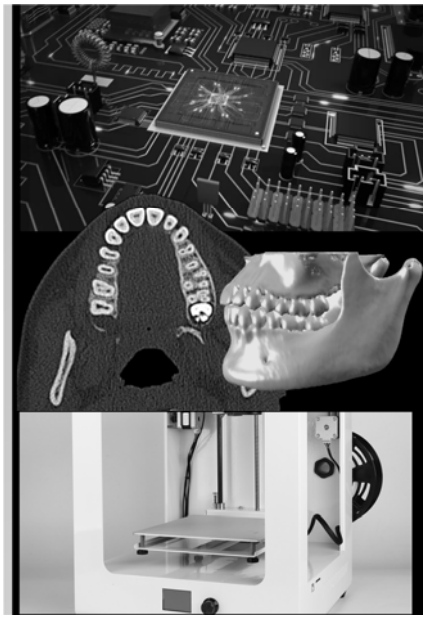
計算機概論
SECURITY OF COMPUTERS

盧家鋒 副教授

國立陽明大學生物醫學影像暨放射科學系
分機 7308

alvin4016@ym.edu.tw



實用技巧

- 資訊安全簡介
- 電腦病毒
- 個人資訊安全措施

課程教學影片與講義
http://www.ym.edu.tw/~cflu/CFLu_course_CompSci.html

資訊安全簡介

資訊安全簡介

實體安全

- 硬體建築物與週遭環境的安全與管制，網路線路或電源線路的適當維護

資料安全

- 確保資料的完整性與私密性，並預防非法入侵者的破壞，例如不定期做硬碟中的資料備份動作

程式安全

- 維護軟體開發的效能、品管、除錯與合法性。例如提升程式寫作品質

系統安全

- 維護電腦與網路的正常運作，例如對使用者宣導及教育訓練

常見資訊安全問題

- 個人私密資料的監視與濫用
  - 網站使用Cookie小型文字檔，追蹤使用者行為的方式
  - 網站經營者用來瞭解造訪次數、瀏覽過網頁、購買過商品等使用者行為
- 網路釣魚
  - 利用偽造電子郵件與網站作為「誘餌」，洩漏私人資料、植入病毒、系統毀損或機敏資訊被竊
- 網路竊聽
  - 不正當擷取網路上的封包進行竊聽分析
- 駭客攻擊
  - 癱瘓服務攻擊、郵件炸彈程式、伺服器漏洞、特洛伊式木馬

資訊安全的本質

覆巢之下無完卵

- 整體資訊安全是建構於一系列環環相扣的保護機制下。
- 攻擊或破壞者只要找出其中最弱的一環，就可以完全瓦解整個保護機制。

電腦病毒

病毒類型、過往案例

電腦病毒簡介

- 特殊電腦程式，常會附著在一些可執行檔案中，待電腦使用者執行檔案後，進駐到開機磁區或記憶體中，並透過複製或覆寫的感染方式，破壞電腦系統或檔案。
- 大多數電腦病毒都具有強大的自我複製繁殖能力，以傳染給其他程式或電腦（佔用記憶體或磁碟空間）。
- 傳染媒介：隨身碟、光碟片、email、網路。

電腦病毒類型

最常見的三大類型

- 木馬/殭屍網路（特洛伊木馬病毒）：45%
  - 在電腦中開啟後門，使控制者得以遠端操縱，藉以竊取帳密、資料甚至使用網路攝影機。
  - 被感染電腦成為控制者之殭屍網路，傳送大量偽造或垃圾封包癱瘓攻擊目標。
- 蠕蟲病毒：25%
  - 可自我複製的程式，會執行垃圾程式碼以發動分散式阻斷服務攻擊，令電腦的執行效率極大程度降低，影響電腦與網路正常使用。
- 指令碼/巨集病毒：15%

電腦中毒徵兆

- 執行速度比平常慢
- 磁碟或磁碟機無法存取
- 顯示不尋常的錯誤訊息
- 執行檔或其他檔案的檔案大小突然無故變大或日期無故改變了。
- 硬碟或記憶體的可用空間無故縮小。
- 不斷的當機或重新啟動

建議以防毒軟體進行掃描！

2005-2017年勒索病毒

趨勢科技資安趨勢部落格 2018.10.3
https://blog.trendmicro.com.tw/?p=57054

- 勒索病毒: Ransomware，檔案加密並要求支付贖金。
- 「你們的檔案都已被我加密，如果真的在乎這些數據，那麼建議你們別浪費寶貴時間，尋找不存在的解決方案」。
- 2015 年FBI:「建議受害人付款了事」引起爭議...

