

食
髓
知
味

遭黑客勒索 全球最大肉商付8580萬

比特幣屢成犯罪工具 多國研加強監管

【大公報訊】綜合《華爾街日報》、美國NBC、CNN報道：全球最大肉類供應商JBS日前遭黑客勒索攻擊，業務受嚴重影響的美國子公司9日表示，為保護客戶資料不被洩，已通過比特幣向黑客支付1100萬美元（約8580萬港元）贖金。近一年來全球網絡攻擊事件驟增，由於比特幣等加密貨幣成黑客勒索、洗錢等非法行為常用工具，多國正考慮嚴加監管。

JBS公司5月遭到黑客組織REvil的攻擊，導致其在美國、加拿大和澳洲等地的肉類加工廠一度癱瘓。JBS美國分公司9日在聲明中證實，已用比特幣向黑客支付1100萬美元（約8580萬港元）的贖金。聲明稱，付贖金時公司絕大多數設施都能正常運行，此舉旨在減少所有與網絡攻擊有關的「不可預見的問題」發生，並確保沒有數據遭到洩露。



▲美國輸油管道運營商Colonial 5月受黑客攻擊，多州出現油荒。美聯社

DarkSide九個月斂財七億

JBS行政總裁諾蓋拉（Andre Nogueira）表示，這是個「相當艱難的決定」，但必須避免為客戶帶來任何潛在風險，並強調初步調查後沒有客戶或員工的資料外洩。

NBC報道，與許多勒索組織一樣，REvil近年通過入侵一些企業的網絡並對文件進行加密來勒索贖金。他們通常要求對方支付大量

「不可追蹤」的比特幣，以換取解密程序以及不對外洩露機密資料的承諾。REvil相信已通過這種手段斂得數百萬美元贓款。

另外，倫敦區塊鏈分析機構Elliptic追蹤DarkSide的比特幣錢包後發現，過去9個月中，該黑客組織至少從47名受害者處獲得價值9000萬美元（約7億港元）的比特幣贖金，平均每次索要190萬美元。收款後，大部分比特幣都被轉移到加密貨幣交易所，並兌換成法定貨幣。

在JBS支付贖金的消息傳出前，美國輸油管道運營商Colonial亦支付黑客組織DarkSide價值440萬美元的比特幣，公司CEO布朗特在參議院作證時說，決定是「為了國家而做的正確的事情」。

新冠疫情期间，人們普遍遠程居家工作，大大增加了

黑客通過勒索軟件獲利的可能性。歐洲聯盟網路安全局（ENISA）統計，2020年「關鍵部門」遭遇304宗重大惡意網絡攻擊事件，較前一年的146間翻倍。而在疫情期間尤為關鍵的醫院和醫療保健網絡更首當其衝，同一時期受攻擊次數驟增47%。另根據美國聯邦調查局（FBI）數據，去年黑客勒索案件達到近2500宗，同比增加66%。

黑客猖獗 醫院學校成目標

與此同時，黑客的目標也遍布各行各業，醫院、學校、律所、機場和政府機構都深受其害，例如黑客趁學校上網課時盜取學生住址、電話、社保號碼等資料來勒索校方，美國休斯敦謝爾登獨立學區去年便以20萬美元換取學生資料不被洩露。拜登政府官員直言，勒索軟件可能是美國面臨的最嚴重網絡安全威脅，是「大規模殺傷性網絡武器」。照



▲JBS在美國多州的牛肉加工廠上週遭黑客攻擊一度癱瘓，影響供應鏈。網上圖片

近期黑客勒索事件簿

巴西JBS肉廠

美國子公司5月31日遭網絡攻擊，全美多地工廠被迫停產。該廠已向黑客支付價值1100萬美元的比特幣贖金。美當局指控俄黑客組織REvil涉事。

美國Colonial管道

5月被黑客組織DarkSide攻擊，燃料供應停擺近一周，東海岸陷油荒。該公司向黑客支付價值440萬美元的比特幣贖金，司法部近日追回約半數金額。

日本東芝公司

歐洲的伺服器5月遭DarkSide攻擊，超過740GB敏感資料被竊取。

法國保險集團安盛（AXA）

5月，亞洲子公司受Avaddon勒索軟件攻擊，在香港、泰國、馬來西亞及菲律賓的業務受影響，約3TB數據被盜。

愛爾蘭醫療系統

5月遭DarkSide攻擊，計算機系統癱瘓，影響多家醫院收治病患的能力。同月，加州聖迭戈醫療健康系統Scripps Health亦遭勒索軟件攻擊，逾10萬名病人資料遭洩露。

