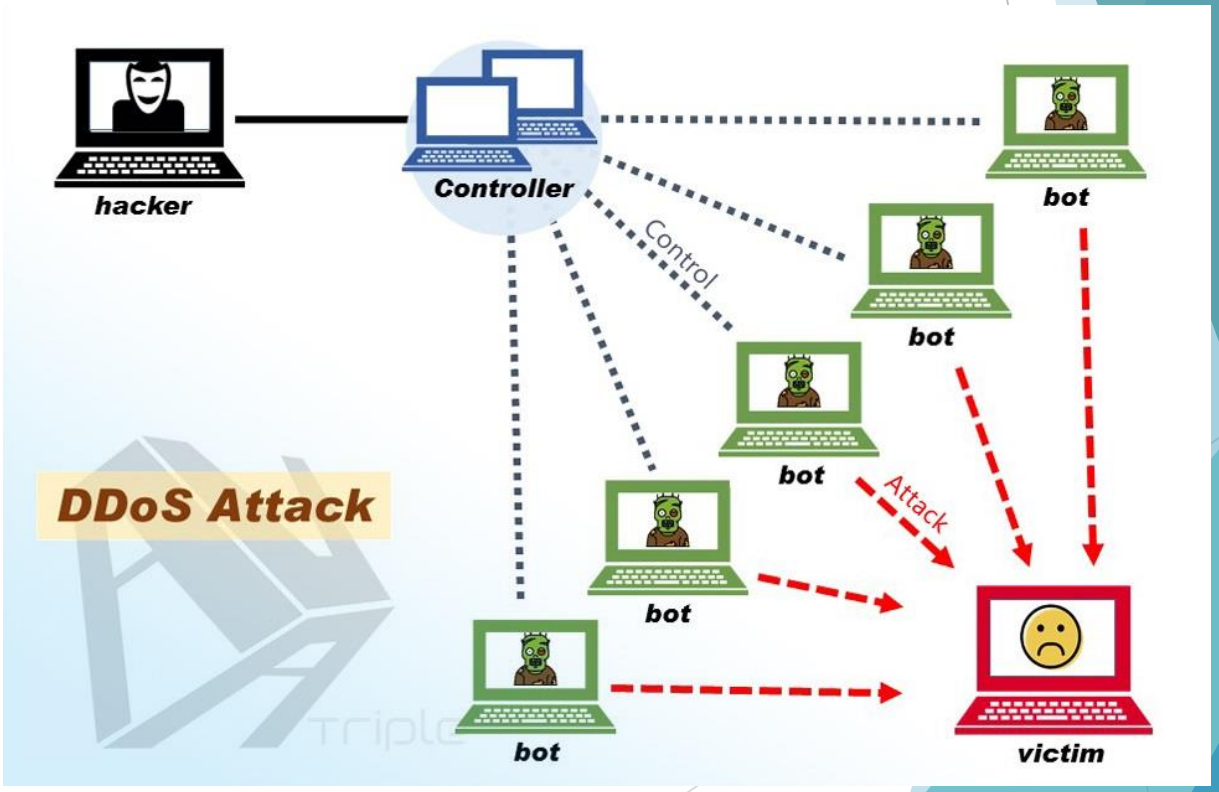


攻擊樣態-非法入侵

- 系統遭入侵
- 植入惡意程式
- 異常連線
- 發送垃圾郵件
- 資料外洩

攻擊樣態-阻斷服務(DoS/DDoS)

- 服務中斷
- 效能降低



攻擊樣態-設備問題

- 設備故障/毀損
- 電力異常
- 網路服務中斷
- 設備遺失

資安與我
資安新知

世界經濟論壇2022年全球風險調查報告

- 數位依賴與網路脆弱性
- 四大研究成果
  - ✓2020年全球勒索軟體案件數成長435%。
  - ✓全球尚缺乏300萬名專業網路人才。
  - ✓預估全球數位商務總產值至2024年將成長8,000億美元。
  - ✓95%網路安全事件可歸因於人為失誤。

