SHALUN
CYBER SECURITY HUB

資安週報

2022.10.01 (六) —— 2022.10.07 (五)

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

資安暨智慧科技研發大樓

駭客透過YouTube傳播惡意的Tor瀏覽器安裝程式

卡巴斯基研究人員發現名為OnionPoison的攻擊行動，正在透過中文的Youtube頻道散佈含有惡意軟體的Tor瀏覽器，Tor瀏覽器是以隱私為中心的瀏覽器，以此保護自己的身份和上網行為，值得注意的是，Tor瀏覽器在中國被禁止，這也讓駭客可以透過誘騙的方式讓受害者下載程式。

【資料來源： HACKREAD, 2022.10.05】

Android新型的間諜應用程式RatMilad

RatMilad是一款新型的Android間諜應用程式，被發現目標是針對中東地區的行動裝置，用於監視及竊取資料，且可修改已安裝應用程式的權限，甚至使用設備的麥克風錄音和竊聽房間，為確保設備資訊安全，請勿從第三方商店下載應用程式。

【資料來源： BLEEPINGCOMPUTER, 2022.10.05】

Microsoft針對Exchange Server零日漏洞提出緩解措施

Microsoft針對最新的Exchange零日漏洞ProxyNotShell更新了緩解措施，分別為CVE-2022-41040及CVE-2022-41082，目前微軟官方尚未針對此漏洞釋出更新程式，建議評估是否先行採取緩解措施。

【資料來源： BLEEPINGCOMPUTER, 2022.10.05】

高通芯片存在遠端程式碼執行漏洞影響數十億台行動裝置

高通在本月的安全公告中披露了12個影響芯片的新安全漏洞，其中兩個被評為嚴重等級，CVE-2022-25748(CVSS評分9.8)及CVE-2022-25718(CVSS評分9.1)已在2022年10月的Android安全更新中修正漏洞，請使用者儘速完成更新。

【資料來源： PENETRATIONTESTING, 2022.10.06】