SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.01.14 (六) —— 2023.01.19 (四)

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

資安暨智慧科技研發大樓

研究人員發現了 3 個向開發者系統傳播惡意程式的 PyPI 包

研究人員發現一名為Lolip0p的駭客已將三個惡意包上傳到 Python 包索引 (PyPI) 存儲庫，意圖將惡意軟件投放到受感染的開發人員系統上。該惡意程式被 VirusTotal 標記為資訊竊取程式，它還能夠刪除其他文件。

【資料來源：THEHACKERNEWS, 2023.01.17】

男子利用暗網販售的信用卡詐騙數千人

一名紐約男子從暗網市場購買了數千份信用卡和金融卡數據，並用這些數據偽造信用卡，並透過這些假信用卡大量購買禮物卡或各式奢侈品，再將這些物品出售以換取現金，請廣大使用者經常注意銀行應用程式的通知，也請避免購買售價過低的禮物卡，避免遭害。

【資料來源：BLEEPINGCOMPUTER, 2023.01.18】

透過 ChatGPT 創建惡意軟體的混淆版

研究人員發現使用 ChatGPT 創建的惡意軟體可以輕鬆繞過安全產品，並且攻擊者僅需要付出很少的成本就能使分析師的分析過程難度驟增，研究人員通過 ChatGPT來生成惡意程式的不同語言版本或是加入混淆函數使得程式難以解析，效果非常好。

【資料來源：INFOSECURITY-MAGAZINE, 2023.01.18】

Netcomm 和 TP-Link 路由器中發現的嚴重安全漏洞

Netcomm 和 TP-Link 路由器中的安全漏洞已被公布，其中一些可以被武器化以實現任意遠程代碼執行(RCE) 。研究人員表明攻擊者可以首先獲得對受影響設備的未授權訪問權限，然後使用這些設備作為新的入口點獲得對其他內部網絡的訪問權限，危害非常大。

【資料來源：THEHACKERNEWS, 2023.01.18】