2022/05/02~05/06 資安週報

變種勒索軟體(AvosLocker)將影響系統安全防護

AvosLocker為變種勒索軟體，從未修補之安全漏洞入侵，並停止系統相關防護(如:Windows update、defender)而躲避防護及檢測，此外該勒索軟體亦可使用Nmap-NSE Script掃描多個端點找尋Log4j漏洞，並傳遞惡意腳本。

【資料來源：The Hacker News, 2022.05.02】

TLStorm 2.0漏洞將影響Aruba及Avaya網路交換機

TLStorm 2.0為Aruba 及Avaya的網路交換機安全漏洞，駭客透過該漏洞可遠端竊取目標主機資料，受影響型號Avaya ERS3500、ERS3600、ERS4900、ERS5900， Aruba 5400R、3810、2920、2930F、2930M、2530、2540，請儘速更新韌體。

【資料來源：The Hacker News, 2022.05.03 】

F5防火牆有允許未經身份認證人員連入設備之系統漏洞

F5發佈系統安全漏洞，該漏洞存在於iControl REST中，允許惡意人員發送未公開的連線請求，並繞過BIG-IP中的iControl REST 驗證，以取得系統操作權限，請儘速更新韌體。

【資料來源：BLEEPINGCOMPUTER, 2022.05.04】

駭客劫持英國NHS電子郵件帳戶，竊取Microsoft登入訊息

英國國家衛生單位(NHS)多名員工電子郵件帳號被利用，並進行對外進行網路釣魚，其中更竊取Microsoft之登錄信息，宜請收發信件時須防範社交工程相關信件。

【資料來源：BLEEPINGCOMPUTER, 2022.05.04】