

# 病毒與蠕蟲對比



病毒 (virus) 與病毒 (virus)，它們都需被執行一次才能啟動 看起來只有2點不同: 1.需依附其他檔案存在與否 2. 病毒 (virus) 只會感染自己LOCAL的檔案 病毒 (virus) 會透過網路、郵件, 擴大感染 對嗎?

你的理解已經很接近正確

但這裡你其實是在對比 「電腦病毒 (computer virus)」 和 「網路蠕蟲 (computer worm)」，而不是兩種「病毒 (virus)」本身。

我們來釐清一下這兩者的差異與共通點

## 一、共通點

項目	電腦病毒 (Virus)	網路蠕蟲 (Worm)
都需執行一次才會啟動	<input checked="" type="checkbox"/> 是	<input checked="" type="checkbox"/> 是
都是惡意程式	<input checked="" type="checkbox"/> 是	<input checked="" type="checkbox"/> 是
可能造成資料損毀、系統異常等危害	<input checked="" type="checkbox"/> 是	<input checked="" type="checkbox"/> 是

## 二、主要差異

項目	電腦病毒 (Computer Virus)	網路蠕蟲 (Computer Worm)
依附性	必須依附在其他可執行檔（如 .exe、.doc、.xls 等）中，透過「感染」方式擴散。	可獨立存在，不需依附其他檔案。
傳播方式	通常只在本機 (Local) 或透過人工傳播（如拷貝到USB）。	可自動透過網路、電子郵件、共享資料夾等方式擴散。
傳播速度	相對慢（需人為觸發或開啟感染檔）。	傳播快（可自動搜尋與感染其他電腦）。
範例	CIH、Michelangelo、Melissa	Code Red、ILOVEYOU、Blaster

## 簡短總結

你說的「需依附其他檔案」與「是否能透過網路擴散」這兩點，**正是病毒與蠕蟲的關鍵區別**。

所以更正如下：

- **病毒 (Virus)**：需要依附其他檔案，通常只感染本機檔案。
- **蠕蟲 (Worm)**：不需依附檔案，可自動透過網路或郵件擴散。

是否要我幫你畫一張對照圖（病毒 vs 蠕蟲）？在課堂上會很好用。



Virus與Worm已經釐清了  
那木馬程式又有何不同?

非常好 你已經掌握了 Virus (病毒) 和 Worm (蠕蟲) 的核心差異，  
接下來我們把 Trojan Horse (木馬程式) 一起放進來比較，就更完整了。

## 一、三者的共同點

特性	病毒 (Virus)	蠕蟲 (Worm)	木馬 (Trojan Horse)
都是惡意程式	<input checked="" type="checkbox"/> 是	<input checked="" type="checkbox"/> 是	<input checked="" type="checkbox"/> 是
都可能造成資料損毀或外洩	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
都需要某種形式「執行」後才會生效	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## 二、三者的主要差異

項目	病毒 (Virus)	蠕蟲 (Worm)	木馬程式 (Trojan Horse)
依附性	需附在其他可執行檔上 (感染宿主檔)	不需依附，能自我複製傳播	通常偽裝成正常應用程式 (例如遊戲、安裝包)
自我複製能力	<input checked="" type="checkbox"/> 會感染其他檔案	<input checked="" type="checkbox"/> 會自動複製傳播	不會自我複製
傳播方式	需使用者開啟被感染檔案	自動透過網路、郵件、共享資料夾	使用者主動下載或執行 (被騙安裝)
主要目的	破壞或感染系統	快速擴散與癱瘓網路	偷資料、開後門、控制電腦
隱蔽性	中等 (通常可被偵測)	中等至高	很高 (常偽裝成合法軟體)
例子	Michelangelo、CIH	ILOVEYOU、Blaster	Zeus、Remote Access Trojan (RAT)

## 三、簡單記法 (老師常用版)

類型	口訣式說明
病毒 Virus	「靠別人活」——要依附在別的程式上。
蠕蟲 Worm	「自己會動」——能自動複製傳播。
木馬 Trojan	「裝好人騙你」——偽裝成正常程式讓你主動執行。

## 舉例情境

狀況	對應惡意程式
你開啟一個 Word 檔後，其他文件被感染。	病毒
電腦沒開任何郵件，卻自動發出垃圾郵件。	蠕蟲
你下載一個「免費遊戲」，結果電腦被遠端控制。	木馬程式

是否要我幫你畫成一張 「**病毒、蠕蟲、木馬**」三者比較圖（表格或圖像版）？

可用於教學投影片。



那電腦的邏輯炸彈（Logic Bomb）又有何特色？

## 邏輯炸彈（Logic Bomb）— 特性與防護重點

很好的問題！邏輯炸彈其實是惡意程式的一種 **觸發型 payload**，以下把重點列清楚，方便教學或筆記使用。

### 💡 定義（簡短）

**邏輯炸彈**：一段被植入在系統或程式中的惡意程式碼，在特定條件或事件發生時才啟動執行其破壞/惡意行為（例如刪檔、加密、開後門、發送資料等）。

### ⚙️ 主要特色（差異化重點）

- **觸發條件**：以條件為核心 — 常見條件有特定日期/時間（time bomb）、某個檔案不存在、系統變更、特定用戶登入、特定帳號餘額或事件發生等。
- **非自我複製**：本身通常不會自動複製或散播（不像 worm）；它可能被藏在合法程式、腳本或管理工具內。
- **潛伏性高**：平常不顯現，難以被即時偵測，直到觸發條件滿足才造成影響。
- **常由內部或受信任程式攜帶**：常見情境是被內部人員或供應商植入於企業系統或部署的軟體中（insider threat / supply-chain）。
- **可搭配其他惡意程式**：邏輯炸彈可以作為病毒、木馬或其他惡意程式的一部分（payload）。

### 📌 舉例說明

- **Time bomb（時間炸彈）**：程式在 2025/12/01 自動刪除特定資料。
- **條件炸彈**：當發現「某帳戶餘額 < 0」或「某服務被停用」時執行破壞。
- **內部植入**：被授權的維運腳本中暗藏程式，當主管離職或特定事件發生才觸發。

## 🛡️ 偵測與防護建議（實務可行）

1. **原始碼審查與變更控制** (Code review、PR 流程、簽署提交)
2. **供應鏈安全檢查** (第三方套件、供應商軟體驗證)
3. **最小權限與分離職責** (避免單一帳號能部署全部)
4. **行為式偵測/EDR** (監控不正常檔案操作、排程或突發大量 I/O)
5. **檔案/系統完整性檢查** (如使用哈希比對、檔案變動告警)
6. **定期備份與災難恢復演練** (即使被觸發，也能快速回復)
7. **日誌與監控告警** (異常登入、未授權變更應即時告警)
8. **員工/供應商安全教育** (降低內部惡意或疏忽風險)

## 💡 與病毒 / 木馬 的比較（一句話）

- **病毒**：靠感染其他檔案複製自己。
- **木馬**：偽裝成合法程式以騙使用者執行，通常用來偷取資料或開後門。
- **邏輯炸彈**：不一定自我複製或偽裝為主體，它是「在特定條件下才爆發的惡意程式碼」，常內嵌在其他程式或由內部植入。

需要我把上面整理成一張教學用的投影片或一張對照圖（含時間炸彈/事件炸彈/範例/防護步驟）嗎？我要是幫你做成 PPT 範本或一張圖表給你上課用。