

張貼日期：2024/09/13

【資安訊息】請各單位加強留意俄羅斯的駭客組織針對臺灣網站發起DDoS分散式阻斷服務攻擊

- 主旨說明：請各單位加強留意俄羅斯的駭客組織針對臺灣網站發起DDoS分散式阻斷服務攻擊
- 內容說明：
 - 近期臺灣有多個單位之網站遭到俄羅斯的駭客組織(NoName057)之DDoS分散式阻斷服務攻擊，引發資安事件，該組織可能持續發動攻擊，請各單位多加注意監控主管系統運作情形，適當系統備援並搭配流量清洗、CDN與靜態網頁等措施，維持系統韌性運作。
 - 近日內請金融、重要網站及工控設備(SCADA)等，相關單位多加戒備防範，並強化SOC監控。
- 影響平台：\無
- 建議措施：
 1. 請各機關持續強化資安防護機制與人員資安意識，並觀察機關網站連線、帳號登入等網站使用情形。
 2. 確認網站服務不中斷，若遭受DDoS攻擊應循「臺灣學術網路 (TANet) 分散式阻斷服務 (DDoS) 通報應變作業指引」申請作業DDoS清洗服務。
 3. 請使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結，以防被植入後門程式。
- 參考資料：
 - 臺灣學術網路 (TANet) 分散式阻斷服務 (DDoS) 通報應變作業指引<https://portal.cert.tanet.edu.tw/docs/pdf/2022101709104545607092166583830.pdf>

計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailling:announcement:20240913_01



Last update: **2024/09/18 09:27**