網安事件頻發 攻防節拍更快

■文：編輯部

在資訊技術飛速發展的今天，網路安全事件頻發，給個人隱私、企業運營乃至國家安全帶來了嚴峻挑戰。本文旨在通過對 2023 年至 2024 年全球重大網路安全事件的梳理，分析網路安全的現狀和趨勢。

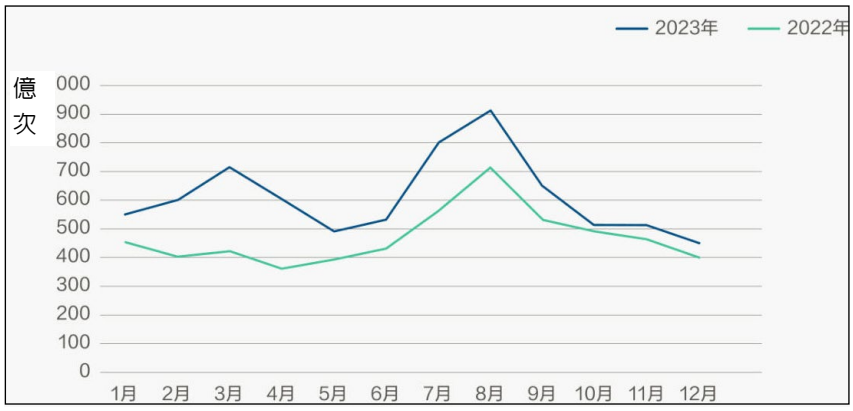
在這段時間內，全球經歷了多起重大網路安全事件，包括資料洩露、勒索軟體攻擊、供應鏈攻擊等。這些事件不僅對受影響組織造成了直接經濟損失，還對公眾信任和品牌價值造成了長遠影響。

2023 年重量級別安全事件

23andMe 個人關鍵資訊遭竊：2023 年 10 月，基因檢測巨頭 23andMe 遭遇撞庫攻擊，導致 690 萬使用者的敏感資訊被洩露，包括家族譜系、出生年份和地理位置等關鍵資料。

供應鏈攻擊事件：MOVEit Transfer 資料盜竊攻擊影響了 2706 個組織，超過 9300 萬人的個人資料被洩露，受害者遍及 20 多個國家、10 多個行業。這種類型的攻擊通常利用軟體或服務的漏洞，通過供應鏈傳播惡意軟體，影響廣泛且難以防範；同期，VoiP 軟體提供商 3CX 遭遇供應鏈攻擊，攻擊發起方是朝鮮駭客組織 UNC4736，他們大約在 2021 年入侵了提供交易軟體的 Trading Technologies 公司，篡改了 X_Trader 軟體的安裝程式，植入了 VEILEDSIGNAL 後門，2023 年一名 3CX 員工下載了被植入後門的 X_Trader 軟體，攻擊者在感染了員工電腦

圖說：wangsucloud 公司 web app 流量中檢測到的攻擊請求相比 2022 年增加了 30%。



資料來源：wangsucloud 公司

之後滲透進入企業網路，最終篡改了 3CX 的桌面應用。

間諜軟體攻擊：技術複雜的間諜軟體攻擊如“三角測量”，利用多達四個零日漏洞，自 2019 年以來被用於監聽 iPhone 用戶。數千台蘋果手機受到了感染，包括俄羅斯公民及外交官員的手機，受影響的對象還包括北約國家、以色列、敘利亞和中國等國，這類攻擊往往由國家級別的駭客組織發起，目的在於竊取敏感資訊和監控目標。

金融業安全事件：中國工商銀行美國子公司遭受 LockBit 勒索軟體攻擊，導致部分系統中斷，影響了美國國債市場的交易。金融行業的網路安全事件可能導致嚴重的經濟損失和市場動盪。

雲資料安全事故：丹麥雲服務商 CloudNordic 和 AzeroCloud 在被勒索軟體攻擊後，無法恢復客戶資料，導致大多數客戶丟失了他們的所有資料。隨著雲計算的普及，雲服務提供者成為攻擊者的重要目標，一旦發生安全事件，影響範圍廣泛。