勒索病毒不斷挑戰執法單位

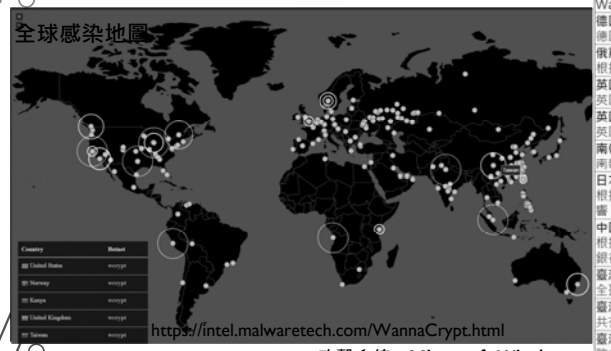
- 麻薩諸塞州 Swansea警察局在2013年支付了750美元贖金
- 伊利諾州 Midlothian警察局2015年支付了500美元
- 田納西州迪克森郡(Dickson County)治安官辦公室2015年支付了572美元。
- 美國緬因州林肯郡 (Lincoln County) 警長辦公室及四個鄉鎮派出所，2015年支付大約 300 美元的贖金。
- 阿拉巴馬州柯林斯維爾(Collinsville) *警察*局在 2015 年6 月被襲，，導致罪犯照片資料庫被加密鎖定。駭客要求500美元贖金，但這家小鎮警局拒絕支付，而是放棄被綁架的檔案資料。

2017年WANNACRY/WCRY USD300

- 第一隻結合蠕蟲擴散行為大規模擴散、遂勒索之利的勒索蠕蟲
- 用.WNCRY副檔名來對檔案進行加密，被針對的副檔名共有176種，包括Microsoft Office、資料庫、壓縮檔、多媒體檔案和各種程式語言常用的副檔名

2017年WANNACRY/WCRY

源自網路釣魚誘使使用者從Dropbox網址下載惡意程式



攻擊系統：Microsoft Windows

法國雷諾汽車（Renault）
雷諾在法國北部Sandouville的工廠，專門記錄員工生產狀況的電子版出現WannaCry勒索訊息。

德國鐵路（Deutsche Bahn）
德國鐵路車站內的電子看板遭WannaCry勒索攻擊，鐵路運行未受到影響。

俄羅斯內政部統計
根據內政部發言人表示，俄羅斯內政部約1千臺電腦受WannaCry攻擊。

英國國民保健署NHS
英國NHS旗下有16家醫院，45臺設備遭WannaCry攻擊，部分手術被迫取消。

英國日產汽車（Nissan）
英國Nissan位在Sunderland的汽車工廠，內部電腦遭WannaCry勒索攻擊。

南韓連鎖電影院CJ CGV
南韓CJ CGV電影院的廣告伺服器遭攻擊，約50間戲院受WannaCry入侵而遭殃。

日本
根據日本JPCERT統計，日本有600家公司，2,000臺電腦受WannaCry攻擊影響。

中國
根據奇虎360資安部門表示，有29,372個機構遭到攻擊，包含政府機構、大學、銀行自動提款機和醫院。

臺灣教育部統計
全臺總共10所學校（大學以下），59臺電腦受WannaCry攻擊。

臺灣電力公司
共有116臺行政電腦遭WannaCry攻擊，供電、輸電系統的電腦並未受到影響。

臺灣新北恩主公醫院
院內有3臺位於加護病房內的行動護理車的電腦，遭受WannaCry攻擊影響。

攻擊持續發生

鎖定台灣企業攻擊的勒索軟體「ColdLock」，五月初發動多起攻勢，加密企業資料庫

2020/05/11 讚 134 分享


戴慈慧

https://buzzorange.com/techorange/2020/05/11/coldlock-ransomware/

勒索病毒全球橫行！資安專家建議企業這麼做避免受害

新頭殼newtalk｜部敏 綜合報導
發布 2020.06.14｜10:38

讚 31

近幾個月來，包括Maze、WannaRen在內的多個勒索病毒肆虐，在美國、日本、台灣、中國等地造成災情。資安專家表示，此種病毒從早年的亂槍打鳥到近年來越來越有針對性，企業除了要建立對外的防護網外，對內也要有清楚的監控與回應機制，並為旗下每位員工建立良好的資安認知，才能將風險降到最低。

https://newtalk.tw/news/view/2020-06-14/420741

感染勒索病毒四大症狀

- 出現不明對外連線
- 各目錄下開始出現奇怪副檔名的檔案，例如：.crypt、.ECC、.AAA、.XXX、.ZZZ等等
- 突然出現很多 Ransom Note檔案（支付贖金的說明檔案）或捷徑
- 在瀏覽器工具列發現奇怪的捷徑

