不見血的戰爭

去年遭攻擊近4千億次

台企淪駭客眼中肥羊

●記者馬瑞璿／專題報導

光是2024年上半年，新興勒索軟體如BlackSuit、Hunters International、Underground Team等，就對台灣企業發動針對性攻擊。

台灣是全球科技製造重鎮，許多企業手中都握有國際大廠研發資料，這些資料含金量高，讓台灣企業成為了全球駭客眼中的肥羊。

根據資安業者Fortinet統計，2023年亞太區共偵測到9703億次威脅，其中台灣占比逾4成，換算下來，台灣被攻擊的次數高達近4000億次，形勢相當嚴峻。

綜觀過去3年，勒索病毒橫行全世界。不過，如果只單看去年，可以發現，駭客的勒索病毒攻擊策略已出現改變。

Fortinet分析，相較於去年上半年，去年下半年的勒索軟體攻擊下降70%，主因攻擊者從傳統的「廣灑與祈禱式策略」，轉向更具針對性的方式。

分析駭客攻擊行為，最老派而經典的手法，就是寄送釣魚信件，透過有毒的副檔或者網址，將病毒送入企業電腦，也就是「廣灑與祈禱式策略」。但並非每一封釣魚信件，企業都會打開，如果企業沒有中招打開信件，駭客的釣魚信件只能宣告失敗。

駭客也在轉型 從「釣魚」變成鑽漏洞

相較於老派駭客手法，新一代的黑帽駭客則是在企業系統後門找漏洞，只要一找到漏洞，就乘機鑽進企業系統裡面潛伏，直到時機成熟、偷出夠多資料後，就會開始在暗網上販售，或者要求企業支付巨額贖金，贖回這些機密資料。

趨勢科技指出，泰國、美國、土耳其、台灣和印度是遭受勒索病毒襲擊最嚴重的前五名，而銀行業、政府機關與科技業則是受害最深的產業前三名。台灣也有多起企業遭駭案例，其中最受外界關注的就是鴻海集團旗下半導體設備大廠京鼎。

台企首見案例 京鼎官網被直接挾持

京鼎的案例之所以令人關注，主要原因在於駭客入侵之後，不僅竊取資料，甚至直接挾持公司網站，這是台灣企業第一次遇到這樣的情況。

京鼎1月遭駭客入侵之後，雖然第一時間已跟駭客集團談判，但京鼎資料仍在5月份被駭客公開於暗網上。京鼎5月也在公開資訊觀測站上發出公告表示，「經查本次駭客揭露內容為113年1月之同起事件，並於113年1月已通報政府部門，同時通知客戶。本公司已全面檢視資安防禦機制並啟動相關檢測，並遵守個資保護法規及法遵規定」。

美國資安主管機關網路安全暨基礎設施安全局資料顯示，2023年前3名勒索軟體組織為LockBit、Clop和BlackCat。今年歐美11個執法組織雖聯手破獲LockBit勒索設施，但其餘組織仍然活躍。資安業者竣盟科技發現，光2024年上半，新興勒索軟體如BlackSuit、Hunters International、Underground Team、Ransom Hub及Qilin等，就對台企發動針對性攻擊。

