Gli hacker nordcoreani hanno messo a segno il colpo del secolo

Miliardi riciclati in crypto: rubati in una ditta di Dubai

A cura di
STEFANO PIAZZA

Il 3 marzo scorso, alcuni esperti di analisi blockchain hanno confermato che gli hacker nordcoreani sono riusciti a trasferire con successo la maggior parte dei 1,5 miliardi di dollari in criptovalute rubati dall'exchange Bybit, con sede a Dubai, verso nuovi portafogli digitali. Questa operazione ha oscurato l'origine dei fondi, rendendo ancora più complesso il lavoro delle forze dell'ordine per rintracciarli e recuperarli. Negli ultimi anni, i cybercriminali nordcoreani hanno affinato le loro tecniche di furto nel settore delle criptovalute, alimentando il timore che Pyongyang stia acquisendo maggiori risorse per aggirare le sanzioni economiche e sostenere il suo pericolosissimo programma nucleare. Per decenni, il regime di Kim Jong Un ha usato test sulle armi, conflitti di confine e atti di terrorismo come strumenti di pressione per attirare l'attenzione internazionale e alimentare le tensioni. Successivamente, Pyongyang sfrutta queste crisi per ottenere concessioni economiche e politiche in cambio di una riduzione delle ostilità. Oggi, la Corea del Nord ha il potenziale per integrare gli attacchi informatici in questa strategia. Già nel 2012, Kim Jong Un avrebbe definito la guerra cibernetica la "spada multiuso" del paese, capace di "colpire senza sosta". Nel decennio successivo, il regime ha affinato le sue capacità informatiche per ottenere vantaggi finanziari, politici e strategici, consolidando così la propria posizione e prolungare la sopravvivenza del regime di Kim.

Il più grande furto

Come rivelato dai media USA a fine febbraio, Bybit ha rivelato di aver subito una grave violazione della sicurezza, che ha portato al furto di quasi 1,5 miliardi di dollari nella criptovaluta Ether, il principale token sulla blockchain di Ethereum. Secondo gli esperti di Chainalysis, società specializzata in intelligence blockchain, si tratta del più grande furto di criptovaluta mai registrato. L'ammontare sottratto in questo singolo attacco supera il totale delle 47 rapine informatiche avvenute nel 2024. Tra il 2017 e il 2023, la Corea del Nord ha orchestrato 58 attacchi informatici, colpendo soprattutto aziende del settore crypto e sottraendo complessivamente circa 3 miliardi di dollari in asset digitali.Pochi giorni dopo l'attacco, l'FBI ha attribuito l'operazione a gruppi di hacker nordcoreani, avvertendo che stavano « rapidamente convertendo i fondi rubati in Bitcoin e altre criptovalute». In passato, questi gruppi hanno sfruttato exchange di criptovalute e istituti bancari cinesi per riciclare il denaro, come evidenziato da un'incriminazione federale e dalle sanzioni imposte dal Dipartimento del Tesoro a due complici di Pyongyang. Nell'ultimo attacco, dopo aver sottratto i fondi da Bybit, gli hacker hanno utilizzato exchange decentralizzati e ponti cross-chain per convertire parte dell'Ether rubato in Bitcoin, secondo un'analisi di TRM Labs. Sebbene l'azienda sia riuscita a tracciare i primi movimenti, ogni transazione successiva che coinvolge portafogli e valute diverse rende sempre qausi impossibile rintracciare gli 1,5 miliardi di dollari sottratti. L'ultimo attacco informatico si inserisce perfettamente nella lunga storia di crimini finanziari attribuiti alla Corea del Nord.

Quasi impossibile rintracciare gli 1,5 miliardi di dollari rubati dagli hacker nordcoreani

L'obbligo di generare entrate

Un gruppo di esperti delle Nazioni Unite, focalizzato sul programma nucleare di Pyongyang e sulle sue tattiche per eludere le sanzioni internazionali, ha avvertito già lo scorso anno che il regime nordcoreano ordina esplicitamente ai suoi hacker di generare entrate per sostenere il governo. Negli ultimi dieci anni, la Corea del Nord ha progressivamente integrato il cybercrimine finanziario nella strategia propria offensiva, utilizzando attacchi informatici non solo per raccogliere fondi, ma anche per ottenere informazioni cruciali a supporto dei suoi programmi missilistici e nucleari. Le ingenti riserve di criptovaluta accumulate da Pyongyang destano ulteriori preoccupazioni, soprattutto per le loro implicazioni a lungo termine. Questi fondi, infatti, non solo proteggono il regime dagli effetti delle sanzioni imposte da Stati Uniti e Nazioni Unite, ma lo posizionano strategicamente per sfruttare i tentativi di Cina e Russia di costruire sistemi finanziari alternativi, svincolati dalle banche occidentali e dall'egemonia del dollaro. Tuttavia, per convertire la criptovaluta in denaro contante, la Corea del Nord è ancora costretta a mascherare le proprie operazioni per poter interagire con le istituzioni finanziarie occidentali. Se in futuro la Corea del Nord sarà in grado di operare esclusivamente attraverso le reti finanziarie russe e cinesi, gli Stati Uniti e i loro alleati perderanno la leva per imporre costi economici al regime di Kim Jong Un per le sue attività illecite. Per questo, affrontare la crescente resistenza di Pyongyang alle sanzioni dovrebbe essere una priorità per l'amministrazione statunitense, che mira a difendere il predominio del dollaro nel sistema finanziario globale. Parallelamente, Washington può adottare misure concrete per contrastare i furti di criptovalute che alimentano le riserve nordcoreane. Diverse aziende specializzate in sicurezza informatica e analisi blockchain stanno già collaborando con Bybit per comprendere le tecniche di hacking e riciclaggio di denaro utilizzate da Pyongyang.