

張貼日期：2024/09/27

【資安訊息】組織型駭客利用物聯網設備建立大規模殭屍網路，恐對我國關鍵基礎設施構成威脅！

- 主旨說明：組織型駭客利用物聯網設備建立大規模殭屍網路，恐對我國關鍵基礎設施構成威脅！
- 內容說明：
 - 轉發 國家資安資訊分享與分析中心 NISAC-400-202409-00000080
 - 資安院依據美方所公布情資，與中國大陸相關之組織型駭客自2021年以來，透過入侵物聯網設備，建立了龐大的殭屍網路，其規模超過26萬台設備且遍布全球，受影響設備包括家用或小型路由器、防火牆、網路儲存設備(NAS)等物聯網設備，攻擊者主要利用已知漏洞入侵這些設備，並植入Mirai變種惡意程式。依其攻擊手法、技術與相關基礎設施，推斷與知名網路威脅組織Flax Typhoon、RedJuliett及Ethereal Panda相關。
 - 該殭屍網路可能被用於對我國關鍵基礎設施發動分散式阻斷服務(DDoS)攻擊或作為跳板進行進一步滲透，請各會員清查與阻斷附件所列相關威脅指標([*].w8510.com)並參考建議措施加強管控所轄之物聯網設備。
- 影響平台：
N/A
- 建議措施：
 1. 各關鍵基礎設施服務提供者應立即檢查轄下所有物聯網設備韌體，並更新至最新版本，特別注意修補附件中列出的已知漏洞。附件-IOC及漏洞清單下載連結：
https://cert.tanet.edu.tw/pdf/ioc_20240927_info.xlsx
 2. 加強對物聯網設備的安全管控，包括更改預設密碼、關閉不必要的服務與通訊埠、停用或加強管控遠端管理功能、汰換停產(End-of-life)設備及實施網路隔離等。
 3. 加強對異常網路流量的監控，及時發現並處置潛在殭屍網路活動。
 4. 依服務需求評估是否部署進階DDoS防禦方案，提升對大規模DDoS攻擊之防護能力。

計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20240927_01

Last update: 2024/09/27 10:07