SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2022.11.18(五) —— 2022.11.25(五)

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

資安暨智慧科技研發大樓

偽造的 MSI Afterburner 以 Windows 遊戲玩家為目標，帶有挖礦、個資竊取等程式

MSI Afterburner為微星開發的電腦超頻工具，主要功能為監控系統性能與修改硬體設定使電腦能超頻運作，為電腦玩家非常主流使用的超頻軟體，但研究人員發現網路上正在散布該軟體的惡意版本，內含有挖礦程式，只要使使用者安裝並啟用就會於背景進行挖礦程式挖取門羅幣，呼籲於網路上下載軟體要尋找官方下載較為安全。

【資料來源：CYBLE., 2022.11.23】

駭客散佈流行的 OpenVPN Android 應用程式中內含間諜軟件

OpenVPN為知名的開源VPN程式，如今遭到駭客組織利用於網路攻擊，駭客註冊釣魚網站並誘使人下載經過修改的OpenVPN 應用程式，該程式內含惡意程式會竊取使用者的所有聊天記錄與文件，請使用者下載程式時需注意發布組織。

【資料來源： BLEEPINGCOMPUTER, 2022.11.24】

GOOGLE 提供檢測 Cobalt Strike 破解版數十種規則

Cobalt Strike為知名駭客組織常用攻擊程式，研究人員搜集網路上高達三百多種的 Cobalt Strike 變形版本後整理出一套YARA規則並開放給人使用，套用該規則可以偵測並阻擋常見的攻擊手法。

【資料來源： SECURITYAFFAIRS, 2022.11.21】

繼 Cobalt Strike 後 Nighthawk 可能成為黑客新的後期開發工具

Nighthawk 由一家名為 MDSec 的公司於 2021 年 12 月推出，類似於其同行 Cobalt Strike、Sliver和Brute Ratel，為對手威脅模擬提供紅隊工具集，駭客經常會利用一個相對未知的框架來避免被防護設備檢測出，希望大家可以多針對不同特徵進行分析辨識，及早定位攻擊避免遭受危害。。

【資料來源： THEHACKERNEWS, 2022.11.23】