張貼日期：2022/03/15

【資安攻擊預警】美國FBI發布RagnarLocker勒索軟體威脅指標，請加強偵測與防護！

- 主旨說明：美國FBI發布RagnarLocker勒索軟體威脅指標，請加強偵測與防護！
- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202203-0504
  - 因應RagnarLocker勒索軟體對能源、金融、政府及高科技等CI領域造成多起資安事件，美國FBI發布相關防護建議，技服中心綜整相關資料供各會員參考，內容詳見建議措施。
- 影響平台:
  Windows平台
- 建議措施:
  1. 針對附件提供之威脅指標(indicators of compromise, IOCs)落實部署防護機制。
  2. 加強電子郵件安全防護與惡意程式檢測。
  3. 加強網路設備之威脅偵測與連線行為監控。
  4. 為強化勒索軟體資安防護，建議強化下列安控措施：
     1. 部署多因子身分鑑別機制，並強化密碼管理。
     2. 落實資料、系統映像檔及組態設定之備份作業，且備份檔應離線保存並定期測試。
     3. 即時更新系統軟體版本與修補漏洞。
     4. 停用不必要之遠端服務與通訊埠，並落實監控遠端存取日誌。
     5. 定期稽核特權帳號與存取規則，落實最小存取權限原則。
  5. 如有發現異常應立即進行通報。
  - 附件-FBI的CU-000163-MW Flash Alert警報：https://www.ic3.gov/Media/News/2022/220307.pdf
- 參考資料:
  https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/fbi-releases-indicators-compromise-ragnarlocker-ransomware

---

計算機與通訊中心
網路系統組 敬啟