SHALUN
CYBER SECURITY HUB

資安週報

2022.07.23(六) —— 2022.07.29(五)

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

瀏覽器的自動填寫密碼可能會通過跨站腳本攻擊(XSS)盜走

研究人員發現一個可以利用大部分瀏覽器都有的自動填寫帳號密碼功能透過跨站腳本攻擊來竊取自動填寫的帳號密碼並上傳到駭客架設的惡意伺服器，研究人員透過針對市面上大部分的主流瀏覽器進行模擬攻擊並成功取得帳號密碼，並分析漏洞發生原因。

【資料來源： Gosecures, 2022.07.29】

來越多駭客使用 WebAssembly 編譯的惡意挖礦程式來逃避檢測

WebAssembly(Wasm)作為一個可以在瀏覽器上面執行C/C++/Rust編譯程式的語言，在近年來越來越受到駭客的喜愛，由於Wasm的流量規則難以被目前的防毒與防護機制偵測，因此越來越多的駭客用於入侵網站植入惡意挖礦程式。

【資料來源： The Hacker News, 2022.07.26】

駭客入侵Microsoft SQL伺服器並安裝代理服務來竊取企業網路頻寬

最近的研究發現駭客利用Microsoft SQL伺服器的漏洞或弱密碼等方式入侵取得權限後，於伺服器上安裝代理服務將伺服器當作網路流量的跳板，並透過該代理服務提供其他人使用該企業的網路頻寬，藉此盈利，獲利金額可以高達每月數千美金。

【資料來源： BLEEPINGCOMPUTER, 2022.07.28】

駭客使用 Google Chrome 插件暗中竊取電子郵件

新研究發現北韓駭客正在進行大規模的社交工程與釣魚攻擊活動，使用的方式是透過瀏覽器的擴充插件來竊取電子郵件，駭客通過精心設計惡意插件誘使使用者下載安裝後就會感染病毒，並通過該病毒程式入侵使用者的公司或機關網路。

【資料來源： BLEEPINGCOMPUTER, 2022.07.28】