# 這些敵人會做些什麼？

## 1. 病毒

電腦病毒是最為人熟知的工具，通常是具惡意的程式設計師所撰寫的電腦程式，病毒會自我複製，並由特定事件觸發感染電腦軟體。

舉例來說，巨集病毒依附在含巨集指令（會自動重複執行的副程式，例如合併郵件）的檔案中，並在執行巨集的同時啟動病毒。這類病毒指示會造成使用者困擾，當每次按到某個鍵時就會顯示一些可笑訊息。其他更具破壞性的病毒，則會拖慢系統速度或刪除檔案等更嚴重的問題。

梅麗莎病毒（Melissa virus）首度出現於 1999 年 3 月，在當時造成全球電腦業界 8 千萬美元損失。

經由磁片或網路下載的外來電腦病毒可能只感染一台電腦，但當一部電腦受到感染後，其所在網路的其他電腦很有可能也受到感染。

## 2. 特洛伊木馬（Trojan Horse）程式

特洛伊木馬程式，簡稱特洛伊，是傳送破壞指令的工具程式。經偽裝後，乍看之下似乎無害，但實際上卻可刪除資料、自動將信件送給通訊錄中所有人，導致電腦後門洞開，受到其他攻擊。

唯有將特洛伊木馬程式複製到系統中才會感染特洛伊病毒，途徑可能是透過磁片、網路檔案下載，或打開電子郵件附加檔。但不論特洛伊或其他病毒都不會單純由電子郵件訊息散佈，而是在郵件附加檔中。

### 3. 攻擊

攻擊的方法有許多種，大致可分成三大類：偵察，存取，以及拒絕服務（Denial of Service，DoS）。

- 實際上，偵察攻擊就是資訊蒐集的行為，駭客可利用所蒐集的資訊危害網路。目前有一些軟體工具，如 sniffers 或 scanners，都可以顯示網路上資源，並找出可能的弱點。舉例來說，特定軟體可以破解資料中的密碼，儘管這些軟體用途是正當的，可是一旦不當使用，它們也是相當危險的工具。
- 存取攻擊主要被用來發掘網路中既有弱點，為了進入電子郵件帳戶、資料庫以及取得所有機密資訊，如認證服務或是檔案傳輸（FTP）功能。

一個西歐駭客集團主要目標便是線上金融網站，並宣稱「在全球金融市場控制下，最佳賺錢方式就是針對企業所設立的形象、信譽及金融資訊進行攻擊。」

- 拒絕服務攻擊的目的在於，阻止所有或部分網路正常存取。方法是把大量沒有用的資料發送至網路上的設備，以阻擋其他正常訊息的流通。另外一種亦具強大威脅性的是分散式拒絕服務（Distributed DoS，DDoS），攻擊者會利用多部設備或主機進行攻擊。

### 4. 惡意破壞者

眾所皆知，ActiveX 與 Java 應用程式可使網頁變得更生動活潑，利用一些特殊效果，就可使網站變得更具吸引力及互動性。但是，也由於程式下載非常容易，已成為進行破壞的媒介。Vandal 是應用軟體或小程式，所造成的破壞從毀損單一檔案，到刪除整個電腦系統都有可能。

將近 43% 的網路內容是屬拍賣詐欺。

### 5. 資訊攔截

任何透過網路傳送的資料，都可能被未授權者攔截。破壞者可能竊聽通訊內容，甚至竄改傳送資訊封包，利用各種方法截取資料，如 IP spoofing，冒用被接受的 IP，偽裝成經過認證的使用者，以進行資訊傳輸。

### 6. 社會工程

社會工程是日漸盛行的行動，主要是透過非科技方法以取得網路機密安全資料。破壞者可能偽裝成網路工程師，並利用電話收集員工密碼、賄賂網路工程師以獲取資料或搜查辦公室，找出被寫下的密碼。

### 7. 垃圾郵件

垃圾郵件泛指無用多餘的電子郵件，以廣告居多。通常這些郵件雖然無害，但也會造成困擾，因為需要花時間閱讀，並佔用儲存空間。