SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.02.04 (六) —— 2023.02.10 (五)

https://stb.stpi.narl.org.tw/
資安暨智慧科技研發大樓

安全工具 binwalk 中存在嚴重的安全漏洞

安全分析工具Binwalk本身存在路徑遍歷漏洞，可能導致遠端程式碼執行(RCE)，對運行過時版本的用戶存在安全風險，並且研究人員還發現了漏洞也影響其他文件系統提取器（即 ubi_reader、Jefferson、yaffshiv 項目）產生不同程度的CVE漏洞。

【資料來源： PORTSWIGGER, 2023.02.03】

公佈了 Killnet 的 DDoS 機器人的代理 IP 列表

Killnet 是一個親俄組織，以攻擊對俄羅斯不友好國家的醫院和其他關鍵基礎設施而聞名，SecurityScorecard 發布了一份代理 IP 列表，以幫助阻止 Killnet DDoS 機器人，可嘗試將該 IP 清單加入防禦系統，阻止遭後DDoS攻擊的機會。

【資料來源： HACKREAD, 2023.02.08】

駭客入侵了 Reddit 並竊取原始程式碼和內部數據

駭客針對 Reddit 員工進行網絡釣魚，釣魚網站的登入頁面假冒成內部網站。該站點試圖竊取員工的憑據和雙因素身份驗證令牌並成功騙取到一名員工輸入資料，攻擊者獲得了對一些內部文檔、程式碼以及一些內部儀表板和業務系統的訪問權限。

【資料來源： BLEEPINGCOMPUTER, 2023.02.09】

破解 VMProtect 的最新技巧

VMProtect 是一種商業用的程式封裝工具，具有高級反編譯和 VM 檢測功能。它還採用了程式碼虛擬化來將程式碼轉化，使得產品被逆向分析後很難確定程式碼的功能與邏輯，但研究人員依然發現破解方法使得原始程式碼依然能有效的被還原。

【資料來源： CYBER.WTF, 2023.02.09】