



雪櫃遭遙控升溫至50℃ 大量食品變質報廢

法國400超市遭黑客攻擊 拉響供應鏈警報

當地時間11日深夜至12日凌晨，法國全境數百家大型連鎖超市遭大規模網絡攻擊。黑客透過入侵智能製冷系統，遠程操控製冷設備使其溫度異常升高到50℃，導致大量生鮮及冷凍產品變質報廢，部分門店甚至因設備過熱引發火警。歐盟農業與食品事務專員克里斯托夫·漢森警告「食品武器化已經成為現實」。歐盟貿易商協會總幹事德爾貝格也指，此次事件「凸顯了整個供應鏈韌性的重要性」。

【大公報訊】截至本港時間13日晚，攻擊者的身份與動機尚不明確。法國總理勒科爾尼已指示法國國家信息安全局（ANSSI）介入，巴黎檢察官辦公室已就此事件展開專門的網絡犯罪調查。當局並與其他歐洲國家協調，評估法國其他企業是否面臨同類風險。

雪櫃加熱長達6小時

據報道，法國全國約15000間超市中有約400間門市受到影響，當中包括家樂福的80間門市、安特馬爾謝及其旗下品牌的180間門市、Monoprix超市則有約5%的門市遭到波及。U合作社有100多間門市受影響，該公司行政總裁謝爾謝在社交媒體上直斥：「破壞對生鮮產品保鮮及法國民眾食品供應至關重要的設備，性質極度嚴重，而且前所未有的，令人無法接受」。有巴黎市民目睹，市中心一家安特馬爾謝超市員工將整車解凍的冷凍食品倒入大型垃圾箱，融化的雪糕還從破裂的容器溢出到路面上。

據法國媒體報道，黑客並未入侵超市的收銀或庫存系統，而是鎖定有關超市使用的丹麥製造商丹佛斯的製冷控制系統。該系統允許零售商遠程監控和調節全國門市的雪櫃溫度，法國大量超市採用此套設備。ANSSI已確認丹佛斯提供的軟件存在漏洞，並已與軟件開發商取得聯繫。

正常情況下，雪櫃夜間會進行短暫除霜，其間設備會切換至加熱模式，融化積霜後再恢復製冷。黑客則利用漏洞，遠程指令設備持續除霜，並將設定溫度調至50℃，使雪櫃加熱長達6小時。有門店員工12日早上打開雪櫃時發現「一股熱浪湧出」，部分門店甚至因設備溫度過高而引發小規模火災。

據報道，早在去年，網絡安全公司Claroty就曾私下通報丹佛斯相關漏洞，丹佛斯隨後發布補丁，但受影響設備並未完成軟件更新，攻擊者可利用漏洞繞過認證、遠程執行代碼並癱瘓雪櫃管理界面。丹佛斯發布聲明稱，受影響的大多是「老

舊」產品，運行了「過時的軟件」，且這些產品「不再接收軟件或安全更新」。多位專家則認為，這起攻擊是「供應商安全控制缺失和產品開發疏忽」的結果。網絡安全專家博蒙特指出，目前仍有數千台丹佛斯製冷設備的管理接口相關信息直接暴露在互联网上，這意味着任何人都能為超市雪櫃調溫。

食品武器化已成為現實

目前尚無全行業損失總額的估算。安特馬爾謝行政總裁科蒂亞爾向BFM電視台表示，這宗「前所未有」的攻擊，預計單日便會為全國造成「數千萬歐元」損失。

網絡安全公司Sekoia的分析師指出，西班牙、葡萄牙、波蘭、德國和比利時也受到了影響。荷蘭零售集團Ahold Delhaize報告公司網絡系統出現安全問題，已將部分系統暫時關閉。旗下荷蘭最大連鎖超市Albert Heijn的線上應用程序與配送系統已無法正常工作，電子價格標籤也頻繁出現錯誤信息，但公司表示目前無證據顯示與法國事件有關聯。

