張貼日期：2023/02/13

【資安訊息】數聯資安202302月IOC資訊

- 主旨說明：數聯資安202302月IOC資訊

- 內容說明：
  - 轉發 數聯資安 ISSDU-ANA-202302-0001
  - 數聯資安(ISSDU)透過監控服務找到異常執行檔，進一步展開分析發現之相關情資。
  - 參考MITRE&ATTACK: https://attack.mitre.org/techniques/T1055/
- 影響平台: 無
- 建議措施:
  - Domain建議將對應的Domain透過防火牆IPS規則或是黑名單阻擋使其在DNS無法解析。而非靠Firewall自動將對應IP解析阻擋，如此設定會造成正常IP遭誤擋。
  - SHA256此為惡意程式、病毒、惡意文件等檔案以不同的演算法經過內容換算得出來的HASH用以辨識不同的樣本，建議透過防毒軟體的CUSTOM HASH BANNING進行手動增加已使對應樣本能被貴客戶所使用之防護設備偵測並阻擋。
- 參考資料:
  - 202302月IOC資料下載連結：https://cert.tanet.edu.tw/pdf/202302ioc.xlsx

---

計算機與通訊中心
網路系統組 敬啟