**張貼日期：2019/01/24**

# [資安漏洞預警通知] 駭客利用名稱解析服務進行資訊竊取攻擊，請各單位注意防範

主旨：駭客利用名稱解析服務(DNS)進行資訊竊取攻擊，請各單位注意防範

- 內容說明:
  - 國際資安廠商公布駭客利用名稱解析服務(DNS)進行下列二種資訊竊取攻擊：
    1. 名稱解析劫持中間人攻擊
       - 劫持方式(1)：入侵DNS伺服器，竄改其上的名稱/位址對應(A Record)將合法網站之主機名稱(Domain Name)對應至駭客控制之中繼站IP當使用者欲連線至該網站時，將會連線至駭客控制的中繼站。
       - 劫持方式(2)：入侵網域註冊商或國家頂級域名主機，竄改其上的網域主機名稱/位址對應(NS Record)將特定網域之NS主機指向駭客控制之DNS伺服器。當使用者欲連線至該網域下之任何主機名稱時，將會轉而向駭客控制之DNS伺服器進行查詢，進而連線至駭客控制之中繼站。
    2. 利用DNS伺服器作為中繼站，進行資訊竊取行為
       - 駭客入侵使用者資訊設備後，惡意程式利用DNS查詢機制，將敏感資訊隱藏在查詢內容中，傳送到駭客所架設之名稱查詢伺服器，駭客可利用DNS往返通訊，傳輸控制命令或竊取機敏資料。
  - 上述二種利用名稱解析服務所進行的攻擊，不易被察覺，請各單位進行DNS名稱/位址對應確認與DNS連線紀錄檢查，相關IP/Domain黑名單資料後列。
- 影響平台: 無
- 建議措施:
  1. 名稱解析劫持中間人攻擊，建議檢查措施：
     1. 使用防毒軟體檢查DNS主機是否受惡意程式感染。
     2. 確認DNS主機上的對應紀錄是否正確。
     3. 確認網域註冊商上的對應紀錄是否正確。
     4. 使用多因子身分認證，強化DNS登入與異動管理。
  2. 名稱查詢服務資訊竊取攻擊，建議檢查措施：
     1. 使用防毒軟體檢查資訊設備是否受惡意程式感染。
     2. 檢查是否有資訊設備嘗試連線至下列IP/Domain黑名單。
        - 185.20.184.138
        - 185.20.187.8
        - 185.161.211.72
        - 0ffice36o[.]com
        - hr-wipro[.]com
        - hr-suncor[.]com
     3. 透過防火牆規則限制資訊設備可對外連線的DNS主機位址。
- 參考資料:
  1. https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign
  2. https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
  3. https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

計算機與通訊中心
網路系統組 敬啟