此次攻擊為全球零售業、製造商、政府部門以及普通消費者敲響警鐘：黑客僅通過控制雪櫃溫度，即可造成巨大經濟損失和食品安全風險。歐盟農業與食品事務專員克里斯托夫·漢森警告「食品武器化已經成為現實」。歐盟貿易商協會總幹事德爾貝格也指，此次事件「凸顯了整個供應鏈韌性的重要性」。（綜合報道）



▲巴黎一家超市冷凍食品區張貼告示，告知顧客櫃內商品已被清空。路透社



►巴黎安特馬爾謝超市的一名員工13日將變質的商品丟棄。路透社



▲一名顧客12日在安特馬爾謝超市內購物，超市生鮮冷藏櫃內的商品已被全數清理。法新社

▼一家受影響超市丟棄因為雪櫃升溫而變質的食品。路透社



企業遭黑客襲擊事件簿

醫療系統

- 美國醫療機構 Covenant Health：2025年5月，美國醫療機構 Covenant Health 遭勒索軟件攻擊，多家醫院、診所IT系統臨時關閉。國際勒索團夥 Qilin 聲稱竊取了850GB數據。
- 美國聯合健康集團：2024年2月，全美第五大企業、醫療保險巨頭聯合健康集團（UnitedHealth）下屬子公司 Change Healthcare 遭勒索軟件攻擊，多地醫院、藥房和醫療機構停運。全美高達三分之一人口的醫療與個人數據洩漏，是美國史上最嚴重的醫療網絡安全事件之一。聯合健康集團行政總裁事後承認，公司支付了高達2200萬美元的比特幣贖金。

基礎設施

- 美國網絡安全和基礎設施安全局（CISA）7月底警告，至少7個州的供水和廢水公用事業公司遭到網絡襲擊，其中部分網攻行動影響水務運作，包括造成水壓降低與淹水等。
- 歐洲多國機場值機系統：2025年9月，為全球多家航空公司提供旅客處理與值機系統的美國柯林斯航空公司 ARINC cMUSE 平台遭勒索軟件攻擊，該事故導致倫敦希思羅、柏林勃蘭登堡等多個歐洲繁忙機場的值機與行李託運系統癱瘓數日，大量航班被取消和延誤，機場被迫改用人工手動辦理登機。

大公報整理

多家媒體聯手 抵制AI企業侵權

【大公報訊】據路透社報道：包括《紐約時報》、法新社及《經濟學人》等在內的逾40家媒體及出版商12日宣布加入名為「出版商使用權標準」（SPUR）的國際媒體聯盟，聯手抵制人工智能（AI）公司未經授權抓取新聞內容或藉此謀利。

SPUR成立於今年2月，與《紐約時報》等一起加入的成員還包括美國《大西洋月刊》、巴西全國報業協會等，使聯盟成員數達到約80家。SPUR創始機構包括英國《金融時報》、英國廣播公司（BBC）及美聯社（AP）等。據悉，

各大出版商正進一步升級法律行動，嚴防AI巨頭未經許可擅用媒體內容訓練其大型語言模型。

聯盟亦致力於推動AI公司規範記錄並公開媒體內容的使用情況，確保創作者獲得合理補償。隨著越來越多搜索引擎推出AI生成式摘要，用戶無需點擊原文鏈接即可獲取新聞內容，致使各大新聞網站面臨流量下降的困境。路透社新聞學研究所援引網站分析公司Chartbeat數據顯示，在2024年11月至2025年11月期間，全球逾2500個網站的谷歌自然搜索流量下降了33%。

目前，SPUR正在制定行業標準與技術追蹤系統，協助出版商實時控管內容去向，並促進出版商與AI公司之間商業授權協議的簽訂。本月稍早時，《今日美國報》及其旗下數家報紙已對美國AI巨頭OpenAI提起訴訟，指控對方侵犯版權。

