國際 深度

北韓的加密幣網絡戰：「以駭養核」走到瓶頸了嗎？

北韓不停改進洗黑錢和編程技術，但其加密貨幣核武大計，仍然起了無可預測的變數。

製圖：Mantha Mok，由midjourney生成

端傳媒實習記者 徐凱鳴 發自阿姆斯特丹 | 2023-06-06

加密貨幣　北韓

「你的一些重要文件被我加密保存了，想要恢復全部文檔，需要付點費用。一個禮拜內未付款，將會永遠

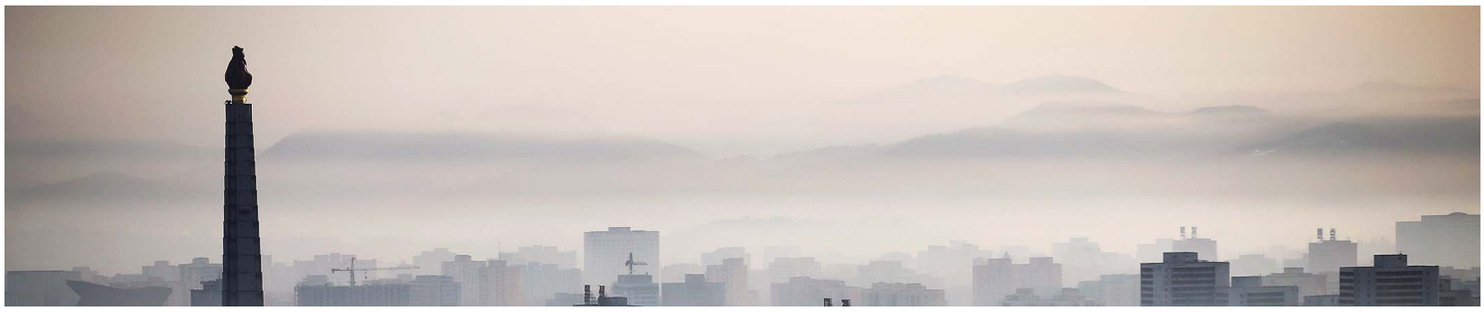
恢復不了。」2017 年 5 月 12 日中午，全球超過二十萬個Windows用家的電腦螢幕跳出一個紅色警示頁面，要求用家轉帳價值約港幣2,400元的比特幣才能將檔案解鎖。

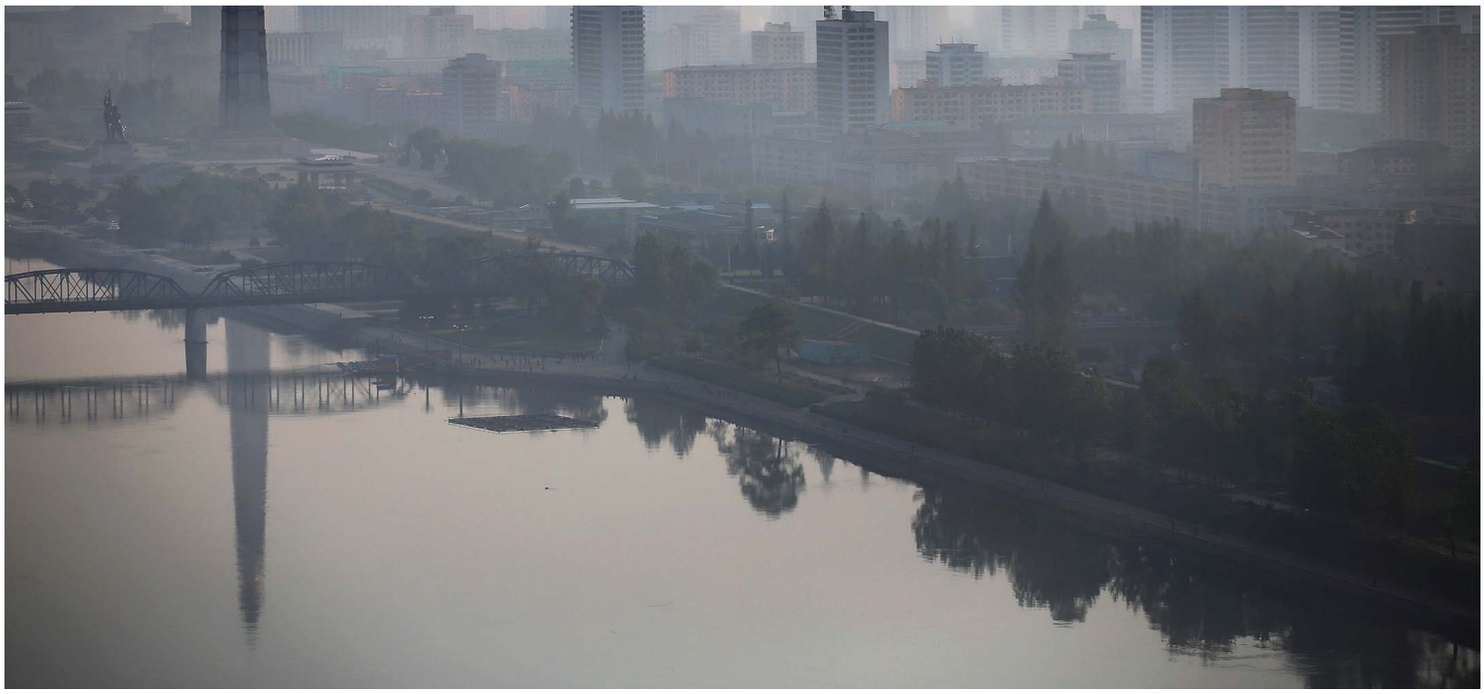
這個病毒後來被名為「WannaCry」。正當受害者都以為這是普通的加密貨幣勒索事件，美國政府則在同年年底宣布，這個席捲超過150個國家，有史以來最嚴重的加密貨幣勒索軟件網路攻擊背後的發動者，正是北韓政府旗下的黑客集團「Lazarus」。在北韓，只有少於1%的人有權使用國家內聯網服務「光明網」（Kwangmyong），但平壤政府卻培養出世界上最出色的黑客，與美國、中國、俄羅斯等主要國家並駕齊驅。近年，平壤政府看準了加密貨幣的去中心化特性，利用發展了二十年的網絡戰能力，以像「WannaCry」這樣的大型金融勒索來籌集核武資金，而且非常成功。

