黑客再襲製冷設備 法國血庫中招

溫度飆升至110℃ 監控系統及時示警

當地時間3日晚，法國血液機構（EFS）發布公報說，該機構部分冷庫近日遭網絡攻擊，溫度設定值從零下30℃被惡意更改為110℃，所幸監控系統及時發出警報，事件未造成血液製品損失。幾乎在同一時間，歐洲多國超市雪櫃所用的製冷系統也遭黑客入侵，溫度被調高，導致食品變質。一連串事件再次敲響網絡安全警鐘，暴露出聯網設備存在安全漏洞。專家表示，設備製造商應及時發布安全補丁，使用者則應採取提高密碼強度，及時關閉非必要遠程訪問功能等措施，以降低風險。



▲法國血液機構冷庫近日遭網絡攻擊，幸而未造成實際損失。 美聯社



▲法國血液機構向全法1900多家醫院提供血液製品。 美聯社



▲瑞典一家超市的雪櫃2日因網絡攻擊出現故障，導致食品變質。 法新社

【大公報訊】法國血液機構表示，該機構位於三處地點的冷庫遭網絡攻擊，其「溫度設定閾值和除霜閾值被調高至極端水平」。這些冷庫用於儲存尚未配送至醫院的血漿等血液製品。在監控系統發現異常後，法國血液機構及時控制或停用相關設備，並將部分庫存轉移至其他地點，因此「沒有任何血液製品或樣本受到損害」，醫療機構所需的血液服務也未受影響。

據法國《鴨鳴報》報道，攻擊發生在1日晚至2日凌晨，目標是為法國血液機構提供製冷設備維護服務的酷世界公司，遭攻擊設施包括位於勃艮第—弗朗什—孔泰大區的冷庫。

法國血液機構向該國1900多家醫院提供血液、血漿、血小板等製品，每年為超過100萬名患者提供服務，一旦其儲存的血液製品因網絡攻擊而變質失效，後果不堪設想。該機構表示，其技術團隊正與法國國家信息系統安全局及衛生部保持聯繫，並加強對所有設備運行情況的監測。酷世界公司發表聲明稱，此次事件涉及的安全漏洞「存在於第三方供應商提供的某個組件中」，不屬於該公司的直接控制範圍。

網安公司設「蜜罐」誘捕黑客

法國血液機構冷庫遭網絡攻擊的同時，歐洲多國超市依賴的製冷系統也遭到攻擊。2日凌晨，瑞典、比利時、愛爾蘭等國數十家超市的雪櫃異常升溫，大量生鮮、冷凍食品變質。3日，德國、意大利、羅馬尼亞、英國發生類似事件。上月，法國數百家超市也曾成為黑客攻擊目標。

分析人士指出，針對這些冷庫和雪櫃的攻擊手法如出一轍。但目前尚不清楚這些事件是否存在關聯，也沒有組織或個人宣稱對這些攻擊負責，或對受影響機構和企業提出勒索要求。據BBC報道，至少三家網絡安全公司已設置「蜜罐」，即看似存在漏洞的系統，用於誘騙黑客進行攻擊。其中總部位於蘇格蘭的Lupovis公司在全球範圍都部署了「蜜罐」，但只有在歐洲的「蜜罐」檢測到疑似黑客的活動。

Synacktiv公司網絡安全工程師泰利耶表示，受影響的製冷設備防護薄弱，發動此類網絡攻擊並不需要複雜的技術。因此，肇事者「可能是任何人」，甚至可能僅僅是想要搞惡作劇的青少年。亦有分析人士認為，最近的幾次攻擊集中在夜間，且規模龐大，更像是有組織、有計劃的行為。

歐洲零售商排查安全隱患

很多原本離線運行的設備，如製冷機組，如今紛紛接入互聯網，以便進行遠程操控。但部分設備較為老舊，缺乏配套防護措施，成為易被黑客攻破的薄弱環節。美國雲服務安全公司Zscaler的專家達洛伊警告說，從智能家電、汽車到電力或交通基礎設施，任何聯網設備都可能面臨類似風險。

