防不勝防還是要防

■文：編輯部

有句話叫，沒有千日防賊，意思是，即時防賊難免有懈怠的時候。但是對與數位世界來說，現在需要面臨的問題已經不是”千日防賊”，而是時時應對五花八門的攻擊。

根據 Akamai 公司提供的資料，商務交易、高科技公司、金融服務位元是前三大重點攻擊目標，主要透過惡意軟體、釣魚網站來執行。來自灰色世界的攻擊已經在攻擊深度、攻擊範圍以及攻擊頻率方面再次升級，這倒是很像新冠病毒的變種—omicron，同樣是在傳播速度和範圍上遠遠超過了前面幾代，但不同之處是，omicron 變種病毒的威力已經減小很多，至少人們在心裡上已經坦然很多，可是網路攻擊卻正好相反，其危害也在升級。

2021 年底被發現的 ApacheLog4j 存在任意代碼執行漏洞，登上多家機構的 2021 年安全威脅榜單，CVSS 給出了最早威脅等級滿分 10 分的評價。美國國家安全局、德國電信 CERT、中國國家互聯網應急中心 (CERT/CC)、紐西蘭電腦緊急回應中心 (CERT) 等多國機構相繼發出警告。

此次漏洞是由 Log4j2 提供的 lookup 功能造成的，該功能允許開發者通過一些協議去讀取相應環境中的配置，但是程式在處理資料時，並未對輸入 (如 ${jndi) 進行嚴格的判斷，從而造成注入類代碼執行。從 Akamai 公佈的網路攻擊時時資料來看，透過 SQL 注入方式的攻擊在 web 攻擊中佔據了最高頻率。

目前，該漏洞受影響應用及元件 (包括但不限於) ：ApacheSolr、ApacheFlink、ApacheDruid、ApacheStruts2、srping-boot-strater-log4j2 等。包括谷歌、微軟、亞馬遜、特斯拉、蘋果、騰訊、百度等一大批互聯網企業受到影響，共有 6921 個 APP

存在被攻擊風險。目前，該漏洞正在被修復中。

2021 年 8 月，Microsoft 發佈聲明宣佈遭遇史上最大規模的 DDoS 攻擊，頻寬負載高達 2.4Tbps。這次攻擊者針對微軟歐洲的一位 Azure 客戶，相比比微軟在 2020 年記錄的最高攻擊頻寬量高出 140%。它也超過了之前攻擊針對亞馬遜網路服務時期的 2.3Tbps 的峰值流量。

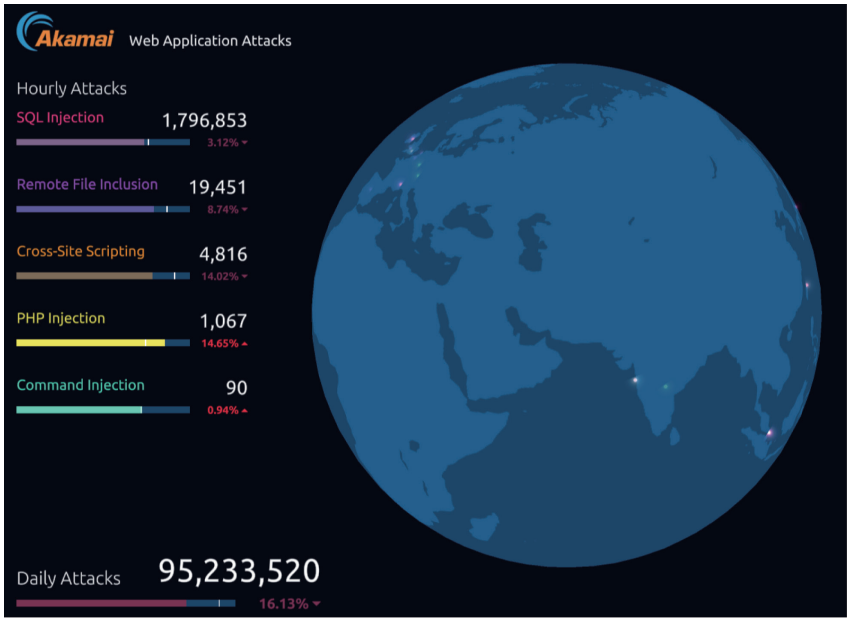
金融、交通、醫療、能源等多個領域成為攻擊者們熱衷的目標。僅 2021 年上半年全球就至少發生了 1200 多起勒索軟體發起的攻擊事件，其中針對醫療系統和教育行業的攻擊增加了 45%，平均贖金從 2020 年的 40 萬美元提高到 2021 年的 80 萬美元。綜合了各方面資訊，我們來看看近一年多以來發生諸多與網路安全有關的事件。

