濫發垃圾信被斷網怎麼辦

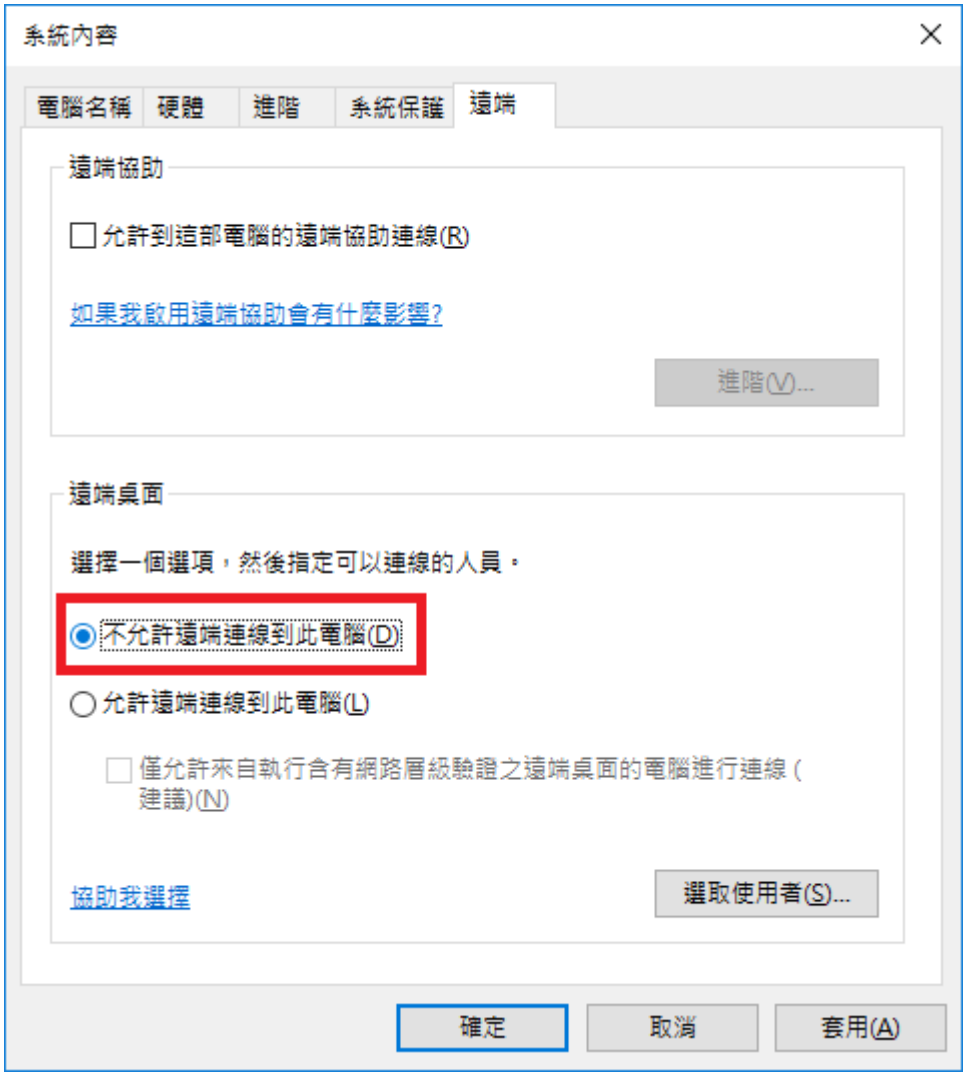
發生原因

工科系過往處理的類似案例通常都是

1. Windows 系統允許遠端桌面連線
2. 帳號密碼太好猜被破解
3. 駭客利用原本的使用者or新創一個使用者下載 Turbo-Mailer (大量發信程式)並執行
4. 計中發現異常後，將該 IP 阻斷

解決方法

- 如果平時沒有遠端連線的需求就關閉這功能 ([控制台\所有控制台項目\系統\進階系統設定]),



有需求建議改用 Teamviewer (https://www.teamviewer.com/zhTW/)

- 在[控制台\使用者帳戶]檢查有沒有多出不明的使用者，有的話將之刪除；另外記得將原先的使用者

密碼更改為強度70分以上的 (http://password.mx500.com/)

- 搜尋 Turbo Mailer 把找到的資料夾跟檔案都刪除，駭客就是用這個軟體大量發垃圾信 (但不會被防毒程式判定為病毒)
- 利用學校提供的防毒軟體(推薦卡巴斯基)或下載 Avira Free Antivirus 徹底全系統掃毒，看有沒有潛藏的威脅
- 進行「網路回報」作業(須有中心 mx□oz□my 或 m系列 的電子郵件信箱帳號)，系統執行自動阻斷解除的作業時間為每週週一至週五的 08:00、12:00 與 17:00 整點。不便之處，敬請見諒。

以上資料，感謝工科系單位網管何孟軒先生提供