英國國家網絡安全中心前行政總裁馬丁表示，製造商需要提升聯網設備的安全性，「我們需要對大型公司提出更多要求，讓它們從一開始就提供更安全的設備和產品」。SentinelOne公司研究員黑格爾指出，使用相關設備的零售商必須更清楚地界定責任歸屬，確定誰負責這些設備的安全。歐洲多國已發布緊急安全預警，要求零售企業第一時間切斷製冷系統的公網直連，將遠程訪問權限限制在指定可信IP範圍內，並全面排查聯網溫控設備的固件版本與弱密碼隱患。

（綜合報道）

製冷系統遭入侵事件簿

11月3日

- 法國血液機構發布公報說，近日該機構部分冷庫遭網絡攻擊，所幸監控系統及時發出警報，事件未造成血液製品損失。法媒稱，黑客將冷庫溫度設定值從零下30℃更改為110℃。

11月2日至3日

- 瑞典、比利時、愛爾蘭、盧森堡、德國、英國等多個歐洲國家超市製冷系統遭入侵，雪櫃溫度被惡意上調，導致生鮮、冷凍食品變質。

10月11日

- 法國數百家超市製冷系統遭入侵，雪櫃溫度被上調至50℃，導致大量食品變質，部分設備過熱起火。

8月下旬

- 美國境內至少6處軍事基地內超市的製冷系統突發故障，導致食品變質，五角大樓將相關事件列為「疑似黑客攻擊」。

大公報整理



大公報AI製圖

聯網設備安全風險Q&A

哪些設備可能遭入侵？

- 網絡安全專家指出，很多原本離線運行的設備如今已實現聯網，面臨新的安全風險。如果沒有適當的防護措施，無論是洗衣機、智能門鎖等家電，製冷系統、電梯、汽車等設備，還是電力、供水、醫療等行業的基礎設施，都有可能成為黑客的目標。

應如何防範？

- 聯網設備的生產廠商應提高設備安全性，在檢測到安全漏洞時及時發布補丁。
- 超市等設備使用者應及時進行軟件更新，停用老舊設備版本；提高各類賬號的密碼強度，以免遭暴力破解；審慎開放遠程控制權限，及時關閉非必要的遠程訪問功能。
- 普通消費者也應更改智能家電等設備賬號的默認密碼，在支持的情況下啓用雙重驗證，並定期安裝軟件更新。

大公報整理

法銀行遭網攻 傳8.8億資金被盜



▲法國互助信貸阿凱亞銀行日前遭黑客入侵。 法新社

【大公報訊】綜合法新社、法國《世界報》報道：法國互助信貸阿凱亞銀行4日發布公報說，該銀行日前遭網絡攻擊，目前情況已得到控制，客戶資產未受影響。暫不清楚攻擊者身份，銀行正配合司法機關和警方進行調查。據法媒報道，黑客發動「惡意交易」轉走資金，涉及金額超過1億歐元（約8.8億港元）。銀行方面則稱，尚不能確認具體涉案金額，但這一金額「不足以危及其財務穩健性」。

互助信貸阿凱亞銀行在公報中說，黑客通過外部服務商平台進入銀行系統，利用銀行自有賬戶向其他銀行機構轉賬，然後將資金兌換為加密貨幣，分散到多個交易平台上。據法媒報道，美國Kraken平台2日收到來自歐洲的異常轉賬，隨即發布警報並阻止了這筆交易。互助信貸阿凱亞銀行稱，部分涉案資金已被凍結，銀行正在採取措施追回資金。此次事件不會對客戶資產造成影響，僅導致部分轉賬操作延遲。

