北區 SOC 中心-常見弱點處理建議措施-網路探測行為

事件名稱	**WORM: W32/Mydoom@MMWorm Variants IV**
說明	此為W32/Mydoom@MM蠕蟲變種IV，入侵偵測系統偵測到大量散發郵件和對等網路的檔案共用蠕蟲W32/Mydoom@MM 的多種變種。 當沒有戒心的使用者開啟附件因而執行檔案時，它會將其自身以taskmon.exe 複製到WINDOWS SYSTEM 目錄，並建立某些登錄項目。該蠕蟲會從受感染的電腦收集電子郵件地址，並嘗試透過傳送帶有病毒附件的電子郵件至所收集到的電子郵件地址來進行自我傳播。
影響	成功的感染可讓該蠕蟲從受害的電腦上收集資訊，並使用受感染電腦做為跳板，進一步傳播和/或發動拒絕服務攻擊。
影響系統	Windows 作業系統
建議解決方法	1. 請確認您的防毒產品更新了最新的引擎和掃描檔案 2. 可在各大防毒軟網站線上病毒資訊庫中，找到手動移除病毒的指示。 3. 確認防毒軟體的病毒碼已更新為最新版本、系統已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。

資料來源：N-ASOC