國際社會真正認識到北韓網絡戰的時間，是2015年1月的孟加拉銀行被駭事件。當時銀行的數名員工收到了一封看起來很普通的求職電郵，有銀行員工下載了附有病毒的履歷和求職信，成功進入了環球銀行金融電信協會（SWIFT）網絡，並發出多條指令，通過SWIFT系統冒充孟加拉央行向紐約聯邦儲備銀行提出將10億美元的資金非法轉出。可幸的是，其中一條指令企圖將資金轉到一家位於菲律賓馬尼拉 Jupiter Street 的銀行分行，而「Jupiter」這詞恰好是被制裁的伊朗船隻的名字，地址欄因而引起美聯儲注意，誤打誤撞發現這樁可疑交易而擱置其餘多條指令。然而，仍然有五筆交易順利通過，黑客們最終轉走了8100萬美元的贓款。

這次北韓在戰略上顯然比過往的DDoS攻擊成熟得多，其社會工程（social engineering）系統足足在銀行系統裏潛伏了一年收集資料，等待時機才採取行動。黑客們運用了孟加拉的周末、紐約的時差，及菲律賓農曆新年假期，爭取更多的時間把錢匯出。而收到資金後，他們選擇了將錢轉到菲律賓首都馬尼拉設立的銀行賬戶，並將大部分金額轉移到賭場，在賭桌上將資金洗淨，繼而再企圖將資金轉移到北韓。

這次孟加拉銀行搶劫案，令西方國家真正意識到北韓的網絡部隊比想像強大。但這次劫案也令北韓堅定了盜竊加密貨幣的決心－－雖然北韓最後成功提走8100萬美元，但只佔目標10億的十分一。同時，北韓經歷了繁複的洗黑錢紙程序，更意外令另外的90%目標資金白白流走。經過這次行動，北韓體會到傳統金融機構的要求的勞動力和時間消耗有多大。其後，而隨着加密貨幣的興起，北韓看中了其去中心化的特質－－這種不用經過銀行、證券商或受政府監管的金融機構的開放式金融系統，正好讓北韓繞過制裁，跳過洗黑錢的程序，直接將得來的資金放到其核武計劃中。





北韓平壤，晨霧籠罩著大同江。攝：Damir Sagolj/Reuters/達志影像

北韓的「以駭養核」計劃

平壤政府對網絡攻擊的野心可追溯到90年代。在1990年開始的波斯灣戰爭中，以美國為首的聯軍在常規武器以外，還利用電子裝備輔助，在短時間擊倒伊拉克。當時的中共看見電子戰的潛力，成立了研究小組專責探討 「電子情報戰」。一本朝鮮人民軍的出版的書籍引述當時的最高領導人金正日看到報告後說：「如果互聯網就像一把槍，網絡攻擊就像原子彈」，並發布指令，要求人民軍總參謀部發展「信息戰」能力。 而發展網絡戰的目標就是支持其核武計劃。

早在2008年，朝鮮就在人民軍參謀部偵察局內成立了「121局」（Bureau 121）。121局也被稱為電子偵察部或網絡戰指導部，負責進行網絡攻擊和網絡間諜活動，收集有關海外政治、經濟和社會的情報。121局成員皆從由北韓頂級技術學院中挑選出來，全體成員均享有朝鮮國內最高層次的待遇。2009年，朝鮮將其所有的情報和內部安全部門合併為「朝鮮人民軍總參謀部偵察總局」（Reconnaissance General Bureau，RGB），121局也收歸其中。據估計，121局現時有3000至6000名員工，分佈在中國、印度、馬來西亞和俄羅斯等不同國家。 而121局旗下則分成不同單位，專研不同技能和工具，負責不同類型的任務；例如「APT 37」和「Kimsuky」專門從事政治網絡間諜活動，而發動Wannacry攻擊的Lazarus則專注於金融勒索和網絡犯罪。

