SHALUN
CYBER SECURITY HUB

# 資安週報

沙崙資安基地

2023.01.07 (六) —— 2023.01.13 (五)

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

資安暨智慧科技研發大樓

## AI 生成的網絡釣魚電子郵件變得更有說服力

研究人員展示了如何使用提示方法來讓語言AI製作魚叉式網絡釣魚電子郵件、社交媒體騷擾、虛假新聞故事和其他類型的內容。透過語言AI協助攻擊者可以在短時間內大量生成具有高度擬真內容的釣魚信件來進行鯛魚攻擊行動，並且使得辨別攻擊的成本越趨升高。

【資料來源：THEREGISTER, 2023.01.11】

## 內部人員透過暗網販售能夠 Telegram 內部服務器連線管道

安全團隊在暗網上發現了一家商店，聲稱內部人員可以訪問 Telegram 服務器。對於 20,000 美元的不可協商價格，商家聲稱可以“通過他們的員工”不受阻礙地訪問 Telegram 服務器；換句話說，該連線是由內部人士洩漏。

【資料來源：SAFETYDETECTIVES, 2023.01.09】

## 亞馬遜上的安卓電視盒預裝了惡意軟件

一位加拿大系統管理員發現，從亞馬遜購買的 Android 電視盒預裝了持久的、複雜的惡意軟件，並嵌入其固件中。該管理員認為設備上安裝的惡意軟件是“CopyCat”，這是Check Point 於 2017 年首次發現的一種複雜的 Android 惡意軟件。

【資料來源：BLEEPINGCOMPUTER, 2023.01.12】

## RAT 組織的惡意程式攻擊活動試圖使用多語言文件規避檢測

在最新的 RAT 攻擊活動中觀察到的自 2018 年以來一個值得注意的案例是將 JAR 和 MSI 格式組合中作為 MSI 執行，也可以作為 JAR 文到一個文件中。這種雙重格式允許它們在 Windows件由 Java 運行時執行，並且JAR 不是可執行文件，因此它們不會受到防病毒工具的嚴格檢查。

【資料來源： BLEEPINGCOMPUTER, 2023.01.12】