張貼日期：2021/01/18

【資安攻擊預警】近期駭客組織攻擊活動頻繁，請加強系統/應用程式更新與防範作業

主旨：【資安攻擊預警】近期駭客組織攻擊活動頻繁，請加強系統/應用程式更新與防範作業

- 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 NISAC-ANA-202101-0622
  - 近期駭客組織攻擊活動頻繁，駭客透過進階持續性滲透攻擊(Advanced Persistent Threat, APT)方式成功入侵目標組織並植入惡意程式，建議各級機關應提高警覺，定期檢視例行性排程設定與派送機制，如於相關日誌發現異常連線或警示，應深入釐清事件原因與影響範圍，避免錯失調查時機，目前已掌握近期駭客利用惡意程式資訊如下：
    - 【樣本1】MD5：D6768C14A9E2064D659F7BF68FF4C1D1SHA-1：DF68B14964A66B774040277BF5A2458FA57A6224
    - 【樣本2】MD5：7AA3A5EBCA6C1064868B780CCF2D6348SHA-1：FAD40A72C0B1E26853AA96C84FF4307040A4909F
    - 【樣本3】MD5：B9A247D240D6CC7F37A22306FE26E79FSHA-1：89AB14854E5A69E2A9B7ABF8AB15E875E647E0FC
    - 【樣本4】MD5：0499D3385BD8E9B4989F2A8C829ADFE6SHA-1：7CCE793C017CE1BA86D088E809DF2733D6CF8D8C
    - 【樣本5】MD5：28544574EA6C80A30EC92D6910999669SHA-1：C69B42E5D46363659A33D6AD8E726D27544A0FE7
    - 【樣本6】MD5：AF6B7576FF97526C081507F3F7C3DA42SHA-1：3B2D8020D59C9DF1BABB4434C08166D2129758A5
    - 【樣本7】MD5：B737D8381F06C183F22F80B550370DECSHA-1：6A6F84E5DD3FC2F69BEE9322849A7A76BB826858
    - 【樣本8】MD5：88312E59D71E7AED15D906E5DFAFFFC0SHA-1：DAEBA07F8A2970103A3820B56D225B06C682483F
    - 【樣本9】MD5：B44EA82AD8C43A6D08BD1A40CB6C8864SHA-1：93982A1FC8E383217D683074F18E9F8B419DB707
    - 【樣本10】MD5：9B46698B08DEDC0D617849B7693A3124SHA-1：F67F1E879DB198A6461675266F395EDCBDACA43D
    - 【樣本11】MD5：E45A17AD2E99B3DD65B51C5F5123B2C1SHA-1：FFB9AF3FA59E849D5DDDFFD41725D0C7EC0619C6
    - 【樣本12】MD5：63DEF2168BFEE348615A5436476AAE39SHA-1：5A6FA3F812F8589B1015DBF35EDEEC8A8CC4B0CA
    - 【樣本13】MD5：80CC33D54B8CCB3B4C482B1DC7BA63F3SHA-1：0C22FECFBFC36D5798872164137135E7C7BB0F7F
  - 此外，近期機關通報事件原因包含廠商維護環境或管理疏失情形，發現駭客透過供應鏈攻擊，入侵機關內部資通系統/設備，或透過廠商維護帳號登入其所開發/維護之系統，而機關系統存取權限未設定或網段不當切割，導致橫向影響內部其他系統。建議機關除落實設備權限控管並定期檢視權限設置情況外，亦應監督委外廠商資通安全維護情形，以避免資安疑慮。
- 影響平台:
  全
- 建議措施:
  1. 如發現資通訊系統存在可疑檔案，建議進行MD5或SHA-1比對，以確認是否為惡意程式。
  2. 定期檢視資通訊系統日誌紀錄，同時檢視資通訊系統排程設定與派送機制，如發現異常連線或新增排程情形，應立即深入了解事件原因。
  3. 不定期檢視資通訊系統帳號使用情況，並定期變更帳號密碼，確保密碼設定符合複雜性原則，

避免字符轉換情況發生。
4. 檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要使用存取。
5. 確認作業系統、防毒軟體及應用程式(如Chrome□Java)更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。
6. 加強教育訓練，請使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結，以防被植入後門程式。
7. 依據行政院資通安全處於109年12月頒布之「各機關資通安全事件通報及應變處理作業程序」之「跡證保存」要求，保存相關資通系統之日誌範圍與項目。

計算機與通訊中心
網路系統組 敬啟