惡意程式簡易分析與防範

中毒的可能情形

- 網路連線正常，但無法上網
- 檔案無故遺失或執行時發生錯誤
- 電子郵件會自動發送垃圾信
- 開啟網頁會自動連到色情網站
- 電腦速度突然變慢
- 經常當機或出現錯誤訊息

惡意程式
定義與類型

定義：

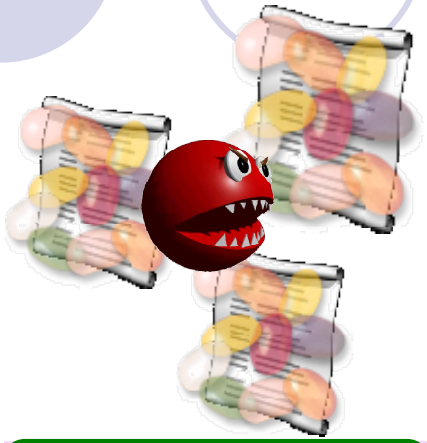
1. 自我複製與感染物件
2. 刪除檔案
3. 強制安裝且難以移除
4. 首頁綁架(hijacking)與廣告彈出
5. 惡意收集使用者與系統資訊
6. 惡意移除用戶端程式
7. 干擾電腦運作與影響系統網路效能

類型：

1. 電腦病毒(Computer viruses)
2. 蠕蟲(Worms)
3. 木馬(Trojans)
4. 駭客工具與其他惡意程式(Hacker Utilities)

電腦病毒的特性

自我複製



感染檔案

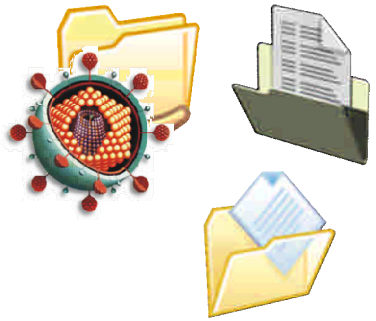
破壞系統檔案

特定時間觸發

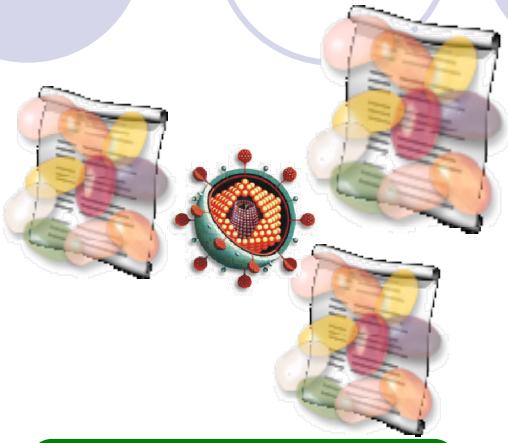
電腦病毒的危害

- 降低電腦效能
- 影響電腦操作
- 刪除檔案
- 影響應用程式與檔案關連性
- 破壞檔案
- 無法開機
- 刪除系統磁區所有檔案

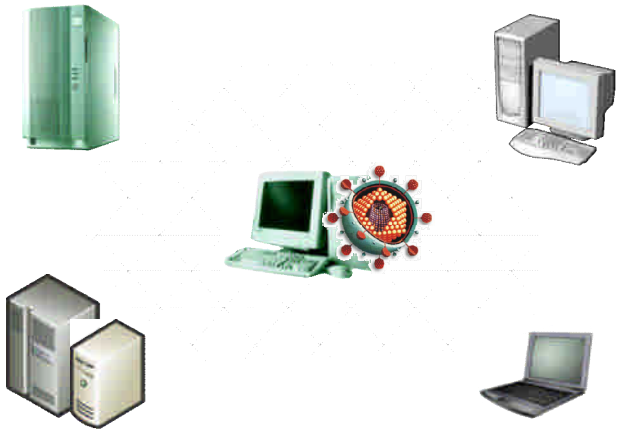
蠕蟲的特性



自我複製



感染檔案



攻擊其他電腦

利用程式傳播

蠕蟲的危害

- 降低電腦效能
- 降低網路效能(區域／廣域網路效能)
- 影響電腦操作
- 結合木馬(Trojans)與後門(Backdoors)竊取資訊
- 遭受DoS、DDoS(Distributed Denial of Service)攻擊
- 檔案遭到感染無法開啟(執行)
- 當成惡意程式傳播或攻擊主機，網域遭到國際組織列入黑名單或可能遭受具大求償

木馬的行為

1. 中止防毒軟體防護
2. 接收惡意程式作者的攻擊指令
3. 竊取並傳送個人可識別資訊
4. 偽裝系統或應用程式檔案名稱、圖示或執行程序
5. 更改系統設定，例如修改IE登錄值，使木馬隨著開啟IE瀏覽器時而觸發
6. 利用社交工具自我傳播
7. 阻止安裝防毒軟體及使用防駭工具
8. 結合蠕蟲(Worms)與後門程式(Backdoor)，利用其特性持續攻擊

木馬的危害

- 降低電腦安全性
- 降低電腦效能
- 影響電腦操作
- 降低網路效能
- 竊取資訊
- 結合間諜程式與垃圾信件，遭受網路詐騙機會增加
- 發送垃圾信件，網域遭到國際組織列入黑名單
- 當成惡意程式傳播或攻擊主機，可能遭受具大求償

惡意程式
傳播方式

- 木馬程式或病毒通常藏在一般檔案內，並使用各種生動有趣的字眼，誘使您執行該檔案。惡意程式通常被種植在以下檔案中：

  (1) *.EXE、*.COM：可執行檔
  (2) *.ZIP、*.RAR：壓縮檔
  (3) *.PIF：Windows程式資訊檔
  (4) *.SCR：螢幕保護程式檔
  (5) *.DOC、*.XLS、*.PPS：Office檔
  (6) *.VBA：Office巨集檔

- 通常電子郵件(E-mail)都會包含上述檔案類例來散播病毒或木馬程式，當您一執行這種惡意程式，您的電腦將會中毒或被安裝木馬程式。接著，遠端的駭客就能大大方方的取得您輸入的帳號、密碼、信用卡資料等。

範例1


她是老婆好友，理應可放心，但是一看收件者是一大堆，就有疑問了！
事實上她的名字，已被複製了，是病毒信
★內文故意寫一則笑話，好引誘您去開夾帶檔案

範例2


日期:
Fri, 22 Dec 2006 10:25:10 +0800 (CST)
寄件者:
angle740207@yahoo.com.tw
主題:
在一个古老的山乡(慕芙)
收件者:
←寄件者我不認識，
收件者又是一大堆人
幾乎可肯定是病毒信

範例3

惡意程式
防範

- 安裝正版作業系統及應用程式，避免使用盜版軟體
- 安裝防毒軟體並定期更新病毒特徵碼
- 定期啟動防毒軟體掃瞄整個電腦系統
- 隨時進行Windows漏洞更新
- 使用隨身儲存媒體時（例：隨身碟、磁碟片、記憶卡等），請先對該儲存媒體執行掃毒
- 避免使用P2P軟體，降低被植入病毒的機會
- 減少接收或開啟不明郵件（尤其是附件）與網頁
- 避免下載、安裝不明應用程式與檔案

- 安裝(啟用)防火牆，停用不使用的系統服務
- 定期變更系統登入密碼與網路社交工具(例:MSN)密碼，設定複雜密碼
- 重要檔案請定期備份
- **注意家中電腦是否中毒，避免家中與學校的電腦，透過隨身儲存媒體交錯、重複感染**