張貼日期：2019/11/06

【資安攻擊預警Lemon_Duck PowerShell加密勒索企業網路

主旨Lemon_Duck PowerShell加密勒索企業網路

說明：

- 內容說明
  - 台灣電腦網路危機處理暨協調中心接獲國際情資，駭客利用Lemon_Duck PowerShell嘗試利用EternalBlue SMB漏洞，暴力攻擊MS-SQL服務或Pass-the-hash攻擊系統，迴避資安防禦機制，入侵終端系統執行惡意勒索並散播惡意程式。
  - 受感染系統會以下列方式散播:
    1. EternalBlueSMB漏洞利用。
    2. USB和網路磁碟:腳本會將惡意Windows *.lnk shortcut files與DLL files寫入感染系統中的USB或連線的網路磁碟機中，並透過Windows *.lnk漏洞(CVE-2017-8464)散播惡意程式。
    3. Startup file:腳本將惡意檔案寫入Windows系統上的啟動位置(如開始中的啟動裡)，並在統重啟後執行。
    4. MS-SQL Server暴力破解: 使用腳本置中的密碼表嘗試暴力破解SQL Server的SA帳戶。
    5. Pass the Hash攻擊: 利用腳本中的hash table執行Pass the Hash攻擊。
    6. 使用WMI在遠端系統上執行惡意指令。
    7. RDP暴力破解。
  - 攻擊來源資訊：
    - Potential C2:
      27.102.107[.]41
    - Potential Brute Force:
      113.140.80[.]197 - Port Scanning/Brute force (CN)
      120.253.228[.]35 - Port Scanning/Brute force port 3389 (CN)
      112.133.236[.]187 - Brute Force port 445 (India)
      58.62.125[.]245 - Brute Force port 445/Port Scanning (CN)
    - Potential Scanning:
      58.221.24[.]178 - Port Scanning (CN)
      221.4.152[.]250 - Port Scanning port 1433 (CN)
      182.140.217[.]226 - Port scanning (CN)
      1.202.15[.]246 - Port scanning port 3389 (CN)
  - Additionally the following are potential host indicators:
    - Scheduled task named Rtsa
    - Listening port of 65529
    - Service with a randomly generated name
    - Mutexes within PowerShell called LocalIf and LocalMn
- 影響平台: 所有Windows系統
- 建議措施:
  1. 安裝Windows SMB 安全更新。
  2. 關閉網路芳鄰(SMBv1)
  3. 使用高強度密碼。
  4. 安裝Windows CVE-2017-8464 漏洞相關安全更新。
  5. 建議封鎖攻擊來源IP

計算機與通訊中心
網路系統組 敬啟