SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.02.18 (六) —— 2023.02.24 (五)

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

資安暨智慧科技研發大樓

勒索組織幫助受駭者調整贖金以便保險公司支付贖金費用

HardBit 勒索軟件組於 2022 年 10 月首次出現在威脅情資中，但與其他勒索軟件操作不同的是該組織並未進行多重勒索，反而積極尋求與受害者和解，並要求受害方提供保險文件以調整金額配合保險公司順利支付贖金。

【資料來源：SECURITYAFFAIRS, 2023.02.21】

研究人員使用 ChatGPT 構建惡意軟件繞過 EDR 並獲得漏洞賞金

安全專家開發了一種方法來誘騙著名的 AI Chatbot ChatGPT 創建惡意程式，並且安全團隊幾乎沒有開發惡意程式的經驗，在測試期間團隊無意間發現 AI 提供的語法能夠能夠繞過 EDR 供應商的一項防禦措施，回報供應商後還得到了漏洞賞金。

【資料來源：CYBERSECURITYNEWS, 2023.02.22】

駭客使用偽造的 ChatGPT 應用程序來推送 Windows、Android 惡意軟件

攻擊者正在利用 OpenAI 的 ChatGPT 聊天機器人的大流行來傳播用於 Windows 和 Android 的惡意軟體，或將毫無戒心的受害者引導至網絡釣魚頁面，騙取受害者繳納高額使用費或是騙取個人資訊，請廣大使用者須小心。

【資料來源：BLEEPINGCOMPUTER, 2023.02.22】

如何用人工智能生成的聲音破解銀行帳戶語音認證

近年來銀行體系開始導入語音認證方式，能夠讓用戶輕鬆驗證並自動認證，但研究人員發現語音認證系統可能無法辨識真人語音或是 AI 產生的語音，並加以測試且成功通過驗證登入帳戶，研究人員呼籲語音認證的弊端與該方法應用於詐騙的高可能性，請大眾需多注意。

【資料來源：VICE, 2023.02.24】