遊戲業網路安全事件：GTA5 原始程式碼在 2023 年聖誕夜被洩露，這是繼 2022 年 Lapsus$ 駭客組織入侵遊戲公司 Rockstar 遊戲後的又一事件。遊戲行業的網路安全事件可能導致智慧財產權洩露和品牌形象受損。

DDoS 攻擊：“匿名蘇丹”的駭客組織的 DDoS 攻擊癱瘓了多家全球科技巨頭的網站和服務，包括微軟服務 (包括 Outlook、OneDrive 和 Azure 門戶)。DDoS 攻擊通過流量超載使服務不可用，影響全球範圍用戶體驗，一度使得使用者更新和升級服務無法連接。

線上金融服務資料洩露：PayPal 披露其用戶帳戶在大規模撞庫攻擊中被洩露，涉及 34942 個 PayPal 帳戶。線上金融服務的資料洩露可能導致使用者財產損失和信任危機。

博彩業受到駭客攻擊：米高梅國際酒店集團遭受 BlackCat 勒索軟體攻擊，攻擊影響了米高梅酒店、賭場的網路系統，造成了巨大的經濟損失。博彩行業由於其高利潤和疏鬆得監管環境，成為網路犯罪分子的目標。

軍工企業安全事件：GE (通用電氣) 疑遭駭客攻擊，包含大量敏感軍事機密資訊資料被駭客在論壇中出售，資料包括大量與 DARPA 相關的軍事資訊、檔等；波音公司遭遇 LockBit 勒索軟體攻擊，LockBit 聲稱竊取了波音的大量敏感性資料。軍工企業的網路安全事件可能威脅國家安全和軍事優勢。

2023 年底的 12 月，美國愛達荷國家實驗室 (INL) 遭受網路攻擊。駭客組織 SiegedSec 宣佈已獲得 INL 資料的存取權限，其中包括“數十萬”員工、系統使用者和公民的詳細資訊。SiegedSec 沒有與受害者談判或索要贖金，而是直接在駭客論壇和該組織運營的 Telegram 頻道上公開洩露了被盜資料。作為美國最大的核能研究設施，愛達荷國家實驗室在核能領域具有舉足輕重的地位。此次攻擊事件引起了廣泛

關注並採取措施確保員工資料安全。

儘管 2024 年還沒有走完，但是一系列安全事件依然讓身處其中的人們神經緊繃 Ivanti VPN 攻擊：Ivanti Connect Secure VPN 的兩個零日漏洞被利用，加拿大全球事務部 VPN 系統被“破壞”：1 月 30 日，加拿大全球事務部 (即外交部) 的虛擬私人網路絡系統被入侵，隱私資料和電子郵件被洩露。受害者名單包括世界各地的政府和軍事部門、國家電信公司、國防承包商、技術公司、銀行、金融和會計機構、全球諮詢公司以及航太、航空和工程公司。這些攻擊促使 CISA 向美國聯邦政府的行政部門發出緊急命令，要求採取緊急措施，在 48 小時內斷開其 ICS VPN 的連接。

多區域互聯網註冊機構資料洩露：1 月 29 日，全球五大區域互聯網註冊機構中的 RIPE、APNIC、AFRINIC 和 LACNIC 四家，因感染惡意軟體，導致暗網上出現大量資料洩露，受害者包含來自多個國家政府、大型金融機構、研究機構和 IT 企業等。

微軟高管帳戶洩露：2024 年 2 月，微軟公司高管的電子郵件系統被洩露，攻擊者訪問到了很多企業電子郵件帳戶。名為 Volt Typhoon 組織劫持了位於美國的“數百台”小型辦公室 / 家庭辦公室 (SOHO) 路由器，並將其組成僵屍網路對美國關鍵基礎設施發動攻擊。FBI 表示，Volt Typhoon 攻擊的目標包括通信、能源、水和交通等關鍵服務提供者。