2012年，金正恩上台，繼承了父親發展網絡戰的野心。上台翌年，金正恩公開宣稱，網絡戰、核武器和導彈都一樣，都是「一把萬能劍（all-purpose sword）」，有了其「無情瞄準能力」，北韓軍隊便能所向披靡。這個宣言奠定了北韓至今為止以網絡攻擊為中心的戰略。

北韓歷年網絡攻擊事件

2007

3月 **Lazarus集團開始開發第一代惡意軟件**

2009

7月4日 **Operation Troy**
發動針對韓國和美國主要政府、新聞媒體和金融網站的DDoS網絡攻擊。此為北韓首次有紀錄的網絡攻擊。

2011

3月 **Ten days of Rain**
為期十天的的DDoS攻擊，目標針對韓國的媒體、金融和關鍵基礎設施及駐南韓美軍。

3月20日 **DarkSeoul**
南韓多間電視台及銀行的電腦遭到癱瘓，自動提款機和流動裝置付費機制也受影響。南韓通訊監察單位將事件提高警戒等級至3級（最高為5級）

2013

9月 **Kimsuky campaign**
北韓旗下Kimsuky集團透過魚叉式網絡釣魚電郵向多個南韓智庫發放木馬程式

2014

1月 **入侵南韓多部電腦**
北韓旗下黑客組織APT37入侵160家韓國公司和政府機構的14萬多台電腦，植入惡意代碼，盜竊了4萬多份與國防有關的文件，包括F-15戰鬥機機翼的藍圖。

8月 **Channel 4 攻擊**
英國電視台Channel 4 宣布開拍一個涉及英國核科學家被北韓俘虜的電視節目。北韓入侵製作公司Mammoth Screen的電腦系統，使該電視節目隨後被取消。

11月 **索尼影業攻擊**
索尼影業（Sony）發布電影《刺殺金正恩（The Interview）》預告片，內容講述中情局刺殺金正恩的故事。北韓旗下的Lazarus入侵索尼電腦系統，凍結多部電腦，並在網上公開盜取的大量機密資料。電影隨後取消拍攝。

2015

10月 **越南先鋒銀行盜竊案**
Lazarus入侵越南先鋒銀行（Tien Phong Bank）並試圖盜取超過100萬美元，交易被銀行截獲。

2016

4月 **孟加拉銀行盜竊案**
Lazarus入侵孟加拉銀行，將其開設於紐約聯邦儲備銀行的賬戶中近10億美元的資金非法轉出，最後35條指令中的30條被紐約聯邦儲備銀行擱置。

