SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.11

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

資安暨智慧科技研發大樓

50個國家與組織聲明不支付勒索軟體贖金

美國舉行的第三屆國際反勒索軟體高峰會（International Counter Ransomware Initiative，CRI）中，50個成員組織決定將共同開發破壞駭客及其基礎設施的能力，藉由共享資訊來改善網路安全，同時也制定了史上第一份CRI聯合政策聲明，闡明成員國政府不應支付贖金。美國司法部長Merrick Garland在CRI開幕致詞中強調了國際夥伴在破壞及減輕勒索軟體威脅上的重要性，例如在今年1月透過全球合作瓦解了惡名昭彰的Hive勒索軟體網路。此外，這一年來國際上的合作也摧毀了BreachForums及Genesis Market兩大網路犯罪市集，以及數家加密貨幣交易所及混合器，打擊勒索軟體網路的供應鏈。。

【資料來源：iThome 2023.11.02】

FBI拆毀IPStorm殭屍網路

美國司法部於本周宣布，美國聯邦調查局已拆毀了危害全球數萬裝置的Interplanetary Storm（IPStorm）殭屍網路，主謀Sergei Makinin已遭逮捕且已認罪。崛起於2019年6月的IPStorm是以Golang所撰寫，原本鎖定Windows裝置進行感染，隨後並將版圖擴大到Linux、macOS與Android，其惡意程式目的是令這些裝置為Makinin所控制，Makinin對外宣稱總共握有全球2.3萬個裝置的控制權，遍及亞洲、美洲與歐洲。根據羅馬尼亞資安業者Bitdefender在2020年針對IPStorm所發表的分析白皮書，被植入IPStorm惡意程式的受害者主要位於亞洲，前三名是香港、南韓與臺灣。

【資料來源：INFO SECURITY 2023.11.22】

NICS 台灣資安計畫」助力中小型企業、非營利組織強化資安

Google 和台灣國家資通安全研究院（資安院）宣布啟動為期兩年的「NICS 台灣資安計畫」，由 Google 旗下慈善組織 Google.org 投注一百萬元美元、資安院執行計畫，協助台灣中小型企業與非營利組織盤點與加強資安防護能力，深化資訊安全領域的產、官、學界合作，提升台灣資安研究量能，並培育更多在地資安種子教師與專業人才。

【資料來源：INFO SECURITY 2023.11.22】

趨勢科技示警微軟 Exchange的四個零日漏洞

趨勢科技披露微軟(Microsoft) Exchange 中的四個零日漏洞，經過身份驗證的攻擊者可以遠端利用這些漏洞來執行任意程式碼或洩露有關易受攻擊的敏感資訊。研究人員表示專業APT組織偏愛利用Exchange高危險漏洞發起針對性攻擊。趨勢科技於 2023 年 9 月 7 日至 8 日向微軟報告了這些漏洞，微軟承認了這些漏洞，但至今尚未修復這些漏洞。

【資料來源：INFO SECURITY INFO SECURITY 2023.11.06】