SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.08.19 (六) —— 2023.08.25(五)

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

HiatusRAT攻擊臺灣市府、民間企業，也瞄準美國軍事採購系統

資安廠商發現一項名為HiatusRAT的木馬程式攻擊行動，近日復出大舉攻擊臺灣半導體、化學等企業、地方政府及美國軍方採購相關的伺服器，懷疑可能和中國有關。資安業者Lumen旗下Black Lotus Labs實驗室今年3月，觀察到名為HiatusRAT的木馬程式感染全球超過100多臺邊緣網路裝置。它寄生在邊緣路由器上，被動蒐集流量並當作C&C伺服器執行。在消失一段時間後，Black Lotus研究人員於6月中再度發現HiatusRAT攻擊活動的跡象。有別於原本外界認為的拉丁美洲及歐洲，研究人員發現HiatusRAT這波攻擊鎖定臺灣，也對一個美國軍事採購單位發動偵察。

【資料來源：iThome 2023.08.22】

Juniper公告 Junos OS漏洞影響SRX及EX所有版本

Junos OS 中 J-Web的多個漏洞，這些漏洞可以組合起來在易受影響的設備上執行遠端程式碼。這四個漏洞的累積 CVSS 評級為 9.8，嚴重程度為「嚴重」。它們影響 SRX 和 EX 系列上所有版本的 Junos OS。Juniper在 2023 年 8 月 17 日發布的公告中表示，藉由串聯利用這些漏洞，未經身份驗證的網路攻擊者可能能夠在設備上遠端執行程式碼。J-Web 界面允許用戶配置、管理和監控 Junos OS 設備。

【資料來源：INFO SECURITY 2023.08.20】

WinRAR 嚴重漏洞，開啟壓縮檔可讓駭侵者遠端執行任意程式碼

資安廠商趨勢科技旗下的資安研究團隊 Zero Day Initiatives 日前發表研究報告，指出該單位的資安研究人員，近期發現 WinRAR 內含一個嚴重漏洞，駭侵者可藉以在使用者開啟 RAR 壓縮檔時，遠端執行任意程式碼。該漏洞的 CVE 編號為 CVE-2023-40477，問題源自對於復原檔案卷宗在處理上的錯誤，未能適當驗證用戶輸入的資訊，使得驗侵者可存取已分配緩衝區之外的記憶體。駭侵者可將特製的 RAR 檔案傳送給攻擊目標，誘使其開啟檔案，即可利用該漏洞遠端執行任意程式碼。

【資料來源：TWCERTCC 2023.08.22】

FBI：北韓的駭客組織準備兌現 4100 萬美元被盜的加密貨幣

美國聯邦調查局警告稱，FBI 追踪到北韓的附屬組織（也稱為 Lazarus Group 和 APT38）所竊取到的加密貨幣。FBI 認為朝鮮可能試圖兌現價值超過 4000 萬美元的比特幣。該聲明是在一項調查發現之前的加密貨幣盜竊案中被盜的大約 1,580 枚比特幣轉移到 6 個加密貨幣錢包中之後發布的。

【資料來源：BLEEPING COMPUTER 2023.08.23】

SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.08.12 (六) —— 2023.08.18(五)

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

資安暨智慧科技研發大樓

中國駭客RedHotel針對包括臺灣在內的17個國家，進行為期3年的網路攻擊行動

長期觀察中國駭客行動的美國資安業者Recorded Future本周揭露，有一由中國政府支持的國家級駭客組織RedHotel，從2019年就開始滲透不同國家的政府及民間組織，特別是東南亞地區的國家，主要任務為情報蒐集及商業間諜，還會冒用其它組織的憑證與基礎設施來展開攻擊。RedHotel最值得一提的事蹟之一，就是在去年底盜走了一個屬於臺灣遊戲公司的程式簽章憑證，並簽署一個DLL以用來載入滲透測試工具Brute Ratel C4，此一工具可與越南國家級科學研究院的基礎設施進行通訊，顯示該越南組織也已被RedHotel攻陷，還被用來當作駭客的命令暨控制中心。此外，直至今年6月，RedHotel仍在使用越南教育及培訓部的TLS憑證。

【資料來源：iThome 2023.08.15】

近 2,000 台 Citrix NetScaler 伺服器在駭客的網路攻擊活動中被安裝了後門

資安公司Fox-IT（NCC 集團）和荷蘭漏洞揭露研究所(DIVD) 的安全研究人員發現了一項大規模的資安攻擊活動，此活動利用了編號為CVE-2023-3519且分類為嚴重等級的漏洞，此大規模的資安攻擊活動會在 Citrix Netscaler 伺服器上植入了 Webshell ，使得駭客可以擁有持久性的遠端存取權限 。儘管該漏洞已在7月18日發布更新程式，但顯然駭客的攻擊活動在更早的時侯已經展開。

【資料來源：BLEEPING COMPUTER 2023.08.15】