SHALUN
CYBER SECURITY HUB

資安週報

2022.08.06(六) —— 2022.08.12(五)

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

使用 25 美元的 Modchip 成功入侵Starlink

研究人員在black hat大會上發表最新研究，利用搭載故障注入技術的微控制器，並將其植入Starlink 天線之後就會繞過系統安全機制並可執行任意程式碼，藉此取得ROOT權限，硬體成本僅需25美元。

【資料來源： Threat Post, 2022.08.11】

專家在 PyPI 上發現 10 個用於竊取開發者數據的惡意套件包

研究專家在python的套件庫中發現了10個惡意套件包，用於竊取開發者的各項數據如環境數據或使用者憑證等資料，這些惡意套件包命名都與熱門套件相似，藉以混淆開發者使其安裝，希望開發者們安裝套件之前需再三檢查。

【資料來源： SecurityAffairs, 2022.08.10】

暗網中對於企業網絡存取權限需求依然旺盛，但銷售額卻是逐漸下

由於世界各國政府對於駭客組織的執法越來越嚴厲，因此駭客組織對於目標的選擇越來越謹慎，因此對於大型企業的存取權限在拍賣市場上越來越少人購買，也發現駭客組織開始將中型企業選為目標，藉此在風險與報酬中取得平衡。

【資料來源： BLEEPINGCOMPUTER, 2022.08.11】

汽車供應商在 2 週內遭到 3 個勒索軟體組織的入侵

一家汽車供應商的系統遭到破壞，三個不同的勒索軟體組織在兩週內對系統文件進行了加密，其中兩次不同組織的攻擊發生在短短兩個小時內，三個組織都是使用相同的漏洞攻破系統取得權限後用不同的方式植入後門，並針對不同的勒索軟體進行互相干擾與刪除彼此足跡，讓災害復原與數位鑑識過程都受到相當大的挑戰。

【資料來源： BLEEPINGCOMPUTER, 2022.08.11】