SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.02.25 (六) —— 2023.03.03 (五)

https://stb.stpi.narl.org.tw/

資安暨智慧科技研發大樓

大疆無人機操作員確切位置可以被精確定位

由於消費級無人機已從昂貴的玩具演變為戰爭工具，因此無人機安全議題也開始備受重視，研究人員針對大疆開發的無人機的無線電協議進行逆向工程，並成功發現其訊號攜帶的GPS座標並無加密可推算操作員的座標，並開源解密工具，希望開發商對於無人機安全議題能更為重視。

【資料來源：WIRED, 2023.03.02】

駭客利用配置錯誤的 Redis 伺服器進行新型加密勒索活動

Redis 作為一種高速存取與輕巧的資料庫服務廣受歡迎，因此也成為駭客的攻擊目標，研究人員通過掃描網路上能公開存取的 Redis 伺服器，發現有大量的伺服器使用不安全的設置，容易遭受惡意攻擊甚至是劫持伺服器，並於2022年以來觀察到大量攻擊事件皆有相關類似攻擊行為被發現。

【資料來源：THEHACKERNEWS, 2023.03.02 】

駭客被發現利用容器化環境竊取專有數據和軟件

研究人員發現最近開始有較多攻擊事件是透過雲端服務的容器託管服務來進行攻擊行為，並發現其中非常有趣的現象，研究人員發現駭客再進行惡意容器部屬時，會先啟用惡意挖礦行為的容器腳本來混淆受害者，在進行機敏資訊外洩的攻擊行為。

【資料來源：THEHACKERNEWS, 2023.03.02 】

CISA 發布免費的”Decider”工具以幫助進行 MITRE ATT&CK 參照

美國網絡安全與基礎設施安全局 (CISA) 前陣子發布了MITRE ATT&CK 實踐指南，引導各大機關企業能準確實踐各項安全指標，最近又發表了新的安全工具，可以讓各大企業在遭受攻擊行為時能快速生成報告，告知用戶目前正遭受MITRE ATT&CK 矩陣中的哪種行為，可加速事件調查與分析，防止事件擴散。

【資料來源：BLEEPINGCOMPUTER, 2023.03.02 】