資訊來源：https://blog.twnic.tw/2022/02/16/21661/

【資安週報】

從國際整體的資安態勢而言，勒索軟體駭客組織Conti疑似另起爐灶的情形，引起研究人員的注意；而在國內的資安新聞裡，上市櫃公司為了尋求資安長之間彼此互通有無，特別組成了聯盟來交流相關經驗

- 從烏克蘭戰爭開戰至今，俄羅斯駭客已攻擊烏克蘭237次
- WordPress網站再度成為駭客攻擊烏克蘭的工具，被用於感染用戶電腦發動DDoS攻擊
- 駭客組織聲稱入侵可口可樂，竊得161 GB資料
- 駭客發動大規模的HTTPS加密流量DDoS攻擊

資訊來源：https://www.ithome.com.tw/news/150703

元大統一證資安事件！
交易密碼勿與網購相同

- 針對元大證券及統一證券複委託系統出現下單異常事件，券商公會理事長賀鳴琦表示，券商外部下單系統資安水準要加強，同時呼籲投資人網購密碼不能與金融交易相關密碼共用，避免遭有心人士利用。
- 新聞連結： https://udn.com/news/story/7251/5919636

駭客攻擊過去與現在

過去	現在
毀損資料	竊取個人隱私
惡作劇	竊取組織資訊
癱瘓個人電腦	加密個人資料勒索
癱瘓內部網路	以個人電腦做為跳板
	以個人電腦作為殭屍電腦
	癱瘓外部網路

常見的社交工程手法

social engineering

社交工程與人性

- 社交工程是一種操控人性的技巧
- 利用人類的好奇心、同情心等天性，在警覺降低時中了駭客的圈套，洩漏了讓駭客進行下一波攻擊的資訊
- 垃圾郵件-經常隱藏著社交工程的誘餌
- 人性常是整個資安防護體系中最脆弱的環節

社交工程(social engineering)?

- 社交工程也本質上就是一種詐騙的技術一樣，是利用社會互動來誘使某人犯安全錯誤的黑色藝術。
- 社交工程攻擊的目的是通過操縱即將成為受害者的人來洩露安全訊息（例如用戶名，密碼或信用卡信息），從而繞過安全性障礙（密碼，處理程序，上鎖的門等），從而提供對上鎖的訪問權限 工具或在網絡或設備上安裝惡意軟件。一個執行得當的社交工程攻擊將在沒有受害者甚至不知道實際發生的情況下結束。

社交工程-釣魚(fishing)

- 網絡釣魚是一種最常見的社交工程攻擊形式，是一種欺詐性電子郵件或網站，誘使人們洩露私人信息（用戶名，密碼，信用卡信息等）或下載惡意軟件。
- 成功的網絡釣魚電子郵件依賴於恐懼策略，例如：來自您的銀行或其他金融機構的緊急電子郵件，“太過令人無法接受真正的交易”，例如提供廉價或難找產品的提議，或者您對雇主的責任感。 數據竊賊將冒充您的老闆或公司中的其他高層人物。 網絡釣魚的目的是使受害者在看起來與真實物品幾乎相同的虛假登錄頁面上輸入密碼或用戶名，或將惡意軟體下載到其設備上。

時事議題引誘

最近有駭客假借世界衛生組織（WHO）的名義寄出釣魚郵件,WHO呼籲:只有@who.int 才是來自世衛的信件 😳

其他如 @who. com 、@who. org 等其他網域，是網路釣魚,可能會被竊取個資或安裝惡意程式

Reference:
https://www.facebook.com/trendmicrotaiwan/photos/a.313734055131/10157840317870132/?type=3

網路釣魚進化成 AI 語音釣魚,偽裝老闆聲音騙走 770 萬台幣!

