張貼日期：2021/06/04

【資安訊息】我國能源領域關鍵基礎設施資安事件防護資訊，請參考並加強防範！

主旨：【資安訊息】我國能源領域關鍵基礎設施資安事件防護資訊，請參考並加強防範！

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202106-0176
  - 近期於國內能源領域關鍵基礎設施發現惡意程式SALTYGHOST為Gh0st RAT木馬程式之變種，針對此事件相關惡意程式分析報告與受駭偵測指標(Indicator of Compromise, IoC)資訊提供如附件，建議各會員應提高警覺，落實加強監控防護與異常連線阻擋，若於監控日誌發現相關異常連線或警示，應深入釐清事件原因與影響範圍，避免錯失調查時機。
  - 影響平台: Windows作業系統
- 建議措施:
  1. 部署黑名單於防護設備進行偵測，監控是否有資訊設備已遭入侵，網路位址與網域名稱黑名單如附件。
  2. 依「我國能源領域關鍵基礎設施之惡意程式分析」檔案中之惡意程式名稱與雜湊值，偵測系統是否存在相關惡意程式，若確認資訊設備已遭入侵，建議立即進行必要處理措施：
     1. 針對受駭電腦進行資安事件應變處理。
     2. 重新安裝作業系統，並更新作業系統及相關應用軟體。
     3. 更換系統使用者密碼。
- 參考資料:

  我國能源領域關鍵基礎設施之惡意程式分析報告

計算機與通訊中心
網路系統組 敬啟