SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2022.12.24(六) —— 2022.12.30(五)

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

資安暨智慧科技研發大樓

ChatGPT 是威脅還是工具？

有鑑於最近自然語言 AI 發展開始出現許多功能強大的 AI 模型，可以讓使用者產生出非常多的應用，該篇研究表明如何利用最近當紅的語言模型 ChatGPT 來進行一些惡意攻擊的演練過程，讓使用者了解該語言模型可能帶來的風險。

【資料來源：SYSTEMWEAKNESS, 2022.12.26】

一種新型的攻擊 EarSpy 透過運動傳感器竊聽 Android 手機

研究人員開發了一種針對 Android 設備的竊聽攻擊，可以在不同程度上識別來電者的性別和身份，甚至可以辨別私人談話，該攻擊手法通過捕獲移動設備中耳機揚聲器的混響引起的運動傳感器接收共振來達成竊聽。

【資料來源：BLEEPINGCOMPUTER, 2022.12.27】

任天堂修補了一個可能讓駭客“完全接管控制台”的安全漏洞

任天堂悄悄修補了一個安全漏洞，駭客可以利用該漏洞訪問受感染的 Switch、3DS 和 Wii U 遊戲，他允許攻擊者在進行特定遊戲線上配對時，配對到該攻擊者個玩家將會觸發攻擊，並在受害者控制台中遠程執行任意程式碼。

【資料來源：EUROGAMER, 2022.12.28】

APT 駭客轉向惡意 Excel 加載項作為初始入侵向量

高級持續性威脅 (APT) 攻擊者和商品惡意軟件家族越來越多地使用 Excel 加載項 (.XLL) 文件作為初始入侵向量，針對該特殊的EXCEL檔案類型多數的防護設備仍無法辨識，因此受到駭客組織的青睞開始大量採用。

【資料來源： THEHACKERNEWS, 2022.12.28】