感染勒索病毒應對步驟

- 立即切斷網路，避免將網路磁碟機或共享目錄上的檔案加密。
- 立即關閉電腦電源：關閉電腦電源的目的是不讓勒索病毒繼續加密電腦中的檔案，關機時間愈快被加密的檔案愈少，**建議強制關閉電腦電源**
- 保留電腦，通報專業資安人員
- 不要付錢

防範勒索病毒：三不三要

三不:

- 不上鉤：收到標題吸引人的郵件，務必停看聽
- 不打開：不隨便打開Email附件檔案
- 不點擊：不隨意點擊Email中的網址

防範勒索病毒：三不三要

三要

- 要備份：依據3-2-1原則妥善備份重要資料—在兩種不同媒介上建立三個備份，其中一個備份要放在不同地方
- 要確認：打開Email前要確認寄件者身份
- 要更新：作業程式、軟體、病毒碼要隨時保持更新狀態，當軟體廠商(例如Flash/SilverLight/IE)公布修補程式請盡快更新。

個人資訊安全措施

十大資安習慣

1. 不名人士要留意

- 不明人士，在宿舍區、研究教學區進出走動，應通知相關管理人員處理與盤查
- 即使是認識同學，進出非其所屬領域，應主動詢問其來意
- 防止非法破壞、竊取裝置

2. 務必小心社交工程

- 利用人際關係的互動特性來竊取資料
  - 例如：同學這裡是學校XX單位，已發現你的電腦有竊取別人資料的情況，疑似中毒，請提供帳號密碼，我們需要進行後續處置。
- 點閱Email要特別注意
  - 寄件者郵件名稱
  - 即使是來自同一單位或是認識人之郵件，留意主旨與內容是否異常
  - 勿隨意開啟連結與附件
  - 善用垃圾郵件篩選功能

3. 電腦不用要登出或自動鎖定

- 長時間離開電腦前，應該要登出或關機
  - 防止資料遭竊
  - 防止帳號被盜用
  - 避免網路破壞
- 建議設定螢幕保護程式，且自動鎖定

4. 保護機敏資料

- 不要任意放置個人帳號密碼（勿貼在筆電或螢幕上）
- 機敏文件(帳密、身分文件、金融、研究資料)不隨便存放桌面
- 機敏文件不隨意散布且應經加密
- 不用email寄送機敏資料

5. 適當設定資料共享權限

- 機敏資料要與共享資料分開存放
- 設定密碼，且權限僅作適當開放（讀取與覆寫）

6. 密碼設定要穩固

- 密碼遭破解統計數據
- 密碼必須定期更換
- 停用Guest匿名帳號

- 以中文輸入法按鍵來當成密碼
- 以英文字或數字穿插
- 以一句英文，每字字首當成密碼

密碼長度	26 英文字母	26 英文字母+10 數字	52大小寫英文字母	96可印出字元
4	0	0	1 分鐘	13分鐘
5	0	10分鐘	1 小時	22 小時
6	50分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	23 年
8	24 天	10.5個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21萬9000年
10	45 年	1159 年	45838 年	2100萬年

7. 重要資料要異地備份

- 預防重要資料或設備損壞遺失或惡意鎖定
- 建議備份在不同裝置，但也需確認安全性

8. 作業系統與應用程式更新

- 駭客經常透過漏洞來入侵電腦
- 作業系統或應用程式設計上的問題
- 定期更新作業系統或應用程式

9.安裝防毒軟體與更新

- 安裝知名防毒軟體（通常有免費版可以使用）
- 定期更新病毒碼
- 隨時注意病毒最新資訊
  - 報章雜誌
  - 防毒軟體廠商

10. 網路瀏覽要小心

- 不要隨意瀏覽不知名網站、點擊連結或下載不明檔案
- 不要安裝未經驗證安全或授權的軟體
- 提供個人資訊時要檢查有無隱私權政策
- 進行線上交易要確定有加密措施
- cookie會自動記錄在網際網路的瀏覽及輸入資料，避免使用公用電腦

THE END

ALVIN4016@YM.EDU.TW