8月9日 **南韓國防綜合數據中心攻擊**
北韓黑客入侵南韓的國防綜合數據中心，盜取了235GB的機密軍事計劃，包括刺殺朝鮮獨裁者金正恩的計劃

2017

波蘭金融監管機構
Lazarus集團以惡意軟件滲透波蘭金融監管機構網站

2月 **Bithumb盜竊案**
北韓黑客從韓國加密貨幣交易所Bithumb竊取價值700萬美元的加密貨幣

4月 **攻擊美國國防承包商**
Lazarus發送一系列針對美國國防承包商的網絡釣魚郵件

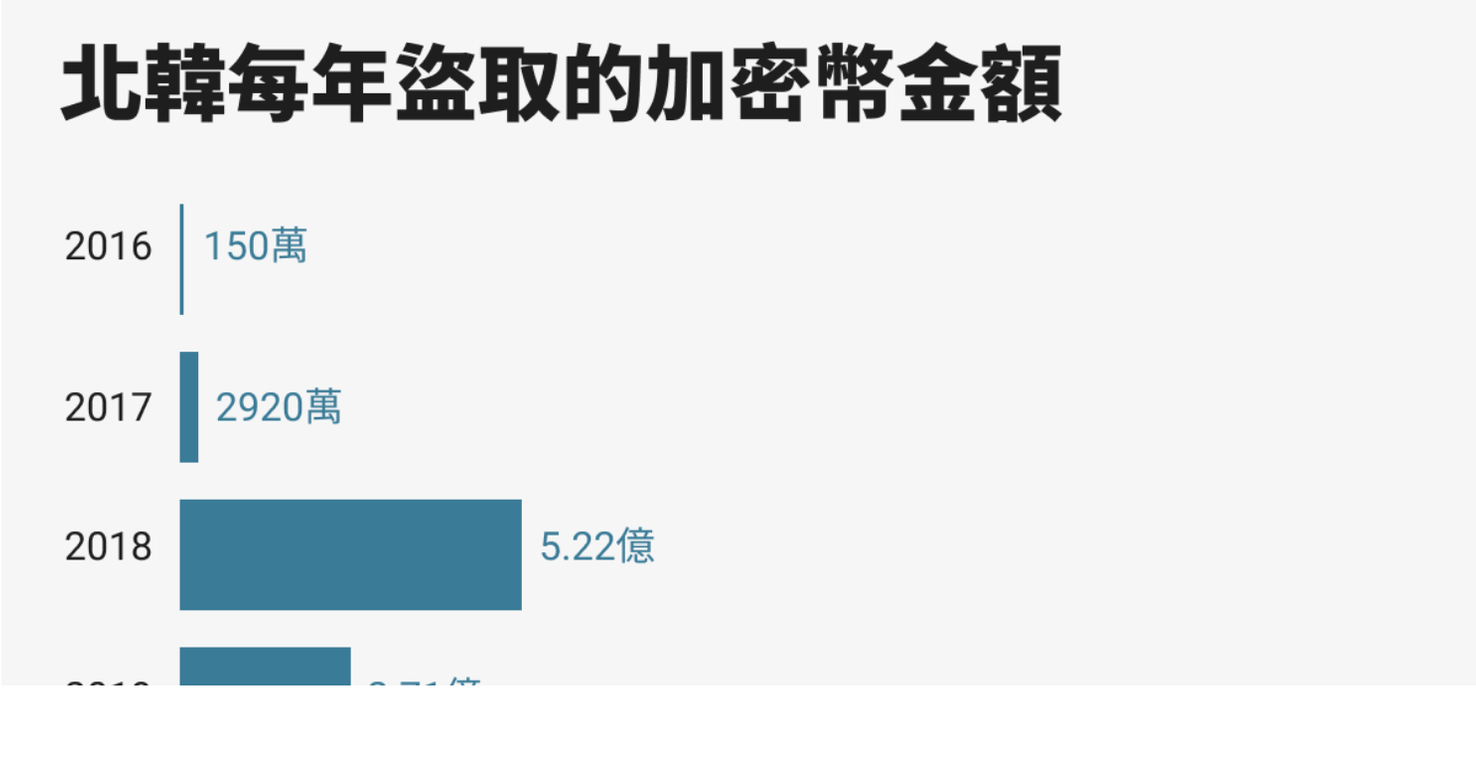
資料來源：端傳媒綜合整理

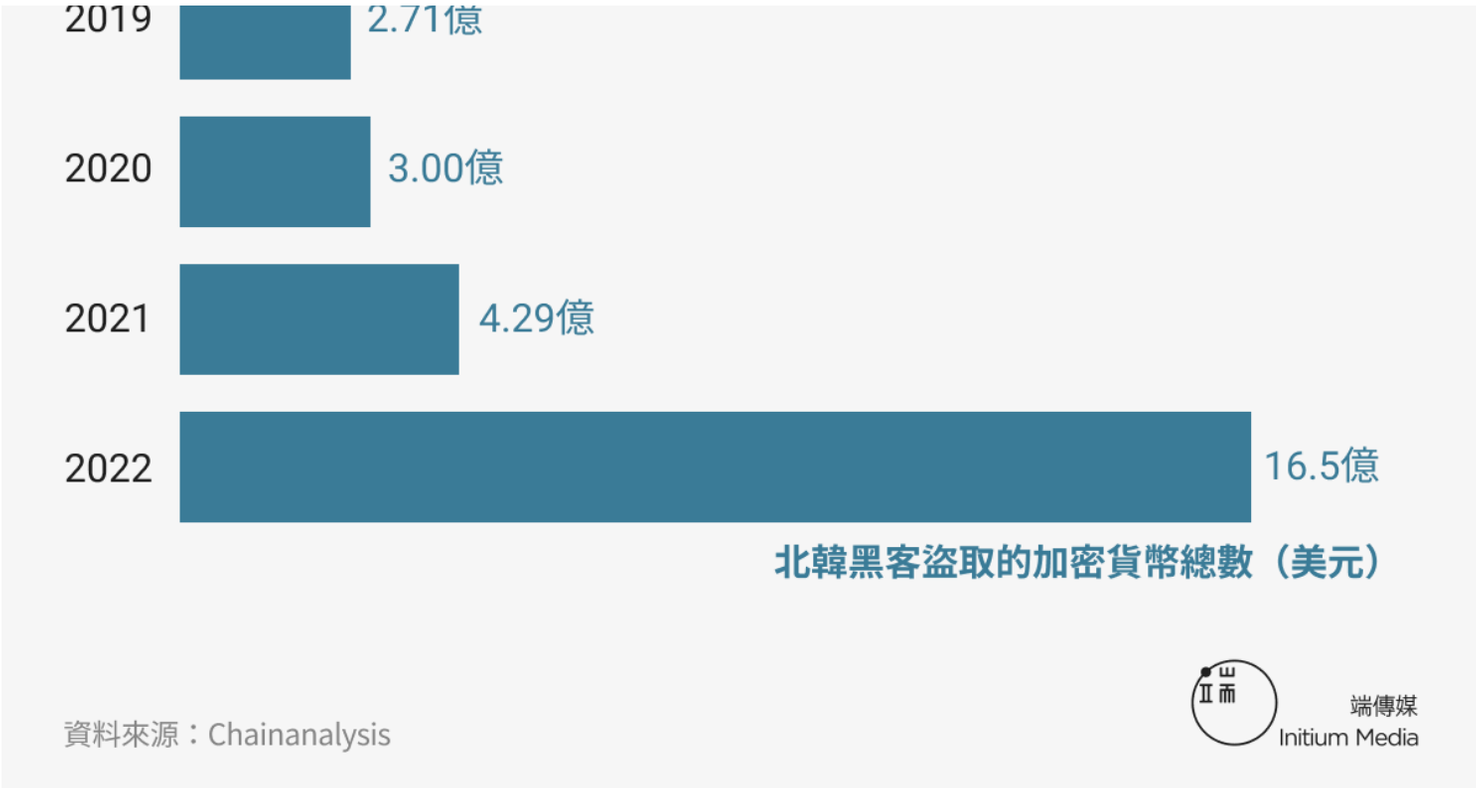
端傳媒 Initium Media

北韓最早的有記錄網絡攻擊是2009年針對南韓的「特洛伊行動」（Operation Troy）。在發現網戰威力的初期，平壤政府傾向於在國際舞台上展示其網絡能力，也因為當時北韓正值第二次核試驗，無論在軍事政策上還是網絡戰略，平壤政府也採取了激烈的立場，彷彿毫不擔心遭到報復。而在2013年至2016年期間，北韓的網絡活動越來越傾向於收集信息，多次向其主要敵人南韓及美國發起DDoS攻擊－－短暫擾亂甚至癱瘓政府機構、電力基礎設施、軍事系統等運作。網絡間諜活動在這時期極為頻繁，僅對南韓就進行了至少六次重大間諜攻擊。

多次的攻擊經驗後，北韓逐步磨練了黑客技術，攻擊對象漸漸再不限於南韓和美國，手段也不再只限於DDoS，平壤政府看到網絡攻擊的真正潛力後，就更大力發展黑客活動，目的是籌集核武資金－－以網絡攻擊獲得的資金，成為了平壤政府維持其獨特「國際地位」的資本。而在2015年後，北韓更逐漸從攻擊傳統銀行和金融機構，轉向盜取去中心化的加密貨幣，用來繼續為大型核試籌組資金。

美國副國家安全顧問Anne Neuberger估計，北韓盜取的加密貨幣中，約有三分之一用於其武器計劃。聯合國報告亦指朝鮮以網絡攻擊竊取的加密貨幣，是平壤的核和彈道導彈計劃的「重要收入來源」。路透社早前引述聯合國一份不公開的報告，指北韓在2022年內竊取的加密貨幣，價值創歷年新高；區塊鏈分析公司Chainalysis使用公開的區塊鏈數據來追踪交易，查出北韓黑客單在去年，便盜竊了17億美元的加密貨幣。對比北韓在2020年的出口總額只有1.42億美元，可見加密貨幣黑客攻擊已成為北韓國庫收入的主要來源。





根據路透社早前報道，北韓領導人金正恩下令增加武器級核原料以提升國家核軍火庫，而美國智庫「北緯38度」（38 North）3月公布的衛星影像顯示，北韓主要核設施有著高度的活動。北韓單在2022年就發射了至少90枚導彈，數目創出歷史新高，美國和南韓政府亦認為第七次核武器試驗的準備工作已經完成。北韓核武的高速發展正正歸功於金正恩政府善用網絡攻擊這把「萬能劍」－－長年專注訓練黑客網軍，以網絡攻擊盜取大量資金，目標由政府機構，金融機構，以至wannacry的普羅網民，皆無一倖免。

