張貼日期：2021/04/23

【資安攻擊預警Qlocker 勒索病毒攻擊事件

主旨：【資安攻擊預警Qlocker 勒索病毒攻擊事件

- 事件簡述：
  - 自 4/19 起，一個名為 Qlocker 的勒索病毒鎖定 QNAP(威聯通)品牌的 NAS 進行攻擊，會將檔案加密壓縮為 7zip 的壓縮檔，並勒索 0.01 BTC (約 14,700 TWD)
- 攻擊方式：QNAP 已就事件作出回應，指 Qlocker 攻擊與 CVE-2020-2509 與 CVE-2020-36195 漏洞有關，該漏洞允許任意人士取得完整的存取權限，並在 NAS 上執行勒索軟體。
- 預防措施:
  - NAS中招勒索病毒 群暉回應：立即做這5步
  - 你的NAS也中了勒索病毒嗎? 防疫三步驟趕快照著做防堵病毒入侵!

  1. 另外新增一組具有管理員權限帳號後，禁用系統預設 admin 帳號
  2. 啟用 2 步驟驗證，強化帳號安全
  3. 關閉未使用的網路服務，並更改預設通訊埠，及勾選使用安全連線 (HTTPS)
  4. 在安全設定中開啟失敗次數過多封鎖連線，選擇「拒絕清單內的連線」與「僅接受清單內的連線」這兩種
  5. 有重大安全的漏洞就更新
- 解決方式QNAP 強烈建議所有使用者立即安裝並使用最新版 Malware Remover 進行惡意軟體掃描，並更新 Multimedia ConsoleMedia Streaming Add-on 及 Hybrid Backup Sync 三個 App 至最新版。使用者若受到勒索病毒影響，或觀察到勒索病毒執行中，並正在加密檔案，應保持 NAS 開機狀態、立即安裝並使用最新版 Malware Remover 進行惡意軟體掃描、並聯繫 QNAP 技術支援單位 (https://service.qnap.com/) 取得協助。
- 其它參考資料:
  - Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices
  - 威聯通NAS遭勒索軟體Qlocker攻擊，疑似甫修補的重大漏洞惹禍
  - QNAP 官方社群討論串
  - 9QNAP的安全防護設定

感謝工科系 何孟軒先生 提供

計算機與通訊中心
網路系統組 敬啟