SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.02.11 (六) —— 2023.02.17 (五)

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

資安暨智慧科技研發大樓

殺豬騙局發展迅速

殺豬騙局起源於中國，基本上將受害者養肥，然後拿走他們所有的東西。這些騙局通常是加密貨幣計劃，但它們也可能涉及其他類型的金融交易。研究人員發現在推特上開始大量發生陌生人新加好友後開始推薦加密貨幣，還利用友情或戀愛等議題騙取受害者信任，詐騙手法越來越多元。

【資料來源： WIRED, 2023.02.13】

PYbot DDoS 惡意軟體偽裝成 Discord Nitro 產生器進行派送

Discord 是近年來較為流行的通訊軟體，因此被駭客盯上利用免費的Discord代幣 Nitro 來騙取受害者安裝後門程式，進而使得設備遭受控制，當感染 PYbot 時，用戶系統可以用作 DDoS 機器人，接收來自威脅參與者的命令以對特定目標執行 DDoS 攻擊。

【資料來源： AHNLAB, 2023.02.15】

Mirai V3G4 殭屍網絡利用 13 個漏洞攻擊物聯網設備

一種名為 V3G4 的 Mirai 變體試圖利用多個漏洞在 2022 年 7 月至 2022 年 12 月期間大量感染物聯網裝置，若裝置被成功感染並執行後門程式後，機器人會發送文字訊息 xXxSlicexXxxVEGA 到 C&C 主機，建議可以參考文章內容盤點公司內資產有沒有受到相關漏洞影響避免遭受攻擊。

【資料來源： SECURITYAFFAIRS, 2023.02.16】

研究人員劫持了具有數百萬下載量的流行 NPM 包

illustria 的研究團隊發現某個每週下載量接近 400 萬的 npm 包可以受到帳戶接管攻擊，便嘗試利用域名劫持與帳號恢復功能嘗試去劫持該 npm 包，並成功接管此帳號，成功接管後可進行任意操作包含修改套件包內容埋入後門等，研究人員表明通過獲取過期的域名來接管流行的套件包是多麼容易。

【資料來源： THEHACKERNEWS, 2023.02.16】