SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.05.27 (六) —— 2023.06.02(五)

https://stb.stpi.narl.org.tw/
資安暨智慧科技研發大樓

新OT惡意軟體COSMICENERGY直衝電網而來

近日Mandiant研究人員發現與俄羅斯相關的新OT惡意軟體COSMICENERGY，主要用來破壞關鍵基礎設施中的電力網路。Mandiant 表示，Solar Polygon於2021 年 12 月上傳到公共惡意軟體掃描實用程式。最初的用途是用來模擬電網的真實攻擊場景。惡意駭客可能重複使用這個程式碼而開發了COSMICENERGY惡意軟體。

【資料來源：資安人INFO SECURITY, 2023.05.29 】

不知名的惡意程式利用iMessage攻擊iPhone用戶

卡巴斯基本周揭露一個全新、不知名的惡意程式攻擊iPhone用戶，並企圖蒐集用戶行為資訊，一旦用戶iPhone被植入間諜軟體，就會開始蒐集iPhone中的麥克風錄音、iMessage的相片、定位及其他多種活動的資料，再送到外部伺服器上。

【資料來源：資安人INFO SECURITY, 2023.06.02 】

改良的 BlackCat 勒索軟體以閃電般的速度和隱秘的策略進行攻擊

BlackCat 勒索軟體的威脅團體提出了一種改進的變種軟體，該變種軟體優先考慮速度和隱藏，試圖繞過安全護欄並攻擊目標。BlackCat，也稱為 ALPHV 和 Noberus，是第一個被發現的以Rust 語言開發的勒索軟體。且自2021年11月以來，它已成為一個強大勒索軟體，至 2023年5月已成功攻擊350多個目標。

【資料來源The Hacker News, 2023.06.01 】

內含間諜軟體SpinOK的Android App在Google Play中下載超過 4 億次

資安廠商 Dr. Web 旗下的研究人員，近日發現一個新的 Android 惡意軟體出現在多個上架於 Google Play Store 的 App 中，合計下載次數超過 4 億次。建議下載過這些 App 的用戶，應立即刪除並進行完整的系統掃毒；此外即使在 Google 官方 Play Store，下載任何 App 前也應先閱讀評價與留言，避免下載可疑 App。

【資料來源twcertcc, 2023.06.02】