SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.09

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

資安暨智慧科技研發大樓

微軟報告顯示中國對東亞及臺灣的網路攻擊與AI認知作戰增加

微軟威脅分析中心（MTAC）發表東亞數位威脅報告《Digital threats from East Asia increase in breadth and effectiveness》，報告指出東亞數位威脅情勢正在迅速變化，中國展開了廣泛的網路攻擊和認知作戰。中國國家相關網路威脅者三個重點攻擊目標，分別是南海周邊國家、美國國防工業和美國關鍵基礎設施。中國國家相關威脅者對南海國家和臺灣的行動特別活躍，報告提到，這反映中國在東亞地區的經濟、防禦和政治利益，因為領土衝突、中國與臺灣的緊張關係，以及美軍的存在，皆是中國發動網路攻擊的動機。

【資料來源：iThome 2023.09.11】

CoinEx 加密貨幣交易所遭駭，損失達 5,300 萬美元

全球大型加密貨幣交易所 CoinEx 日前對外公開駭侵事件，該交易所的熱錢包遭駭侵攻擊，大量加密貨幣資金遭竊。雖然 CoinEx 並未在公開的訊息中提及此次駭侵事件造成的數位資產財務損失金額，但區塊鏈資安公司 PeckShield 指出，據該公司的監測資料，CoinEx 的損失包括 1,900 萬美元等值的 ETH、1,100 萬美元等值的 TRON（以 BSC 形式存於幣安的 Binance Smart Chain 上）、600 萬美元等值的 BTC、約 29.5 萬美元等值的 Polygon。全球大型加密貨幣交易所 CoinEx 日前對外公開駭侵事件，該交易所的熱錢包遭駭侵攻擊，大量加密貨幣資金遭竊。

【資料來源：TWCERT/CC 2023.09.14】

ALPHV勒索軟體集團承認是駭進MGM Resorts的元兇

WithSecure研究長Mikko Hypponen張貼了來自ALPHV（BlackCat）勒索軟體集團外洩網站的一則訊息，指出該集團為駭進米高梅國際酒店集團（MGM Resorts International）的元兇，而且是在MGM Resorts關閉所有Okta Sync伺服器並切斷部分元件的網路服務之後，才在 9/11 於超過100臺的ESXi伺服器上展開勒索軟體攻擊。

【資料來源：iThome 2023.09.15】

中國駭客在臺灣論壇散布假「Whoscall」破解版，暗藏間諜軟體，該討論串已有10萬瀏覽次數

資安業者Volexity在9月22日揭露中國駭客組織EvilBamboo（或稱Evil Eye）鎖定行動裝置的多起攻擊行動，特別的是，當中特別提到一起鎖定臺灣民眾的攻擊事件，手法是聲稱分享「Whoscall來電辨識」破解版，並在臺灣的論壇上散布安卓間諜軟體BadBazaar，受到國內資安界的關注。根據Volexity研究人員的說明，這些中國駭客從2023年1月17日開始，就在Android台灣中文網（Apk.tw）的論壇上，持續假藉提供Whoscall新破解版的名義，在貼文底部提供QR Code的下載連結，引誘國人下載他們提供的惡意APK安裝檔（其載點則是他們濫用了Google Drive、Dropbox的雲端硬碟服務），讓用戶將檔案下載到手機上安裝。

【資料來源：iThome 2023.09.23】