SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2022.11.05 (六) —— 2022.11.11 (五)

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

資安暨智慧科技研發大樓

駭客濫用微軟Dynamics 365 Customer Voice發送釣魚連結

Dynamics 365 Customer Voice是一款微軟的產品，它可用於客戶滿意度調查，以及透過電話與客戶互動，駭客偽裝成Dynamics 365調查功能並發送惡意電子郵件，通知受害者有新的語音郵件訊息，建議使用者在點擊陌生連結時要保持高度懷疑。

【資料來源：HACKREAD, 2022.11.05】

名為StrelaStealer的惡意軟體正在竊取 Outlook、Thunderbird 帳戶

DCSO CyTec的分析師於2022年11月上旬首次發現了新的惡意軟體StrelaStealer，目標為講西班牙語的用戶，該惡意軟體試圖從瀏覽器、加密貨幣錢包應用程式、雲遊戲應用程式等竊取數據，由於該惡意軟體使用西班牙語誘餌進行傳播，因此它可能被用於高度針對性的攻擊。

【資料來源： BLEEPINGCOMPUTER, 2022.11.09】

Amadey Bot惡意軟體被用於部署LockBit 3.0勒索軟體

駭客透過Amadey Bot惡意軟體安裝LockBit勒索軟體，且正在通過兩種方式分發，一種是使用惡意Word文檔文件，另一種則是偽裝成Word檔案圖示(icon)的可執行檔案，研究人員發現Amadey Bot目前正透過Kakao Talk進行發送惡意軟體。

【資料來源： SECURITYAFFAIRS, 2022.11.09】

PyPI上的圖片後面隱藏惡意程式代碼

PyPI是Python的正式第三方軟體套件的軟體存儲庫，研究人員在存儲庫中發現了一個新的惡意程式，它可以使用隱寫技術隱藏圖像中的惡意代碼，並通過Github上的開源項目感染用戶。

【資料來源： THEHACKERNEWS, 2022.11.10】