

張貼日期: 2020/05/11

【資安攻擊預警】APT駭客族群對醫療服務與多種其他重要服務進行攻擊活動訊息

主旨: 【資安攻擊預警】APT駭客族群對醫療服務與多種其他重要服務進行攻擊活動訊息

- 內容說明:

- 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202005-0214
- 美國CISA與英國NCSC報告指出，近期觀察到APT駭客族群利用COVID-19疫情相關主題對醫療機構、製藥公司、醫學研究組織、學術界及地方政府等重要服務進行網路攻擊活動。分享相關威脅指標與資安報告，供會員注意防範。

- 影響平台:

全

- 建議措施:

1. 依威脅指標清單(詳如附件)，檢查資安防護設備是否有相關的連線紀錄與郵件紀錄。
2. 修補提供遠端辦公服務設備的資安漏洞，如Citrix\Pulse Secure\Fortinet\Palo Alto的VPN設備漏洞。
3. 使用線上會議服務時，不要將會議存取資訊公開，且應設定會議密碼。
4. 強化使用者認證機制，如多因子認證、強制密碼複雜度等。
5. 提醒使用者小心釣魚郵件、釣魚簡訊及釣魚網站等攻擊手法。

- 參考附件: <https://cert.tanet.edu.tw/images/threat-ioc-20200511.zip>

- 參考資料:

1. <https://www.us-cert.gov/ncas/alerts/AA20126A>
2. <https://www.us-cert.gov/ncas/alerts/aa20-099a>

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:20200511_01



Last update: 2020/05/12 11:18