DeFi：北韓的新收入來源

在傳統金融業，法定貨幣如美金和港幣皆由中央機構發行，要作出金錢交易需要依賴金融機構，例如透過銀行提存法定貨幣。相反，加密貨幣則建基於區塊鍊技術上，並非由任何中央機構發行，也能匿名創建用以接收和匯出資金的的錢包，不依靠銀行來驗證交易。而當用家轉移加密貨幣資金時，交易會被記錄在一個「分散式帳本（Distributed ledger Technology，簡稱 DLT）」中，而該帳簿也不由單一機構持有，而是分佈於對等式網絡（peer-to-peer， 簡稱 P2P）上，當中每個節點都複製及儲存與賬本完全相同的複本，任由互聯網使用者查閱。

加密貨幣「匿名性」和「去中心化」的特質意味着，盜竊加密貨幣的話，便不會再重覆孟加拉銀行的事件－－即再也沒有美聯儲來阻止他們提取8.51億美元。

Wannacry 攻擊成功盜取了6.25億美元的加密貨幣，使Lazarus更堅決要將攻擊重心轉移到加密貨幣目標。起初，他們的目標主要是加密貨幣交易所。儘管黑客的目標不再是傳統金融機構，手法仍是大同小異

– –以社會工程網絡釣魚將受到感染的檔案設法植入到目標公司的電腦，從而進入公司的電腦系統以從其錢包轉走大筆金額，當資金進入北韓控制的地址後，黑客便開始洗錢過程。

北韓歷年的加密幣網絡攻擊

2017

5月 **WannaCry勒索軟件攻擊**

9月 **南韓加密貨幣交易所攻擊**

Lazarus集團以釣魚郵件攻擊包括Bithumb在內的數個南韓加密貨幣交易所，盜竊了最少 700 萬美元。

2018

Operation Sharpshooter

目標涉及世界各地的政府部門、電信、能源、國防和其他組織，將木馬程式植入到受影響的組織。

4月 **Gate.io Hack**

Lazarus黑客通過釣魚電郵活動入侵一加密貨幣交易所，共盜取了當時價值近2.3億美元的加密貨幣資產。該交易所從未公開公司身份，根據推斷很可能是Gate.io。

2019

3月 **DragonEx Hack**

新加坡的交易所DragonEx被黑客攻擊，損失了大約700萬美元的幾種加密貨幣。

2020

5月 **UpBit Hack**

黑客針對加密貨幣交易所UPbit的韓國用戶，盜取了342,000個以太幣（ETH），當時接近4500萬美元。

9月 **KuCoin Hack**

新加坡的交易所KuCoin被黑客攻擊，損失了價值超過2.8億美元的各種加密貨幣。

2021

8月 **Liquid Exchange**

日本加密貨幣交易所Liquid.com宣布，一名未經授權的用戶進入了交易所管理的一些加密貨幣錢包，其後67個不同的ERC-20代幣，以及大量的以太幣和比特幣，從這些錢包轉移到了由代表朝鮮的一方控制的地址。

