

# 資安通報平台威脅情報說明

當收到資安情資後，經適當且有效的系統調查後，並未發現有直接或間接證據可證明系統遭受到資安事件之威脅即可選擇 TII(威脅情報)。建議您在進行系統調查時進行下列步驟：

- 檢查系統或網路相關 LOG 資訊，查看是否有異常之處。
- 利用如 TCPVIEW 工具軟體或 netstat 指令來查看系統是否有開啟可疑之服務或是否有可疑之來源連線。
- 查看防火牆之連線記錄，確認是否有可疑之連線。
- 如果有設置入侵偵測軟體 (IDS)，進行查看是否有惡意的連線行為。

## 4. 資通安全事件：基本資料

◎事件分類：

TII ( 威脅情報 ) : 經確認為威脅情報(說明)

- INT ( 入侵攻擊 ) :
- 系統被入侵(資訊設備遭惡意使用者入侵)
  - 對外攻擊(對外部主機進行攻擊行為)
  - 針對性攻擊(針對特定個人的資訊洩漏與身分盜取)
  - 散播惡意程式(主機對外進行惡意程式散播)
  - 中繼站(主機成駭客之中繼站，接收惡意程式連線)
  - 電子郵件社交工程攻擊(帳號遭盜用對外發動社交工程攻擊)
  - 垃圾郵件(Spam)(資訊設備從事Spam Mail散播行為)
  - 命令與控制伺服器(C&C)(主機疑似為駭客之Botnet C&C Server)
  - 殭屍電腦(Bot)(資訊設備疑似成為駭客所控制之Botnet成員)
  - 其它類型的入侵攻擊

- DEF ( 網頁攻擊 ) :
- 惡意網頁(網頁遭駭客置換或放置不當內容)
  - 惡意留言(網頁遭駭客放上惡意留言)
  - 網頁置換(網頁遭駭客置換)
  - 釣魚網頁(主機遭駭客置入釣魚網頁)
  - 個資外洩(主機遭個資外洩)
  - 其它類型的網頁攻擊