大公報整理



網友評論

@LeChatdOsiris

如果美國政府能追回比特幣，這意味着它將因不安全而一文不值。

@BTCization

這和凍結銀行匯款或扣押資金沒什麼區別。不是你的私鑰，也不是你的幣。

@老粥科普

此消息如果屬實，只能說明兩個問題：

- 一，比特幣所謂的「去中心化」造就的安全性實際上並不安全，它的密碼是可以被美國破解的；
- 二，這是一起「左手」勒索「右手」的鬧劇，加害者與受害者都是演員。

美追回黑客贖金 打破比特幣安全「神話」

【大公報訊】綜合路透社、《金融時報》報道：美國最大輸油管道運營商Colonial此前遭網絡攻擊，被迫向黑客支付價值440萬美元的比特幣贖金。然而美國司法部7日宣布，已成功追回其中230萬美元贖金。事件意味着比特幣不可追蹤的「神話」被打破，令其安全性和去中心化遭質疑。

Colonial公司上月透露，在遭黑客勒索後幾個小時內就向黑客組織Dark Side轉賬75個比特幣，當時價值約440萬美元。而美司法部副部長摩納哥周一表示，司法部旗下新成立的勒索與數碼敲詐工作組（RDETF）已找到並追回「大



▲美國司法部副部長摩納哥7日宣布成功追回Colonial支付的大部分贖金。美聯社

部分」贖金，即63.7個比特幣，但這些比特幣價值已下跌至約230萬美元。

司法部沒有透露追回這批比特幣的方式，不

過法庭文件顯示，執法人員使用區塊鏈賬簿實時監控工具，追蹤了數筆交易並最終確認了接收贖金的比特幣錢包地址。

此外，他們還透過某種渠道，獲得了這個錢包的「私鑰」（private key，相當於密碼），成功將比特幣轉移出去。

消息公布後，比特幣等加密貨幣價格單日跌幅超10%。市場分析認為，這一事件讓外界對比特幣引以為傲的安全性和去中心化產生質疑。區塊鏈分析集團CipherTrace認為，聯邦調查局（FBI）據信已查封了DarkSide的一些服務器，這些服務器可能存放了錢包私鑰。

勒索軟件「如核武」嚇跑保險公司

【大公報訊】綜合《華爾街日報》、《金融時報》報道：近年來，隨著勒索軟件不斷更新，黑客攻擊事件的複雜性、頻率和嚴重性急劇升級，已逐漸走向「產業化」。這一現象亦促使網絡保險公司調高保費、設置更為嚴格承保條款。

《華爾街日報》指出，黑客越來越善於在所謂的暗網（Dark Web）上交流有關網絡漏洞的資訊，加上用加密貨幣支付贖金限制執法部門的追蹤能力，且賠付勒索軟件贖金的保險產品增多，都為一個日益專業化的勒索軟件產業，提供了生存的土壤。區塊鏈分析公司Chainalysis指出，2020年勒索軟件攻擊數量，較2019年增長311%。不僅是肉廠、輸油管，連醫院、學校

都中招。

美國司法部高級官員卡林（John Carlin）將勒索軟件比作「大規模殺傷性網絡武器」，與核武器一樣，其威力和破壞力都在不斷增強。卡林說，勒索軟件行動的成功讓黑客向受害者索要越來越多的贖金，並將所得錢財重新投資於新的工具和服務，以發動更多更厲害的攻擊。

另外，隨著攻擊的嚴重程度和頻率的增加，網絡保險的成本也在飆升。保險經紀公司怡安（Aon）的數據顯示，從4月初到5月中旬，保費較去年水平上漲了27%。與此同時，保險公司也提高承保門檻，例如美國國際集團（AIG）對客戶的網絡安全措施提出25個詳細問題，如果網絡安全水平非常低，可能根本不承保。

韓國虛擬貨幣騙局 7萬人損失268億

【大公報訊】據韓國《中央日報》報道：韓國近日曝出一樁以虛擬貨幣為幌子的龐氏騙局，約6.9萬人被騙3.85億韓圓（約268億港元），其中不少受騙者是老年人。涉案「V Global」公司的CEO及約70名員工正在接受警方調查。



▲韓國警方近日搜查一間加密貨幣交易所。

網上圖片

警方表示，這間公司自稱運營虛擬貨幣交易平台，勸說民眾在該平台開戶投資，最低投資額為600萬韓圓（約4.2萬港元），並承諾投資者可在短時間內收穫幾倍回報。一名警官說：「這看起來是一樁龐氏騙局。我們正在進一步調查，預期會發現更多受騙者。」不過，由於許多受騙者、尤其是老年人遲遲不肯報案，警方調查面臨不小難度。

一名40多歲的男子說，他的母親被騙投資1300萬韓圓（約9萬港元），但她總覺得能把錢拿回來，拒絕報警。由於虛擬貨幣對年長者是新事物，還有許多老年人受騙。另有一名五旬婦人說：「有個熟人告訴我這個投資機會，我就投了大約6000萬韓圓（約42萬港元）……現在我想報警，但是她勸我再等等，等賺回錢再說。」

龐氏騙局是指以承諾高額回報騙取投資者資金，並將新加入投資者的資金用於支付老客戶投資回報，卻幾乎不從事實際投資。這種金字塔式累積資金的騙術在上世紀20年代因行騙人查爾斯·龐齊而得名。