2022

1月 **Qubit Finance**

北韓黑客利用QBridge代碼的漏洞，轉走了價值大約8000萬美元的BNB幣及數種BEP-20代幣。

6月 **Harmony Bridge 攻擊事件**

北韓攻擊Harmony 與以太坊之間的跨鏈橋「Horizon」，竊取 11 種 ERC-20 代幣以及 13,100 枚 ETH，受害金額當時高達 1 億美元。

資料來源：端傳媒綜合整理

端傳媒 Initium Media

隨着加密貨幣的興起，全球亦出現大量集中式加密貨幣交易所（Centralized Exchanges，CEX），方便用家使用美元等法定貨幣購買加密貨幣，或者用一種形式的加密貨幣交換另一種形式的加密貨幣，以及加密貨幣替換成法定貨幣。這種加密貨幣交易所跟傳統銀行運作模式相似，用家先在交易所開設錢包，再匯入存款作為交易資金，用家可以在交易所內作出交易，亦可將存款匯出到別的交易所或是自己的離線加密貨幣錢包。這也意味着，這種集中式交易所跟傳統銀行一樣，客戶需要提供實名認證，而交易所也持有所有資金流動紀錄。所以不論盜取加密貨幣有多容易，北韓仍需投放大量資源鑽研洗錢技巧。

要入侵加密貨幣交易所不難，真正的挑戰在於如何將加密貨幣兌換成現金以購買核武材料。值得國際社會關注和擔憂的，並非誰是北韓的攻擊目標，而是北韓日漸成熟的洗黑錢手段－－如何在轉換法定貨幣之前，盡可能隱藏區塊鍊上的資金流向紀錄，令調查人員無法追溯資金來源。

起初數次攻擊，Lazarus通過編寫自動程式（automation scripts） 執行剝離鏈（peel chain）洗黑錢。「剝離鏈」是指將盜來的大額資金逐少而密集地轉移到不同的加密貨幣地址，以小額交易避過交易平台的注意。同時，黑客亦問始使用混幣器 （mixer）。加密貨幣混幣器用意在於透過將一筆加密貨幣交易與其他交易混合，從而減低第三方發現交易源頭的可能。

然而，這個洗黑錢流程仍然存在漏洞，北韓多次重複使用了相同的混幣器，令調查人員使更容易推斷出組織的洗錢模式。加上前任美國總統特朗普於2017年擴大了美國單方面制裁的範圍，任何人士或公司假如跟北韓有業務聯繫，在美國的資產皆會被凍結。各國企業因擔心失去進入美國市場的機會，傾向停止與北韓進行交易，有效地切斷了北韓與全球金融體系的聯繫，使平壤政府選擇起用「場外交易經紀人」協助將被盜的加密貨幣資金兌現為法定貨幣。在這次攻擊中，便有兩名中國公民田寅寅（Tian Yinyin）和李家東（Li Jiadong）協助將被盜的加密貨幣兌現為法定貨幣，而被美國財政部制裁，凍結他們在美國的資產，並禁止美國人與他們從事交易。

2020年9月，新加坡一家名為KuCoin的加密貨幣交易所的網絡安全遭到大規模破壞，黑客從該交易所的錢包中竊取了價值超過2.8億美元的加密貨幣，當中以太坊區塊鏈的ERC-20代幣為主。佔2020年所有被盜加密貨幣的一半以上。在這次攻擊中，Lazarus開始使用Defi服務Uniswap。Uniswap是最大的去中心化ERC-20代幣交易平台（DEX），通過使用智能合約，讓用家可以從一個地址向Uniswap發送資金，就能在同一地址收到另一種代幣。以被盜的ERC-20代幣 LINK為例，黑客將被盜的LINK從地址A發送到Uniswap，以將其轉換成以太幣，同一地址會收到同等價值的以太幣。因此，如果調查人員不知道黑客控制了哪些收發資金的錢包，就很難追踪這些資金的流動。