法國《世界報》稱，這是一次「前所未有」的網絡攻擊，暴露出歐洲銀行系統的安全隱患。韓國金融業近期亦頻繁遭黑客入侵。韓國金融部門5日表示，近一個月來，該國共有37家金融公司遭入侵，包括銀行、保險公司、虛擬貨幣交易公司等；相關事件共造成約47.3萬條信息外洩，約10億韓圓（約584萬港元）資金被盜。

歐洲一日內逾20航班遭炸彈威脅

【大公報訊】綜合美聯社、法新社報道：歐洲航空業近日連續遭遇虛假炸彈威脅，5日又有至少27個航班受影響，部分航班改降、機場短暫關閉。各國調查仍在進行，尚不能確定事件是否相互關聯。目前所有接受檢查的航班均未發現爆炸物。航空安全專家指出，一日內多國、多條航線接連收到匿名威脅「極為不尋常且罕見」，不排除是有組織或個人精心策劃的惡意行動，旨在擾亂歐洲空域。

據法媒報道，一架從愛爾蘭都柏林飛往意大利羅馬的空客A320客機5日收到炸彈威脅警報，改道飛往法國，隨後安全降落在埃夫勒空軍基地。機上151名乘客和6名機組人員均未受傷，已被轉移至安全區域，排爆人員已抵達現場。芬蘭航空一架從赫爾辛基飛往羅馬的航班由意大利空軍戰鬥機護航，安全降落在羅馬。

同日，瑞安航空3架飛往保加利亞索非亞的航班收到炸彈威脅，其中從哥本哈根和馬德里起飛的2架已抵達，從倫敦起飛的一架緊急改道保加利亞普羅夫迪夫機場。威茲航空一架從意大利米蘭飛往波蘭華沙的客機在捷克上空收到威脅，改道奧地利維也納；另一架從華沙飛往巴黎的航班在滑行時被叫停檢查，更換飛機後繼續行程。

歐洲多國航空公司近日接連收到炸彈威脅。2日，威茲航空一架從英國倫敦盧頓機場飛往保加利亞索非亞的航班收到威脅，改降匈牙利布達佩斯。北約防空系統發布警報，匈牙利空軍出動「鷹獅」戰鬥機護航，檢查後未發現爆炸物。3日，波蘭、西班牙等國相繼報告客機收到炸彈威脅，涉及至少7個航班。



◀炸彈威脅5日擾亂歐洲航空業。圖為旅客在保加利亞一家機場查看航班信息。 美聯社

全法大罷工 逾25萬人抗議生活成本危機

【大公報訊】綜合法新社、CNN報道：法國多個主要工會5日發起全國大罷工及大規模示威，抗議生活成本高漲及公共服務不足。法國總工會稱，截至當地時間5日中午，示威活動已在至少73個城市展開，超過25萬人走上街頭。法國政府高度戒備，在全國部署7萬名警力應對。

此次罷工和示威活動由包括法國總工會在內的多個工會發起，並獲得學生團體的支持，參與者涵蓋醫療、民航、郵政、教育及鐵路等行業員工。工會方面的訴求包括調升工資、加大公共服務投入、保障就業與工業發展、推動稅收公平等。

在法國首都巴黎，示威者用垃圾桶堵路，與警方對峙。受示威活動影響，艾菲爾鐵塔和羅浮宮部分展廳臨時關閉。在東南部城市里昂，示威者與防暴警察發生衝突，警方動用催淚彈和水炮車驅散人群。西南部圖盧茲附近一所高中遭縱火。

法媒稱，法國的大規模抗議已持續了一個多月。本次罷工和示威不僅涉及公共部門，也擴大至私營領域，私立教育機構工會首次加入罷工行動。法國教育部表示，全法約16%的教師參與罷工。多個城市的高中生同步發起抗議，高中生協會稱，若計入遭封鎖及因罷工停課的學校，全法停課中學多達1000所。



▲法國民眾5日舉行大規模罷工和示威。 路透社

責任編輯：王可嘉 美術編輯：賴國良