多家醫療機構機構遭到攻擊或勒索

美國加州大學聖地牙哥分校健康中心在 2020 年 12 月 2 日至 2021 年 4 月 8 日期間，有人未經授權訪問了“某些員工電子郵件帳戶”。主管負責人表示，攻擊中可能被訪問和洩露的資料可能包括全名、位址、出生日期、電子郵寄地址、傳真號碼、索賠資訊 (包括接受護理的日期和費用)、實驗室結果、醫療診斷和條件、醫療記錄號、處方資訊、治療資訊、社會安全號、政府識別號、財務帳號、學生識別號、用戶名和“患者、學生和員工社區的子集”的密碼。

2021 年 5 月，愛爾蘭醫療系統遭勒索攻擊，網上疫苗預約等重要工作均無法進行。愛爾蘭公共衛生事務的衛生服務執行局官員證實這次攻擊行為試圖破壞 HSE 的 IT 系統的勒索行為。

圖說：2022 年 5 月初，僅半日 web 網路攻擊即時情況截圖



圖片來源：akamai.com

2021 年 8 月，義大利拉齊奧地區政府證實，駭客攻擊了管理羅馬周邊的拉齊奧地區 COVID-19 疫苗預約的公司的 IT 系統，導致該系統被迫關閉。所有的系統都被停用，包括該地區的衛生門戶網站和疫苗接種網路的系統，導致接種計畫受到影響。

8 月 15 日凌晨，美國醫療連鎖機構 Memorial Health System 遭遇勒索軟體攻擊，致使 IT 系統癱瘓，旗下三家醫院無法正常運營。該機構下轄的大部分醫院診所還取消了當時所有非緊急手術和放射性檢查。

同樣在 2021 年 8 月份，奎斯特診斷公司向美國證券交易委員會 (SEC) 提交通報，公司旗下生育診所 ReproSource 在八月份遭到了勒索軟體攻擊，約 350,000 名患者的大量健康資訊和財務資訊遭到洩漏，部分患者的社會安全號碼 (ssn) 和信用卡號碼也遭到洩漏。

針對基礎設施攻擊

2021 年，2 月 8 日，一名駭客侵入了佛羅里達州奧德瑪律一家水處理廠，通過篡改可遠端控制的電腦資料，將該廠水中的氫氧化鈉含量調高到了極其危險的水準，試圖讓整個城市的人都差點中毒。所幸水廠的運營商及時發現了問題，避免了一場災難。雖然沒有釀成大禍，但是這次事件，讓**數位化後的關鍵基礎**設施的脆弱性暴露出來，並由此引發了新一輪對關鍵基礎設施的攻防大戰。

2021 年 3 月，據美聯社消息，管理全球主要超過 400 家航空公司的機票處理和常旅客資料的 IT 服務公司——SITA (全球資訊技術公司) 宣佈伺服器被駭客入侵，攻擊者經入侵了 SITA 的旅客服務系統 (PSS) 來訪問他們的某些隱私資料，PSS 是 SITA 用來處理乘客從訂票、登機和行李控制的一系列交易的關鍵業務系統，全球多家知名航空公司和航旅企業的顧客資料遭洩漏。

歐洲能源及基礎設施企業提供技術方案的廠商，挪威公司 Volue，在 2021 年 5 月 4 日 -5 日遭遇勒索軟體攻擊，被搞得疲於奔命。

2021 年 4 月，倉儲與運輸服務商 Bakker Logistiek 遭遇勒索軟體攻擊。Bakker Logistiek 是荷蘭國內規模最大的物流服務商之一，專門荷蘭各超市提供恒溫倉儲與食品運輸服務。4 月，Bakker Logistiek 公司遭遇勒索軟體攻擊，業務網路上的設備被對方加密，食品運輸與配送體系也隨之癱瘓。

同樣在 2021 年 4 月，汽車尾氣排放測試公司 Applus Technologies 遭遇惡意軟體 (很可能是勒索軟體) 攻擊，導致包括康涅狄格州、喬治亞州、愛達荷州、伊利諾州、麻塞諸塞州、猶他州和威斯康辛州等八個州的車輛無法進行年檢。

2021 年 4 月 10 日，美國和以色列情報機構的情報消息來源表示，以色列摩薩德是對伊朗伊朗納坦茲核設施進行網路攻擊的幕後黑手，**該行動導致核設施斷電**。據估計，該網路行動破壞了伊朗濃縮鈾的能力。

