SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.03.11 (六) —— 2023.03.17 (五)

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

資安暨智慧科技研發大樓

將公司機密數據複製到 ChatGPT 中的風險

Cyberhaven Labs 的產品檢測到每 100,000 名員工有 3,381 次將公司數據複製貼上到 ChatGPT 的嘗試情況，研究專家呼籲向聊天機器人模型提供了公司數據，可能會使機器人公開分享基於機密數據構建出的資訊，須小心謹慎。

【資料來源：SECURITYAFFAIRS, 2023.03.13】

ChatGPT 建構的多型態惡意軟體能夠繞過端點檢測過濾器

研究人員使用 AI 語言模型創建了一種會自動變換型態的鍵盤側錄器的惡意程式，每次調用鍵盤記錄器時都會編寫一個獨特的 python 腳本。這使得它具有 “多態性” 並且 EDR 更難以偵測它。

【資料來源：CYBERSECURITYNEWS, 2023.03.15】

嚴重的 Microsoft Outlook 錯誤 PoC 表明利用它是多麼容易

研究人員分享了利用 Windows 版 Microsoft Outlook 關鍵漏洞 (CVE-2023-23397) 的技術細節，該漏洞允許黑客通過接收電子郵件遠端執行程式並竊取雜湊密碼。

【資料來源：BLEEPINGCOMPUTER, 2023.03.15】

微軟工程師在系統註冊失敗後為客戶 “破解” Windows

南非自由技術專家以 200 美元購買正版 Windows 10後註冊失敗，聯繫官方工程師後發現，工程師使用繞過 Windows 激活過程的非官方工具 “破解” 他的電腦時大吃一驚，並且經查證後該行為常見於售後處理方法之一。

【資料來源：BLEEPINGCOMPUTER, 2023.03.16】