張貼日期：2025/08/04

【資安訊息】瀏覽器擴充功能遭惡意劫持威脅活動，敬請加強擴充功能安全管理

- 主旨說明:【資安訊息】瀏覽器擴充功能遭惡意劫持威脅活動，敬請加強擴充功能安全管理

- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 NISAC-400-202507-00000048
  - 資安院觀測外部資安情資，近期發現駭客針對瀏覽器擴充功能進行惡意劫持活動（如Red Direction活動）， 其攻擊手法為利用合法之擴充功能，於後續更新中植入惡意程式碼，可監控使用者網頁瀏覽活動並傳送至C2伺服器，甚至導向釣魚網站。 影響範圍 Chrome 與 Edge 共計18種擴充功能，其可能含蓋超過230萬名使用者。
  - 詳細清單下載連結：https://cert.tanet.edu.tw/pdf/2023057048ioc.zip
- 影響平台:
  - N/A
- 建議措施:
  - 1 清查並移除所有已確認存在惡意威脅之瀏覽器擴充功能。
  - 2 清除瀏覽器快取Cookie及相關會話資料，避免持續的憑證洩漏風險。
  - 3 持續監控受影響主機及相同網段的網路行為，確保異常活動不再復發。
  - 4 如懷疑帳號憑證已外洩，請強制重設相關使用者密碼及多因素驗證設定。

計算機與通訊中心
網路系統組 敬啟