在 2021 年 5 月 7 日，美國科洛尼爾油管公司遭遇勒索軟體攻擊，並引發一場全美有史以來規模**最大的輸油管線停擺事故**。

2021 年，加拿大最多倫多的公共交通系統遭到勒索軟體襲擊，大量內部 IT 系統癱瘓；包括交通委員會內部的郵件服務、駕駛員通信系統、殘疾人交通預定系統、出行規劃應用、車站螢幕、車輛即時資訊等均無法正常工作。

2021 年 7 月，南非重要港口被網路攻擊癱瘓。事件發生後，南非國家運輸公司 (Transnet，南非國營港口運營商兼貨運鐵路壟斷企業) 在努力淡化事件中的嚴重性，最初只是將其定性為**“IT 網路中斷”**，但在港務碼頭部門發給客戶的函件中，已經確認事件屬於**“網路攻擊、安全入侵與破壞行為”**。

2021 年 8 月，CNN 援引海岸警衛隊的事故分析報告及美國高級網路安全官員的公開聲明，墨西哥灣沿岸重要港口休士頓港遭受網路攻擊，攻擊者疑似有國家背景。官網站顯示，休士頓港每年的貨物輸送量可達 2.47 億噸，是墨西哥灣沿岸最大的港口之一。所幸官方早期調查發現了入侵者，尚未對港口的船運活動進行干擾。

金融一直是重點目標

2021 年 3 月底，美國最大的保險公司之一 CNA Financial 被勒索軟體攻擊，在試圖恢復檔無果之後，他們開始與攻擊者談判，以贖金的方式挽回損失。最後，CNA Financial 在事件發生兩周後支付了 4000 萬美元贖金，以重新獲得對其網路的控制權，創造了勒索贖金的新高紀錄。

“盾”的升級

網路世界日趨複雜多變的安全形勢，防不勝防的安全事件，促使世界各地和各國，從企業到政府層面都在提升防護水準，指定相應法規，以維護數字世界的“和平”。

美國發佈《2021 財年國防授權法案》《臨時國家安全戰略綱要》《改善國家網路安全行政令》等，致力於強化網路空間安全能力、彈性。2021 年 2 月，美國網路安全與基礎設施安全局 (CISA) 發佈《CISA 全球參與》檔，通過加強國際合作以增強全球關鍵資訊基礎設施的安全性和韌性。在 2021 年 5 月和 7 月出臺針對關鍵資訊基礎設施安全防護的行政令，並於 9 月批准了一項修正案，為 CISA 增加 8.65 億美元，用於相關行政令的落實、安全運營和人才培養。

美國公佈的 2021 財年 IT 總預算為 922 億美元，其中**網路安全領域總預算為 188 億美元，比 2020 財年高出 14 億美元，網路安全預算占 IT 預算的比例為 20.4%**。

俄羅斯總統普京簽署的新版《國家安全戰略》首次將資訊列入，而正在進行的戰爭，讓俄羅斯軍隊正在深刻感受資訊戰的力量，在資訊領域獲得部分優勢的烏克蘭人，正在把俄羅斯的入侵拖入泥潭。

歐盟發佈《歐盟數位十年網路安全戰略》，對美國科技公司說“不”，**歐盟正在拾回其“數字主權”**，同時將提升關鍵基礎設施的保護和恢復能力作為未來五年網路安全的重點工作方向。

英國發佈《網路戰略 2022》《安全、防務、發展和外交政策綜合評估報告》，將網路安全作為戰略重點，以提升英國在全球網路空間的地位。**日本發佈《未來三年網路安全戰略綱要》**，強化網路空間安全的戰略指導。

西班牙政府計畫在三年內投資超過 4.5 億歐元，以促進國家網路安全技術、產業和人才發展。

中國大陸作為互聯網創新的熱門地區，相繼出臺了《資料安全法》、《網路安全法》、《個人資訊保護法》、《網路安全審查辦法》。2021 年 7 月 12 日，工信部公開徵求對**《網路安全產業高品質發展三年行動計畫 (2021-2023 年) (徵求意見稿)》**的意見。行動計畫中提出：到 2023 年，網路安全產業規模超過 2500 億元，年複合增長率超過 15%。

邁向零信任 (ZeroTrust) 架構

2021 年 4 月，美國國防部 (DOD) 宣稱計畫推出一個零信任戰略。5 月拜登總統簽署行政命令，強制要求政府部門全面邁向零信任架構。這一年後續的時間裡，美國聯邦政府發佈**《聯邦零信任戰略》**、**美國國防部要求撥款 6.15 億美元用於與零信任網路安全架構相關的工作**。

