SHALUN
CYBER SECURITY HUB

資安週報

2022.07.09(六) —— 2022.07.15 (五)

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

Windows上的Node.js含有 CVE-2022-32223漏洞，能通過 npm CLI 劫持 DLL

Aqua Team Nautilus發現在windows上的node.js容易受到DLL劫持攻擊影響，研究人員發現含有漏洞版本的npm命令執行時會DLL搜尋，來尋找本機上符合的DLL，該行為發現可以被駭客利用進行DLL劫持進而引用任意DLL來執行，透過DLL劫持可以引發執行任意程式的風險。

【資料來源： Aqua Blog, 2022.07.12】

駭客透過在LinkedIn上發布虛假工作機會針對Axie Infinity 的一名員工發動社交工程攻擊，導致5.4 億美元的盜竊

駭客通過LinkedIn 向Axie Infinity公司的一名高級工程師發送虛假的工作面試邀請，通過提供報酬即為豐厚的薪資誘使該工程師受騙，接受該公司提供的薪資報價PDF檔，該檔案含有惡意程式，點開檔案後駭客就入侵該公司並滲透進系統，最終竊取走價值5.4億美金價值的虛擬貨幣。

【資料來源： Security Affairs, 2022.07.11】

Bandai Namco (南宮夢萬代)在ALPHV遭受勒索軟件威脅數據洩露後確認遭受黑客攻擊

BlackCat勒索軟件(又名AlphV)聲稱在攻擊過程中破壞了Bandai Namco 並竊取了公司數據，萬代南夢宮控股有限公司確認，在其亞洲地區（日本除外）的多家集團公司的內部系統遭到第三方未經授權的訪問，但卻沒有提供有關網絡攻擊的任何技術細節。BlackCat 目前也尚未公佈任何 Bandai Namco 據稱被盜的數據。

【資料來源： BLEEPINGCOMPUTER, 2022.07.13】

研究人員發現了 Qakbot 惡意軟件為了逃避檢測的新方法

Qakbot 是一種靈活的後滲透利用工具，它結合各種防禦規避技術來防止攻擊被發現，並採用的其他方法包括代碼混淆、在攻擊鏈將惡意程式載體拆分，以及使用多個 URL 以及未知的文件擴展名(例如，.OCX、.ooccxx、dat或.gyp)來儲存惡意程式碼。

【資料來源： The Hacker News, 2022.07.12】