張貼日期：2017/11/23

[資安漏洞預警通知]Android.Congur資安事件頻傳，建議各學校優先封鎖連線的惡意目的IP

主旨：Android.Congur資安事件頻傳，建議各學校優先封鎖連線的惡意目的IP

說明：

1. 從106年5月開始在學術網路中發生陸續發生Android. Congur資安事件，偵測規則為Android.Congur.Botnet或MALWARE-CNC Andr.Trojan.Congur variant outbound connection detected。根據TACERT團隊觀察，該類型資安事件的觸發率有逐漸升高之趨勢，而該類型資安事件單的中毒裝置並非只有手機，有安裝 Android 模擬器的電腦也有可能中毒。
2. 經TACERT團隊檢測，當使用者於Android系統玩一款來自韓國的手機遊戲時，會出現連至中國IP:123.56.205.151:6280之連線行為，此IP目前被Fortinet公司和AlienVault公司視為惡意IP，並列入黑名單，建議各學校遇到此類資安事件時，優先封鎖此惡意IP，封鎖該IP不影響該遊戲之使用。
3. 影響平臺：所有的Android作業系統版本
4. 建議措施：
    1. 確實使用Android平台提供的基本手機防護。
    2. 盡量避免使用Wi-Fi自動連線功能。
    3. 在下載來自第三方應用程式商店的APP前請審慎考慮。
    4. 當有程式或網頁請求授權時，請詳細閱讀其請求授權的內容。
    5. 安裝具有信譽且有效的智慧型手機防毒軟體。
    6. 請各學校封鎖連線的惡意目的IP:123.56.205.151:6280。
5. 參考資料:
    1. 個案分析-校園Android手機感染Congur病毒事件分析報告

https://portal.cert.tanet.edu.tw/docs/pdf/201711200411575799014698919071 5.pdf

---

計算機與通訊中心
網路系統組 敬啟