2 月底，FBI 發現並消滅了俄羅斯網路間諜在惡意軟體活動中使用的另一個小型辦公室 / 家庭辦公室 (SOHO) 路由器僵屍網路。該僵屍網路由網路犯罪分子使用已知的“Moobot”惡意軟體構建，後來被俄羅斯 APT 組織 (APT28，也被稱為 Forest Blizzard/Sofacy/Fancy Bear，與俄羅斯情報局 GRU 有聯繫) 收編。網路犯罪分子在 Ubiquiti Edge OS 路由器上安裝了 Moobot 惡意軟體，而這些路由器仍然使用公開的預設管理員密碼。GRU 駭客隨後使用 Moobot 惡意軟體安裝他們自己的定制腳本和檔，重新調整僵屍網路的用途，將其變成一個全球網路間諜平臺。

醫療保健系統中斷：Change Healthcare 公司遭受勒索軟體攻擊，導致美國醫療保健系統中斷數周，許多藥店和醫院無法處理索賠和接收付款。

ConnectWise ScreenConnect 存在兩個漏洞，可導致數萬家企業遭受重大網路攻擊，駭客們利用這兩項漏洞部署勒索病毒。

XZ Utils 軟體供應鏈攻擊：在最新版本的 XZ Utils 中發現

被植入的惡意程式碼，涉及 Linux 發行版本中的通用資料壓縮格式，Redhat 和美國網路安全與基礎設施安全局 (CISA) 警告稱，這些惡意程式碼可能會引發軟體供應鏈攻擊危機。

AT&T 資料洩露攻擊：涉及約 760 萬當前客戶和約 6540 萬前客戶的個人資訊洩露。

美國國家環境保護局資料洩露攻擊：涉及超過 850 萬使用者的個人隱私資訊洩露。

Giant Tiger 使用者資料竊取攻擊：超過 280 萬客戶的個人資訊被竊取。

佳士得拍賣行網路攻擊：導致其拍賣網站在春季拍賣活動開始前臨時離線。

CDK 網路攻擊：CDK Global 遭遇勒索軟體攻擊，導致其汽車經銷商客戶軟體平臺癱瘓。

2024 年 4 月到 7 月間，微軟發現伊朗 APT 組織使用新型 Tickler 惡意軟體對美國和阿聯酋的政府、國防、衛星、石油和天然氣部門組織的網路進行後門攻擊。該組織利用 Microsoft Azure 基礎設施進行命令和控制，使用欺詐性的、攻擊者控制的基礎設施。此外，微軟還發現伊朗 APT 組織冒充著名記者進行魚叉式網路釣魚攻擊。

根據中國大陸有關機構公佈的資料，從 2023 年 7 月至 2024 年 6 月間，全球共有 26 個勒索病毒組織向中國大陸的 71 個機構組織發動了攻擊並實施勒索，同比增長 100% ！其中製造業受害情況最為嚴重。中國的製造業企業的運營技術系統落實最優的網路安全實踐方案，其有限的防禦能力使得製造業企業更容易成為勒索軟體攻擊的目標。

提升網路安全防護能力

上述網路安全事件的原因多種多樣，包括技術漏洞、人為失誤、內部威脅、國家間的網路戰爭等。為了應對日益複雜的網路安全威脅，企業和政府機構正在採取多層次的安全性原則。這包括技術防護、員工培訓、應急回應計畫和合規性管理。此外，定期的風險評估和危害分析、業務影響分析、應急組織的建立、應急程式和流程的制定也成為必不可少的工作之一。

網路安全事件的頻發和複雜性要求全球範圍內的政府、企業和組織加強合作，共同提升網路安全防護能力。通過實施綜合性的安全性原則和持續的技術創新，可以有效地降低網路安全風險，保護關鍵資料和系統免受攻擊。

(本文參考了包括零信任關鍵技術與產業發展研究、2023 年下半年全球威脅態勢研究報告、CyberEdge 2024 Cyberthreat Defense Report 以及 Microsoft Digital Defense Report 2023 等多個資料來源，以確保分析的準確性和全面性。) CTA