SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2022.11.26(六) —— 2022.12.02(五)

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

資安暨智慧科技研發大樓

▶ 中國駭客使用 USB 設備實體攻擊菲律賓

Google的研究人員發現，疑似中國的駭客組織正在對於東南亞、美國、歐洲、亞太及日本地區進行惡意攻擊行為，最近被捕捉到的攻擊行為是透過投放實體USB來誘使被害人安裝惡意程式，但較為特別的是研究人員分析該攻擊腳本發現惡意程式能針對氣隙系統進行攻擊竊取機密。

【資料來源：THEHACKERNEWS., 2022.11.30】

▶ 研究人員找到了惡意 NPM 庫可以逃避漏洞檢測的方法

網絡安全公司 JFrog 的新發現表明，針對 npm 生態系統的惡意程式可以利用 npm 命令行界面 (CLI) 工具中的”意外行為”來逃避安全檢查，安裝包遵循某些版本格式時，安全建議不會顯示，從而導致可能直接或通過依賴項將嚴重缺陷引入其係統的場景。

【資料來源： THEHACKERNEWS, 2022.11.30】

▶ 狡猾的駭客使用“域老化”來逃避安全偵測平台

域老化是指威脅行為者註冊域並等待數年才能使用它們，以期繞過安全平台偵測技術，這種技術的工作原理是，長期未參與惡意活動的舊域在 Internet 上贏得信任，使它們不太可能被安全工具標記為可疑，進而騙取使用者信任。

【資料來源： BLEEPINGCOMPUTER, 2022.11.30】

▶ 現代汽車行動應用程式漏洞允許駭客遠端解鎖、啟動汽車

安全研究人員發現了關於手機應用程式的安全問題，並在其他製造商（豐田、本田、FCA、日產、Acura 和 Infinity）使用的 SiriusXM “智能汽車”平台中探索了類似的攻擊面，這些平台允許他們“遠程解鎖、啟動、定位、閃爍並按喇叭”但目前已修復漏洞，請廣大使用者請注意要更新應用程式。

【資料來源： BLEEPINGCOMPUTER, 2022.12.01】