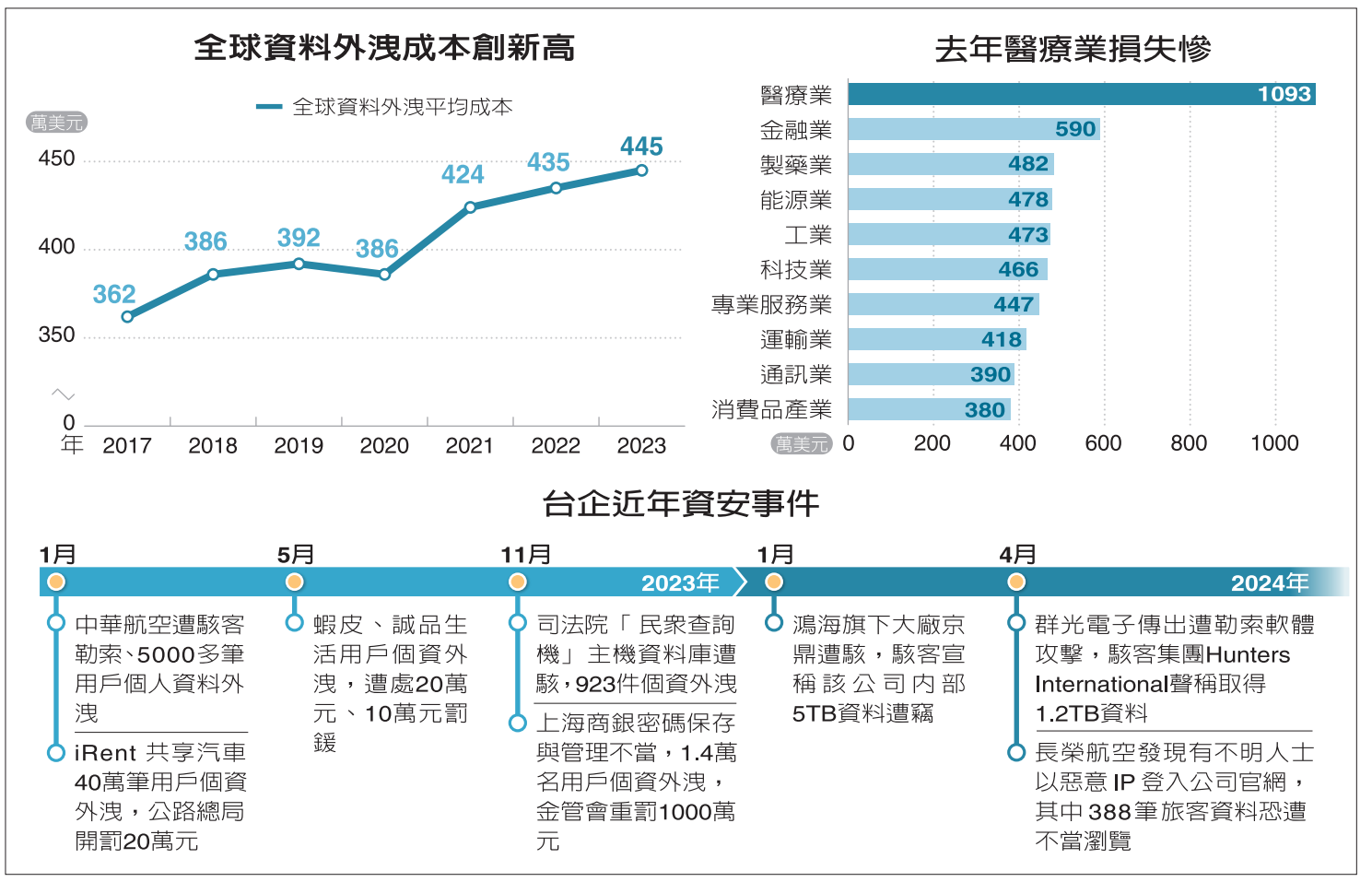
不只金錢損失 資訊操弄更影響經貿

竣盟科技創辦人鄭加海指出，台灣的製造業連兩年成為勒索軟體攻擊的主要目標，反映出科技業、製造業對網路安全的迫切需求。

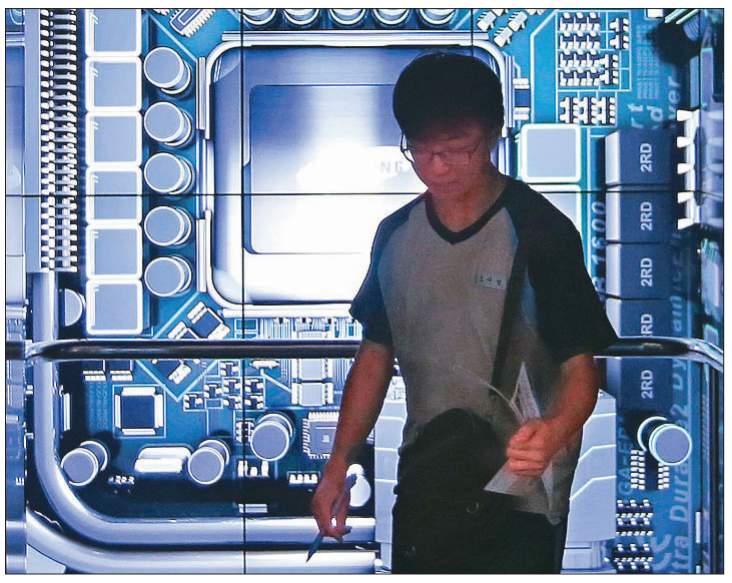
而駭客攻擊不只會影響企業經營，長期來看，也會對全球經貿帶來極大影響。

鄭加海表示，除了勒索軟體病毒之外，也有些駭客組織會透過「資訊戰」的方式，利用「資訊操弄」，影響各地經貿活動。

鄭加海以中國駭客組織Dragonbridge為例，這個組織擅長散布不實言論，針對台灣年輕人散布特定政治言論，換言之，駭客攻擊帶來的不僅是企業經濟或運營損失，恐引發一系列負面後果，包括供應鏈中斷、信任度下降、短暫經貿癱瘓，能以低成本達到實體破壞和經濟重創等效果，不管是企業或者政府單位，對於各式駭客攻擊，不可不慎。



