SHALUN
CYBER SECURITY HUB

資安週報

2022.10.08 (六) —— 2022.10.14 (五)

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

資安暨智慧科技研發大樓

CSA 提供了由中國國家支持的黑客利用的常見漏洞

CSA 和 NSA 與 FBI 聯合發布了關於2020年以來，中國的駭客組織經常利用的已知漏洞清單，中國駭客組織經常利用這些漏洞攻破企業與關鍵基礎設施，希望各大企業與機關能檢視環境內是否含有相關漏洞，盡早修補避免駭客入侵遭受更大的危害。

【資料來源：CYBERSECURITYNEWS, 2022.10.08】

偽造的 Windows Defender 警報被武器化以執行欺詐交易

研究人員發現最近一種新型態的釣魚網站攻擊，進入釣魚網站時會彈出 Windows Defender 警報視窗，騙取使用者點擊掃描或是執行下載安裝惡意程式等手法，若成功點擊執行會竊取信箱跟登入憑證或信用卡等資訊。

【資料來源： CYBERSECURITYNEWS, 2022.10.13】

新的 Alchimist 攻擊框架針對 Windows、macOS、Linux

研究人員發現幾種新型態的後滲透C2框架，類似於中國駭客組織常用的 Manjusaka C2框架，擁有更強的偵測規避機制與Golang編寫的可快跨平台特性，並且由於框架尚未被標註因此大多數防護軟體無法識別。

【資料來源：BLEEPINGCOMPUTER, 2022.10.13】

咖啡因，一種新的網絡釣魚即服務工具包

研究人員發現一種新型態的釣魚即服務平台，該平台不像以往的釣魚及即服務平台都潛藏於暗網或駭客工具交易網站，該平台可透過任何郵件進行註冊並使用，非常的親民，並且提供大量範本與工具包可供訂閱使用，用以竊與 Microsoft365憑證。

【資料來源： SECURITYAFFAIRS, 2022.10.11】