張貼日期：2021/02/08

【資安攻擊預警NoxPlayer模擬器被植入惡意程式，針對臺灣、香港及斯里蘭卡進行攻擊，請各會員注意防範！

主旨：【資安攻擊預警NoxPlayer模擬器被植入惡意程式，針對臺灣、香港及斯里蘭卡進行攻擊，請各會員注意防範！

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 NCCST-ANA-G2021-0056
  - 資安公司ESET近期觀察到NoxPlayer模擬器被植入惡意程式，針對臺灣、香港等進行特定目標攻擊。建議除使用防毒軟體檢查資訊設備是否受惡意程式感染，也可透過檢查連線紀錄與惡意程式資訊確認感染與否。
- 影響平台:
  微軟Windows與蘋果Mac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下：
     - 210.209.72.180
     - 103.255.177.138
     - 185.239.226.172
     - 45.158.32.65
     - cdn.cloudistcdn.com
     - q.cloudistcdn.com
     - update.boshiamys.com
     - http://cdn.cloudfronter.com/player/upgrade/ext/20201030/1/35e3797508c555d5f5e19f721cf94700.exe
     - http://cdn.cloudfronter.com/player/upgrade/ext/20201101/1/bf571cb46afc144cab53bf940da88fe2.exe
     - http://cdn.cloudfronter.com/player/upgrade/ext/20201123/1/2ca0a5f57ada25657552b384cf33c5ec.exe
     - http://cdn.cloudfronter.com/player/upgrade/ext/20201225/7c21bb4e5c767da80ab1271d84cc026d.exe
     - http://cdn.cloudfronter.com/player/upgrade/ext/20210119/842497c20072fc9b92f2b18e1d690103.exe
     - https://cdn.cloudfronte.com/player/upgrade/ext/20201020/1/c697ad8c21ce7aca0a98e6bbd1b81dff.exe
     - http://cdn.cloudfronte.com/player/upgrade/ext/20201030/1/35e3797508c555d5f5e19f721cf94700.exe
     - http://res06.bignox.com/player/upgrade/202009/6c99c19d6da741af943a35016bb05b35.exe
     - http://res06.bignox.com/player/upgrade/202009/42af40f99512443cbee03d090658da64.exe
  2. 各會員可依參考資訊連結，取得詳細惡意程式特徵如雜湊值與偵測規則，用以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. 針對受害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:
  - https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

計算機與通訊中心
網路系統組 敬啟