SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

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

資安暨智慧科技研發大樓

2023.04.01 (六) —— 2023.04.07 (五)

▶ 使用 ChatGPT 提示構建了一個無法檢測到的零日漏洞

研究人員透過誘導 ChatGPT 產生部分功能程式碼的部分，將各種部分的程式碼組合起來研湊成一種難以辨識的惡意程式，還可以任意添加混淆與規避的函數來使其更加隱匿，最終完成的惡意程式甚至能讓 VirusTotal 無法檢測出來。

【資料來源：FORCEPOINT, 2023.04.04】

▶ Telegram 現在是販售網路釣魚工具和服務的最佳選擇

卡巴斯基的研究人員觀察到一種趨勢，Telegram 已成為網路釣魚機器人和工具創建者的銷售與服務平台，有經驗的釣魚集團可以開發各式自動化機器人，產生釣魚攻擊中需要的各式服務與各式認證機制，過程可以完全自動化大幅降低成本與暴露的風險，因此釣魚業務目前由暗網開始大量轉移至 Telegram 並蓬勃發展中。

【資料來源：BLEEPINGCOMPUTER, 2023.04.06】

▶ 小偷如何利用汽車網絡總線偷車

汽車安全專家表示，他們發現了一種偷車方法，該方法通過車頭智能大燈的線路可以直接訪問車輛的系統控制總線，該攻擊可以稱作 CAN 注入攻擊，竊賊通過連接大燈進而進入汽車控制總線，並發送偽造訊息騙取控制器誤以為是汽車的智能鑰匙訊號發送開鎖請求，進而成功啟動車輛並將車輛開走。

【資料來源：THEREGISTER, 2023.04.06】

▶ “BEC 3.0” 於稅收季節 QuickBooks 網絡攻擊一起出現

電子商務詐騙攻擊(BEC)的攻擊行為一直在進化，研究人員發現攻擊者的攻擊策略已經進化到一個新的型態，可以稱為 BEC 3.0，攻擊者開始利用大量合法的SaaS服務或各式合法服務來取得合法信箱，來規避各種檢測技術，並搭配大量新型腳本來誤導受害者，僅憑目前的檢測技術與自然語言偵測方式已經沒辦法防止這類型攻擊發生，建議各團隊還是以強化驗證機制與安全意識較能防止攻擊發生。

【資料來源：DARKREADING, 2023.04.07】