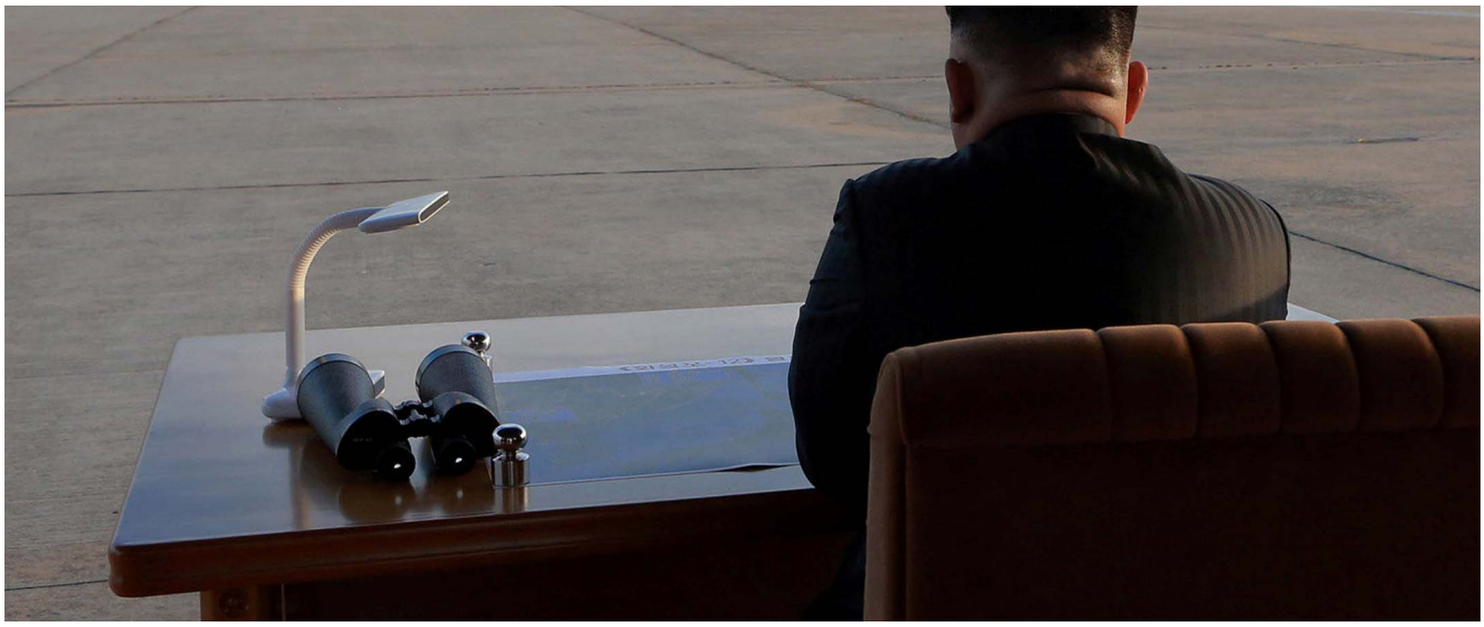
DeFi全名為「Decentralized finance」，即「去中心化金融」，意思是不依賴交易所或銀行等受監管的金融機構，而是利用區塊鏈上的智能合約（smart contract）讓用戶自由進行金融活動，例如是將一種加

密貨幣換成另一種加密貨幣。嚴格來說，DeFi服務不是一個機構，而是一組在以太坊區塊鏈上執行的電腦程式，所以不需要保管資金，也不需要中心化的基礎設施或人力。與集中式交易所不同，端對端的性質，使DeFi交易幾乎是即時發生的，以致很少有機制防止不正當交易，而且，許多DeFi平台不需要客戶提供「客戶身分審查」（KYC，Know your customer）信息，這些特質對於北韓匿名轉移資金全部非常有利。

北韓黑客對加密貨幣不斷變化的監管措施適應迅速，同時在混幣器以外開始使用跨鏈橋（Cross-chain bridge），讓資產在區塊鏈之間移動。加密貨幣的「分散式帳簿」存放於區塊鏈中，而目前通用的區塊鏈不止一條，除了最有名的區塊鏈比特幣和以太坊之外，還有各種公鏈陸續冒出，例如 Solana、Terra、Binance Smart Chain 等。 這些區塊鏈是獨立和互不相通的，例如在以太坊上的資產，若不使用跨鏈技術，就無法轉移到其他區塊鏈。以傳統金融系統作比喻，情況就像要將資產由香港的銀行轉移到美國的銀行，我們需要使用銀聯等服務。但跟銀聯不同的是，去中心跨鏈橋不受任何中央機構監管，也不需實名認證。同時，跨鏈橋亦能將北韓持有的加密貨幣轉換為Monero、Dash和Z-Cash等匿名加密貨幣，以減低交易的可追溯性，讓追踪資金流動變得更複雜。

例如，北韓會將盜來的ERC-20代幣以混幣器打散，再將打散後的代幣換成比特幣，然後再次使用比特幣混幣器，繼而將多次混合的比特幣合併到新的錢包中。最後一步就是將資金存入亞洲監管較鬆散的加密貨幣交易所，換成人民幣等法定貨幣，或是聘用「場外交易經紀人」協助洗錢。雖然北韓仍然需要依賴中心化交易所或第三方的協助，但透過DeFi、混幣器和跨鏈橋等技術，要追溯資金來源的困難度大大提高。