OpenAI及其主要投資者微軟也面臨包括《紐約時報》在內的知名作家與新聞機構的多項版權訴訟。《紐約時報》戰略合作負責人兼首席運營官格羅斯曼-科恩表示，知識產權保護與技術創新「可以且必須共存」。

韓國男子商場持刀施襲釀8傷

【大公報訊】綜合韓聯社、《韓國先驅報》報道：韓國仁川市一間大型賣場13日發生無差別持刀襲擊案，造成8人受傷，其中一名20多歲女子心臟驟停後被送往醫院進行緊急手術，疑兇當場落網。

事發於13日13時40分許，地點位於仁川市九月洞的Homeplus大型賣場3樓。一名59歲男子身穿登山服，背包內藏有約10件武器，雙手疑似綁着利刃，在商場多個樓層遊走並揮舞兇器襲擊行人，隨後被一名顧客當場壓制。警方接報後趕赴現場將其逮捕，消防部門亦在一樓設立緊急醫療站。事件共造成8人受傷，除了心臟驟停的女子之外，其餘7名傷者年齡介乎20多歲至50多歲，已被送往就近醫院搶救，部分人傷勢嚴重。

據悉，疑犯為仁川市桂陽區居民，曾因謀殺未遂入獄四年。韓國司法部13



▲韓國仁川商場13日發生無差別持刀襲擊案，警方和消防員抵達現場。美聯社

日證實，疑犯自2019年獲釋後佩戴電子腳環，並定期接受酒精成癮與心理問題治療。

警方在調查中發現該疑犯持有大量毒品，疑犯亦供認案發時處於吸毒狀態。此外，疑犯此前曾因與某醫院發生糾紛，獨自持菜刀在抗議標語上戳洞示

威而被捕，但當局指該次示威與本次襲擊的關聯仍有待證實。

這已非韓國今年首例持刀襲擊事件。今年5月，西南城市光州一名23歲男子在街頭持刀刺死一名17歲女高中生並刺傷一名青年，公共安全問題引發社會極大憂慮。

美遊樂園過山車致命事故 1死多傷

【大公報訊】綜合BBC、CNN報道：當地時間12日下午4時左右，位於美國佐治亞州的「六旗」主題公園發生致命事故，一名遊客從「歌利亞」過山車墜落身亡，另有多人受傷。

據科布縣警方發布的聲明，警方已即時接手對此宗致命事故展開全面調查，目前尚未公布遇難者的具體死因及其他傷者的受傷細節。多名現場目擊者向當地媒體透露，一名男子搭乘過山車途中，懷疑在半空從座椅被拋出，墜落至軌道旁的林地後當場身亡。網上流傳的視頻片段顯示，該男子墜落期間曾三度撞擊車廂，過程甚至被同車其他遊客的紀念照片捕捉。有目擊者透露，過山車返回車站後，涉事座位上的安全壓欄已呈完全解鎖狀態。

六旗樂園事後發表聲明，對發生遊客身亡事故表示深感悲痛，並承諾提供全面支援。園方隨即宣布暫時關閉全美其他相近設施。據園區網站介紹，「歌利亞」過山車於2006年投入服務，最高點達61米，

時速高達約112公里。

六旗是北美最大的遊樂園運營商，在加拿大、美國和墨西哥擁有逾40座主題樂園、水上樂園及度假村。專門處理遊樂園事故的杜安律師事務所統計，本次事件已是該佐治亞州樂園發生的第7宗死亡慘劇。六旗集團旗下多間遊樂園也面臨安全相關的法律糾紛。上個月，位於南加州的六旗魔術山遊樂園宣布關閉其著名的「X2」過山車。該過山車在2022年至2026年間捲入多起嚴重事故與訴訟。



▲美國佐治亞州的「六旗」主題公園內的「歌利亞」過山車。網絡圖片



◀工作人員12日對發生事故的「歌利亞」過山車進行安全檢查。網絡圖片