SHALUN
CYBER SECURITY HUB

資安週報

2022.09.03(六) —— 2022.09.08(四)

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

Worok 駭客組織瞄準亞洲知名公司和政府

一個最近發現的駭客組織Worok專門針對亞洲的知名公司與政府機關進行針對性攻擊，研究人員發現初期針對目標會在選定的系統中使用ProxyShell 漏洞來進行初步滲透，取得權限後會進而埋入後門，並且會使用隱寫術從 PNG 文件中提取隱藏的惡意負載，企業須定期檢視系統有無可疑連線避免遭受攻擊。

【資料來源： TheHackerNews, 2022.09.06】

一種新的網路釣魚詐騙針對美國運通卡持卡人

Armorblox 研究人員發現了一項針對美國運通卡客戶的新網絡釣魚活動，使用惡意附件，其內容試圖誘使持卡人打開它，單擊消息中的鏈接後，受害者將被重定向到虛假的美國運通登錄頁面，其中包括公司的圖標和下載美國運通應用程式的連結，呼籲企業須小心社交工程攻擊，盡量不要點擊任何郵件裡的連結。

【資料來源： Securityaffairs, 2022.09.04】

暗網中出現繞過 MFA的 EvilProxy 網絡釣魚即服務

Resecurity最近發現了一種新的網絡釣魚即服務 (PhaaS)，稱為 EvilProxy ，在暗網上宣傳，透過特殊技術使用反向代理 和 Cookie 注入 方法繞過 2FA 身份驗證，屬於非常新型的駭客攻擊，建議企業需要定期進行釣魚演練加強人員亦是避免遭受有心人士利用。

【資料來源：Securityaffairs, 2022.09.05】

SharkBot 惡意程式繞過防護潛入 Google Play 竊取您的登錄信息

研究人員發現曾經在Google Play商店中橫行的SharkBot 惡意程式，經過改版後又重新上架於商店內，惡意程式存在於兩個 Android 應用程序中，這些應用程式在提交給 Google 的自動審查時竟然沒有偵測出任何惡意程式碼，希望使用者在商店內下載程式時須謹慎，避免遭受攻擊。

【資料來源：BLEEPINGCOMPUTER, 2022.09.04】