跨鏈橋除了是北韓的洗黑錢工具，更進一步成為了黑客的攻擊目標。Lazarus在2021年及2022分別攻擊Ronin Network和Harmony Bridge兩個跨鏈橋。像大多數跨鏈橋一樣，這兩個跨鏈橋使用權威證明（proof-of-authority，PoA）技術，原理是預先指派一定數量的驗證者（validator）運行驗證器節點（validator node），而只有驗證者才有權限驗證交易和將新區塊添加到區塊鏈。用家要進行交易，要先向智能合約發起交易，並提交到驗證者網絡，然後收到交易請求的驗證者會簽名，一旦有足夠的驗證，該區塊鏈中就會添加一個新的區塊，代表交易請求被接納。以Ronin Network攻擊為例，Ronin由 9 個驗證器節點組成，Lazarus入侵系統，偷取了智能合約當中五個管理密鑰，成功假冒了5個簽名，將當時價值超過6.2億美元的加密貨幣竊取到手。



2017年9月16日，北韓領導人金正恩在觀看導彈發射。攝：KCNA via Reuters/達志影像

加密幣監管愈加嚴密，北韓的「以駭養核」計劃會否受到威脅？

然而，儘管北韓不停改進洗黑錢和編程技術，其加密貨幣核武大計仍然起了無可預測的變數。

在北韓改進加密貨幣能力的同時，執法部門對加密地址網絡追踪資金的能力也同步增強，陸續開始追回贓款。挪威警方在今年查獲了北韓從Ronin Network攻擊盜得的價值580萬美元的加密貨幣。而美國聯邦調查局也聯同加密貨幣組織作出調查，追踪到北韓試圖將被盜資金轉換為法定貨幣的地點，並與執法部門和業內人士聯絡，凍結了超過3000萬美元的加密貨幣，使北韓透過攻擊交易所拿到手的資金白白流走。這既反映了聯邦調查局和其他機構不斷增強的能力，也反映了美國對打擊北韓網絡攻擊的重視。

Chainalysis的的高級調查主任Erin Plante對記者表示，預計未來幾年同樣的情況陸續有來。「這是因為區塊鏈的透明度。每筆交易都被記錄在公共賬簿中，意味著追查資金去向不受時間限制，可以在案發多年後仍然能追回資金。加上外國資產管制處等機構努力切斷黑客首選的洗錢服務與加密貨幣生態系統的其他部分，意味著這些黑客將隨著時間的推移變得越來越難，越來越沒有成果。」

其次，無論北韓持有多少加密貨幣，要使用資金的話，仍然必須將貨幣兌換成現金。全球第二大加密貨幣交易所FTX繼而在年尾宣布破產，隨即被揭露資產負債模糊不清，創辦人私下挪用客戶資產，引起擠提。FTX的醜聞驅使各地政府對加密貨幣行業作出更大的監管審查，使加密貨幣更符合傳統的金融體系及其監管結構，意味着北韓要將資金轉成法定貨幣的難度將大大提高。

例如美國財政部已開始將制裁目標由平壤政府擴大到混幣器。執法機構在追踪資金的過程識別出北韓經常使用的混幣器，2022年，美國財政部下令凍結北韓常用的混幣器 Tornado Cash 和Blender.io的資產，

並禁止美國公民使用 Tornado Cash 平台。加密貨幣行業以致全球經濟均受到影響，有加密貨幣貸款機構申請破產，或是暫停發放新貸款。

加密貨幣價格的不確定性也為北韓的核武大計帶來了變數。2022年中，加密貨幣價值突然暴跌，而隨着FTX的消亡，加密貨幣行業發展變得更不可預測。除了一眾投資者大失預算，平壤政府的武器計劃亦受到影響。Google旗下網路安全公司首席分析師Luke McNamara指出，北韓習慣將盜來的加密貨幣換成另一種加密貨幣，而各種貨幣的價格變動是獨立的。所以，網絡攻擊中涉及的不同資產價格變動相互關聯，因此我們沒有辦法得知北韓實際持有多少金額。但根據Chainalysis分析，北韓在2017年至2021年間49次黑客攻擊盜得的資金，當中未被清洗的加密貨幣價值自2022年初以來已從1.7億美元降至6500萬美元。

印度軟件公司Subex的網絡安全部門Sectrio表示，有跡象表明北韓在最近數月又開始加強對傳統銀行的攻擊。Chainalysis的的高級調查主任Plante亦指，其團隊看到朝鮮黑客對非加密貨幣平台的攻擊有所增加，而原因很大機會是日漸收緊的制裁和扣押被盜資金。

McNamara預計，北韓對加密貨幣行業的攻擊並不會減少。加密貨幣仍是一個非常新的產業，因此不同類型的投資者投入了大量資金到不同的區塊鍊項目，但區塊鍊的資訊保安卻沒有趕上區塊鍊技術發展，沒有好好徹底審查或測試的程式代碼。同時，北韓政府旗下不同黑客集團互相協作也使執法部門追查資金困難增加。McNamara指出，調查團隊進行分析的第一步，就是從惡意軟件的代碼入手，分析程式出自哪組開發人員的手筆。但北韓的網絡攻擊，我們會看到不同黑客集團重覆使用同樣的代碼，令我們難以評估攻擊出自哪個團隊。

「儘管加密貨幣市場存在的巨大的波動性，有商機就有投資者。北韓便是看準了這一點，對於各項目系統背後的軟肋進行了攻擊。所以只要市場上持繼出現新的區塊鍊項目，加密貨幣仍然會對北韓有很大的吸引力。」McNamara對記者說。