SHALUN
CYBER SECURITY HUB

資安週報

2022.10.15(六) —— 2022.10.21(五)

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

PHP版本的竊密軟體Ducktail以偷取Facebook帳號為目標

WithSecure研究人員發現一款使用PHP版本撰寫的惡意軟體Ducktail，該惡意軟體早期使用.NET Core撰寫，駭客將惡意軟體隱藏在破解版Office、免費版遊戲及色情影片當中，引誘使用者下載並執行，當惡意軟體執行後會在背景中竊取瀏覽器的Facebook帳密資料及敏感資訊。

【資料來源： SECURITYAFFAIRS, 2022.10.15】

偽裝成Windows更新且難以被檢測的PowerShell後門程式

SafeBreach研究人員警告，一種新穎的攻擊方法且難以被檢測的PowerShell後門程式，該後門程式假冒成LinkedIn工作申請Word文件，此惡意word文件包含巨集程式，下載後的script程式會自我註冊成Windows Update行程的一部份，偽裝成Windows合法排定任務而避過安全工具的檢查。

【資料來源： ITPRO, 2022.10.19】

網路儲存伺服器NAS公司Synology修補其產品嚴重漏洞

Synology的NAS作業系統 DSM(DiskStation Manager)共有四個漏洞，其中CVE-2022-27624、CVE-2022-27625和CVE-2022-27626(CVSS評分：10），駭客可利用該漏洞來執行任意命令，請盡快將設備升至7.1.1-42962-2或更高版本以解決這些漏洞。

【資料來源： PENETRATIONTESTING, 2022.10.20】

Abode智慧家庭安全套件中存在漏洞可能允許駭客關閉攝像頭

Cisco Talos最近在Abode安全套件中發現了幾個漏洞，其中包含駭客可修改用戶登錄密碼、將程式碼注入設備、操縱敏感設備設置及關閉系統，Cisco向Abode 披露了該漏洞，並在Patch發布後公開披露這些漏洞，請使用者盡快修補受影響的產品。

【資料來源： TALOS, 2022.10.20】