SHALUN
CYBER SECURITY HUB

資安週報

2022.06.11 (六) —— 2022.06.17(五)

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

▶ #資安工具 [Metasploit 更新了6.2.0版，新增了一個竊取憑證功能、改進了SMB支持功能]

Metasploit 是一個由Rapid7開發的滲透測試框架，該框架通常用作滲透測試活動中的重要工具，是當今網絡安全專業人員使用的最受歡迎的工具之一。

【資料來源： BLEEPINGCOMPUTER, 2022.06.13】

▶ #惡意軟體 [新的勒索軟體BlackCat 出現，針對未修補的Microsoft Exchange 服務器]

BlackCat被認為是第一個用 Rust 編寫的跨平台勒索軟件之一，這體現了攻擊者正在轉向不常見的程式語言試圖逃避檢測的趨勢。

【資料來源： Microsoft, 2022.06.13】

▶ #安全漏洞 [工業控制系統中的漏洞讓攻擊者遠程解鎖門]

Carrier 的工業控制系統中檢測到8個零日漏洞，如果被利用，攻擊者可以完全控制系統，包括攻擊者遠程操縱門鎖的能力。

【資料來源：HACKREAD, 2022.06.13 】

▶ # 後門程式 [PyPI 中的 “keep” 套件包錯誤地包含了一個密碼竊取器]

某些版本中的keep、pyanxdns和api-res-pyrequest套件被發現其中的依賴套件requests因拼寫錯誤或遭受攻擊而變成request，該request套件含有後門與鍵盤側錄器。

【資料來源： BLEEPINGCOMPUTER, 2022.06.12】