SHALUN
CYBER SECURITY HUB

資安週報

2022.08.20(六) —— 2022.08.26(五)

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

駭客控制了退役衛星用來播放電影

於DEF CON大會上研究人員展示了透過入侵並接管已經退役的衛星，並利用該衛星發送電影的訊號，甚至能任意播放任何內容；研究人員也揭露入侵衛星的手法，僅需利用價值300美元的Hack RF工具搭配特定的無線波長訊號就能劫持衛星的訊號進而接管衛星。

【資料來源： CYBERSECURITYNEWS, 2022.08.22】

超過20萬名用戶下載的Google Chrome 瀏覽器插件Internet 下載管理器是假的

Internet Download Manager 是Tonec公司開發的下載工具，能夠下載網路上的影片圖片等各式檔案，但從2019年開始Chrome上的瀏覽器插件市集開始出現該工具的多種不同的詐欺版本，會在瀏覽器中顯示廣告甚至會劫持瀏覽器的搜尋結果，請用戶安裝插件時須格外小心。

【資料來源： CYBERSECURITYNEWS, 2022.08.25】

駭客濫用原神遊戲的反作弊系統來關閉防毒軟體

趨勢科技發現最近有駭客利用熱門遊戲原神在執行中會啟用防作弊偵測，透過注入惡意程式碼來使該偵測程式關閉防毒軟體進而執行其他惡意程式，屬於非常新的攻擊手法。

【資料來源： TRENDMICRO, 2022.08.24】

駭客採用 Sliver 控制框架作為 Cobalt Strike 的替代品

最近許多資安業者發現駭客組織逐漸棄用Cobalt Strike，因為該工具已被各大資安設備能夠輕鬆偵測並識別攻擊，因此駭客組織開始轉向使用其他控制框架如Sliver、Brute Ratel等，建議可以開始研究其他種控制框架的特徵，用以提早偵測威脅。

【資料來源： BLEEPINGCOMPUTER, 2022.08.25】