資料來源／2023年IBM資料外洩成本報告、記者整理　製表／蔡佩蓉、林雨荷　■聯合報　2024.06.23製表



台灣是全球科技製造重鎮，許多企業手中都握有國際大廠研發資料，讓台企成為了全球駭客眼中肥羊，圖為示意圖。　（美聯社）

企業被駭 成本轉嫁消費者

●記者蔡佩蓉／專題報導

根據IBM最新年度報告顯示，2023年全球資料外洩平均總成本達445萬美元（約新台幣1.4億元），創下此年度報告發表以來的最高金額。該報告分析來自16個國家和地區、553家組織資料被竊取案例，涵蓋17個不同行業，其中以醫療保健業損失最慘重，已連續13年高居各行業榜首。

在所有遭外洩的資料類型中，客戶個人身分識別資訊（PII）最貴，每筆紀錄的成本高達183美元，其次是員工的個人身分識別資訊，每筆紀錄成本為181美元。

網路釣魚和憑證被盜是兩種最常見的駭客攻擊媒介，分別占所有資料外洩事件的16%和15%，網路釣魚所造成的損失金額高居各攻擊手法的第二位。

此外，研究也發現，隨資料外洩成本上升，企業通常將成本轉嫁給消費者，進而提高商品和服務的價格。

近60%受訪企業表示，他們在資料外洩事件發生後，提高了產品和服務價格。駭客勒索、釣魚等犯罪事件看似影響的是企業，但最終苦到的仍是廣大消費者。

車輛愈智慧 駭客工具就愈多

自動駕駛上路 衍生安全漏洞

●記者洪欣慈／專題報導

特斯拉今年4月開放全美車主免費試用其全自動輔助駕駛（Full Self-Driving，FSD）一個月，特斯拉執行長馬斯克訪問中國大陸後，FSD登陸也已有譜，日前輝達（NVIDIA）執行長黃仁勳更大讚FSD技術遙遙領先，自駕勢不可擋。不過，資安專家同步示警，車輛愈智慧，風險也愈高，各車廠推動未來交通革命的先進駕駛輔助系統（ADAS）、AI模型攻擊等，都是車商將面臨的新資安挑戰。

去年12月至今年2月，特斯拉因Autopilot自動輔助駕駛風險陸續召回400多萬輛車。美國國家公路交通安全管理局（NHTSA）指出，Autopilot存有警示燈字體太小、使駕駛過度信任系統等安全漏洞，自2022年1月至2023年8月總計造成467起碰撞事故。

另有前員工爆料，指Autopilot軟硬體都還未準備好上路，BBC報導，該員工指出，曾有客戶投訴車輛因不存在的障礙物，產生「幻象煞車」。

汽車網路資安公司VicOne長期針對全球銷量前十的電動車款進行安全測試，VicOne副總裁張裕敏表示，駕駛輔助系統運作依賴大量感測器、攝影機、雷達運作，只要有訊號傳遞，就可能存有被入侵、干擾、控制，以及演算法、AI模型漏洞等安全風險。

有心人亂貼道路白線 就能誤導系統

張裕敏舉例，自駕系統主要靠演算法來辨識物體和影像，若演算法品質有瑕疵，有心人士在地面上亂貼道路白線，就能將自駕車誤導到對向車道，導致相撞；光學雷達在傳遞和接收訊號時，若駭客在第三處放設干擾裝置，就能影響車輛判斷，造成急煞、連環車禍。這些情境都非假設，而是團隊曾實測過的攻擊模式。

遠端遙控、聲控、語音助理等智慧功能近期也陸續發現漏洞。日前社群X上一段中國電動車廠蔚來的影片引發熱議，內建AI助理被問到「本周有誰坐過副駕」時竟一一細數，連何時搭車、在車上做哪些事都清楚描述，被網友戲稱為「離婚神器」，AI還兼具抓姦功能。趣聞背後衍生出AI幻覺、侵犯隱私、資料外洩等疑慮。

另有購買小米SU7車款的用戶po出一段影片，影片中儘管車輛已上了中控鎖，站在車外的人仍可透過聲控，從車外打開車門。

側錄電子鑰匙電波 車輛輕易失守

美國去年也頻傳「無鑰匙攻擊」，偷車集團透過網上幾百美元就可買到的無線電波接收器，偷偷在車輛附近側錄電子鑰匙的無線電波後回放，順利將車開走。

張裕敏表示，當車輛不再是封閉系統、有更多裝置和軟體運用其中時，駭客和犯罪集團可利用的工具就愈多。聯合國歐洲經濟委員會（UNECE）、美國汽車工程師學會（SAE）、國際標準化組織（ISO）等單位已針對汽車網路安全發布標準，建議民眾購車時可詢問該車款是否符合相關規範，當詢問的消費者愈多，就能讓車廠更重視車輛資安。