SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.04.29 (六) —— 2023.05.12(五)

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

資安暨智慧科技研發大樓

Microsoft 5 月安全更新解決40個漏洞，包括在攻擊中被積極利用的零日漏洞

微軟5月的安全更新解決了40個漏洞，包括兩個在攻擊中被積極利用的零日漏洞。這些缺陷會影響Microsoft Windows和Windows組件、辦公室和辦公室組件、Microsoft Edge(基於Chromium)、共享服務器、視覺工作室、系統內部和微軟團隊。已解決的漏洞中有7個被評為嚴重，31個被評為重要。

【資料來源： SECURITYAFFAIRS, 2023.05.10】

Royal勒索軟體組織擴展到威脅 Linux、VMware ESXi

Royal 駭客軟體組織是由Conti的前成員所組成，自去年成立以來，發動了數起對關鍵基礎設施和醫療保健團體的攻擊。最近，更擴展成脅到Linux和VMware ESXi的作業系統。Palo Alto Networks Unit 42部門發布的分析中指出，該組織團體最近推出了一種針對ESXi/Linux的加密勒索變種軟體。

【資料來源： DARKREADING, 2023.05.09 】

新勒索軟件”CACTUS “利用 VPN 漏洞滲透網絡

資安研究人員指出有一種名為CACTUS的新型勒索體變種，可以利用VPN設備中的已知缺陷來獲得對目標網路的初始訪問權限。自 2023 年 3 月以來，該勒索軟體一直以大型公司企業為目標，且在攻擊時會採用雙重勒索策略，並在資料加密前竊取敏感數據。

【資料來源The Hacker News, 2023.05.09 】

前美國國土安全部長首度訪臺，分享從國土安全部學到如何降低風險的經驗

曾擔任5年國土安全部(DHS)部長暨美國加州大學柏克萊分校政治安全中心創辦人Janet Napolitano首度訪臺，Janet Napolitano在5月9日舉辦的臺灣資安大會2023中，以當年國土安全部(DHS)在全美推廣的"See Something Say Something”(一看到、就通報)活動為例，通報可疑的人事物可以降低實體社會面臨的風險，也同樣適用於網路環境。

【資料來源：iThome, 2023.05.10】