- 《華爾街日報》報導，新型的詐騙透過 AI 合成的語音，一家英國能源公司主管以為接到德國總公司執行長來電， 因為對方操著德國口音，語調也跟他熟悉的德國總公司 CEO 幾乎一樣，因此不疑有他，就把款項轉了過去, 被騙走了 22 萬歐元（近台幣 770 萬元） 。
- 史丹佛大學、普林斯頓等大學發表了一項研究，新技術已經發展到可以任意篡改編輯影片人物講話的嘴型和語音，甚至有 59.6% 的受試者看不出被修改過的影片。 聲音影像也可像文字一樣簡單的從中間修改,對一些影音工作者的確是個好消息 但如果遭不法份子利用,可能會這比語音釣魚(Voice phishing)更容易掉入陷阱 。

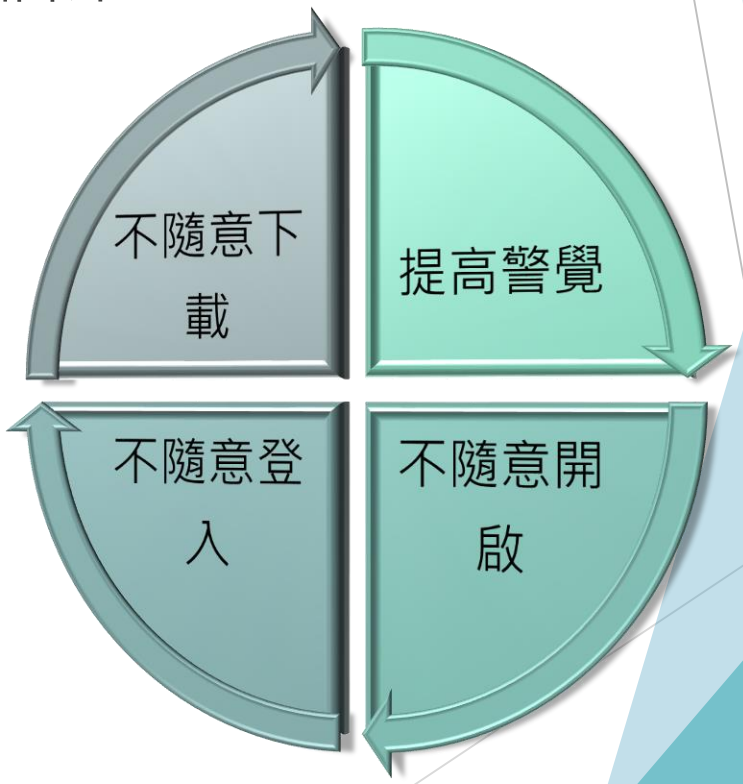
參考連結：
https://www.youtube.com/watch?v=0ybLCfVeFL4&feature=emb_logo

社交工程的基本防護

- 執行各種作業系統、應用軟體的更新及設定。
- 必須安裝防毒軟體，並確實更新病毒碼。
- 密碼設定要符合複雜度的要求。
- 不要輕易相信電話中任何非經正式授權的請求。
- 不要任意安裝未經授權的軟體。
- 小心釣魚網站、詐騙廣告的陷阱。
- 不使用公務信箱作為登入的帳號。
- 不於社群網路中談論有關公務之相關內容。
- 修改個人資料的隱私設定(提供最少個資為宜)。
- 不要輕易點選陌生的加好友請求。
- 不任意點選社群網路聊天室或電子郵件的連結。

防治社交工程的方法

- 隨時提高警覺不未經確認及提供資料
- 不開啟來路不明的電子郵件及附加檔案
- 不連結及登入未經確認的網站
- 不下載非法軟體及檔案



電子郵件使用者習慣

- 密碼記得定期更新
- 不要回覆垃圾郵件
- 定期管理郵件過濾黑白名單
- 轉寄信件前影刪除原寄件人資料
- 多收件人，請盡量使用密件副本傳送
- 重要郵件內文/副檔影加密
- 收信時，盡可能以純文字方式閱讀
- 閱信時須限制直接下載圖片

Q&A