SHALUN
CYBER SECURITY HUB

資安週報

2022.05.23 (一) —— 2022.05.27 (五)

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

俄羅斯殭屍網路(Fronton)對外進行惡意社交媒體宣傳活動

Fronton為一個Web 儀表板，可部署大規模的社交媒體趨勢文章。系統所建立的惡意社交媒體訊息，被稱為 Инфоповоды(newsbreaks)，並使用VPN 或Tor匿名網路與前端服務進行通訊，並使用大量已受感染之物聯網設備(殭屍網路)，進行DDoS與訊息攻擊活動。

【資料來源： The Hacker News, 2022.05.23】

容器化開發(Containers)的資訊安全風險

容器化(Containers)開發，已成為系統開發與IT維運(DevOps)的基本技術與趨勢，但該技術所帶來的安全風險無法被經易查覺，若無法有效識別風險，組織將容易受到相關網路攻擊，請系統與IT人員注意相關風險與攻擊。

【資料來源： The Hacker News, 2022.05.23 】

駭客偽造Windows系統，並利用Cobalt Strike手法進行攻擊

駭客使用偽造的Windows 及利用已修補之遠端服務漏洞，讓惡意的後門程式(Cobalt Strike)可感染目標設備，而資訊安全人員亦使用相關驗證漏洞機制來檢測單位內部防禦措施，並推動及執行系統安全更新。

【資料來源： BLEEPINGCOMPUTER, 2022.05.23】

Chaos Ransomware Builder已出現新的變種勒索軟體Yashma

Chaos出現最新的勒索變種軟體(Yashma)。Chaos為製作勒索軟體的工具並於2021年6月9日出現於地下論壇中，而Yashma為Chaos的第六版勒索軟體工具，有心人士可使用該惡意工具開發勒索軟體病毒。

【資料來源： The Hacker News, 2022.05.24】