SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.04.15 (六) —— 2023.04.21 (五)

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

資安暨智慧科技研發大樓

Elon Musk 聲稱聯邦調查局可以“完全訪問”推特上的私人信息

馬斯克在接受採訪時描述說多年以來美國政府都有權利取得推特上的所有資料，根據記者取得的資料，美國中央情報局還參與推特的言論內容審查，還刻意屏蔽部分用戶。

【資料來源：NYPOST, 2023.04.17】

攻擊者使用久未更新的 WordPress 插件植入後門

研究人員根據攻擊趨勢發現開始有大量攻擊者使用一種 WordPress 插件存儲庫可以下載到的一個插件 Eval PHP ，該插件在過去十年沒有更新被認為是廢棄插件，攻擊者利用該插件來建立後門，並且由於為合法插件因此攻擊行為相當隱蔽難以偵測，並且非常容易能夠重複感染，後門被移除後僅需裝回插件即可再次感染。

【資料來源：BLEEPINGCOMPUTER, 2023.04.20】

當ChatGPT中的PT指的是滲透測試時

研究人員展示如何透過旁敲側擊的方式，繞過 ChatGPT 的部分限制，使其能夠幫助滲透測試的各個階段，研究人員展示了從搜集目標網域資訊甚至是提供正確掃描目標的方法，都能得到正確的 AI 回答，該過程可以幫助廣大的滲透測試執行者。（本篇文章需註冊才能閱讀，可使用10分鐘信箱註冊）

【資料來源：HAKIN9, 2023.04.20】

“GhostToken” 打開永久感染 Google 賬戶的大門

研究人員發現 Google 雲平台(GCP)中的一個安全漏洞，該漏洞可能允許網路攻擊者在受害者的 Google 帳戶中可以創建一個隱藏並且不可刪除的惡意應用程式，該惡意程式無法於儀表板或其他地方查看，使得該帳戶會永久性的處於感染狀態並且無法偵測得到惡意程式。

【資料來源：DARKREADING, 2023.04.21】