不久國際電信標準組織 ITU-T 正式對外發佈《Guidelines for continuous protection of the service access process》**(《服務訪問過程持續保護指南》)** 標準，這被認為是全球首個零信任的國際標準。

終結密碼時代

據 Verizon 公司年度資料洩露報告，弱且易於猜測的密碼占所有資料洩露的 80% 以上。鑒於

密碼洩露，弱密碼被撞庫工具頻頻攻破。近日，Apple、Microsoft、Google 分別於“世界密碼日”宣佈，將會全面支持 FIDO 聯盟和萬維網協會 (W3C) 通用的“無密碼登錄”標準，讓使用者無需使用傳統密碼便能在任何平臺及設備上登錄網站，改以**更安全、更簡易的無密碼登錄，取而代之的是更具唯一性和複雜性的升密碼，如指紋、人臉識別等方式**。

FIDO 聯盟執行董事兼首席行銷官安德魯．施基爾 (Andrew Shikiar) 表示：新功能的啓用將帶來一波 FIDO 標準實施的浪潮，助推安全金鑰的持續不斷增長，並為服務提供者提供抗網路釣魚身份驗證的全方位選擇。整個行業範圍內的合作將為無密碼的未來奠定基礎。

美國網路安全和基礎設施安全局 (Cybersecurity and Infrastructure Security Agency，CISA) 局長仁．伊斯特利 (Jen Easterly) 說：“CISA 正在努力提高所有美國人的網路安全水準。**無密碼登錄技術的擴大極具前瞻性，是網路安全維護的一個重要里程碑**。我們很高興看到內置安全的實踐並最終說明顛覆密碼的存在。”

2021 年月 9 月，一次大規模 DDoS 攻擊導致多家俄羅斯銀行系統宕機，部分服務無法正常使用。在此期間，各銀行使用者紛紛遭遇支付與卡片服務問題。

2021 年 8 月，日本加密貨幣交易所 Liquid 遭網路攻擊，9400 萬美元失竊。這可能是該交易上一次被攻擊的後續，在上一次攻擊中，攻擊者通過劫持其 DNS 基礎設施竊取了部分使用者資料。

繼美國之後，日本的保險公司也被成功攻破。日本收入最高的的財險集團東京海上披露其新加坡分公司遭到了勒索軟體襲擊。

2021 年 10 月，巴基斯坦國民銀行 (NBP) 當地時間 10 月 30 日發佈聲明稱，已檢測到對該國商業銀行 NBP 的網路攻擊已中斷其服務，這些服務需要一些時間來恢復。

也在同期，因遭遇網路攻擊，厄瓜多爾最大私營銀行皮欽查銀行關閉了部分網路和系統，業務被迫中斷；此次攻擊導致該銀行業務大面積中斷，ATM 機、網上銀行、移動用戶端、數位管道和自助服務、電子郵件均無法運行。

科技公司製造業被勒索的情況頻發

臺灣科技行業一直籠罩在勒索軟體攻擊的陰影之下，宏碁、研華、仁寶、廣達等知名廠商均遭受過重大打擊。

2021 年 3 月，REvil 勒索軟體宣佈他們已經成功入侵宏碁公司的系統，並同時公佈了相關證據，包括關於財務試算表、銀行結餘以及銀行往來資訊的文檔，並開出了 5000 萬美元天價。同期，技嘉 GiGa-Byte 遭 RansomExx 勒索軟體攻擊，位於臺灣的系統被迫關閉，超 112GB 簽署保密協定的商業資料遭洩露，涉及英特爾、AMD 等合作夥伴；過去幾

2021 年 9 月，日本奧林巴斯關閉了其在歐洲、非洲和中東的電腦網路，同時對其系統遭到的網路攻擊進行調查。

2021 年 10 月，德國企業 Ebersp cher Group (為知名汽車品牌供應空調、供暖及排氣系統) 遭勒索軟體攻擊，官網、郵件、辦公網路、生產系統等紛紛癱瘓，部分工廠員工在宕機處理期間留在家中帶薪休假。

英國工程公司偉爾集團披露，2021 年 9 月遭受了一起勒索軟體攻擊，導致出貨、製造與工程系統發生中斷，僅 9 月因開銷不足與收入延後帶來的間接損失高達 5000 萬英鎊。

進入 2022 年，一個名為 Lapsus$ 的南美駭客組織顯得格外活躍，他們先後攻擊了包括 nVidia、三星電子、Microsoft 等科技公司，拿到大量核心代碼，並提出相應的要求。安全方面的人士認為，從網路系統尋找漏洞可能並非唯一的攻擊手段，他們可能花錢從內部人士那裡“購買”到了重要的帳號。CTA