«Il più grande furto di sempre»

CRIPTOVALUTE / Presunti «hacker» legati alla Corea del Nord avrebbero svuotato in pochi minuti i portafogli di Binance, il più importante «exchange» al mondo, per circa 6,3 miliardi di dollari – La piattaforma ha sospeso i prelievi e promesso di coprire ogni perdita, ma metà del bottino sfugge ai blocchi

Dimitri Loringett

«I vostri soldi sono al sicuro e stiamo coprendo ogni perdita». Così Richard Teng, co-amministratore delegato di Binance, si è rivolto su X ai clienti della più grande piattaforma di criptovalute al mondo, poche ore dopo che gli *hacker* l'avevano alleggerita di circa 6,3 miliardi di dollari controvalore, in quello che gli addetti ai lavori definiscono «il più grande furto di sempre». E non resta che credergli sulla parola, anche se sul mercato il bitcoin è scivolato ai minimi delle ultime settimane (cfr. grafico). Un colpo che arriva su un settore già in affanno: il crollo di fine 2025, ricordiamo, aveva fatto «bruciare» oltre mille miliardi di dollari di capitalizzazione.

La parola, del resto, è quasi tutto ciò che Binance può offrire per ora: depositi e prelievi sono sospesi e la ripresa è attesa entro il fine settimana. L'azienda afferma di aver accantonato 6,34 miliardi di fondi propri, di cui 5 già detenuti negli stessi *token* sottratti; il resto lo sta comprando sul mercato. «Non usiamo mai i fondi dei clienti, che quindi non sono toccati», ha ribadito Teng. Più sfumato il fondatore Changpeng Zhao, che stima in circa 2 miliardi il buco ancora da colmare: «doloroso, ma gestibile», ha scritto su X, ricordando che il gruppo possiede azioni SpaceX per oltre un miliardo.

Credere sulla parola, con Binance, non è però mai stato scontato. Nel 2023 la società si è dichiarata colpevole negli Stati Uniti di aver violato le norme antiriciclaggio e ha pagato una multa di 4,3 miliardi; Zhao ha lasciato la guida del gruppo ed è stato graziato da Donald Trump l'anno scorso. Binance, tra l'altro, non ha una sede ufficiale, ma dal dicembre 2025 è vigilata ad Abu Dhabi, la cui autorità segue «da vicino» l'incidente. In luglio Binance ha dovuto chiudere le attività nell'UE, non avendo ottenuto la licenza prevista dalle nuove regole europee (MiCAR), mentre nel Regno Unito non può accettare nuovi clienti dal 2021.

18.270
i bitcoin sottratti
In pochi minuti gli «hacker» li hanno suddivisi in 19 «wallet», con esattamente mille bitcoin ciascuno

Dove sono i soldi

Il colpo si è consumato giovedì sera nel giro di una ventina di minuti e le società di analisi TRM Labs e Chainalysis lo attribuiscono a un gruppo di *hacker* nordcoreani, noto come «TraderTraitor»; lo stesso a cui l'FBI ha imputato il furto di 1,5 miliardi all'*exchange* Bybit nel febbraio 2025. Pyongyang nega da sempre, ma secondo le autorità statunitensi e sudcoreane il regime usa da anni unità informatiche statali per spionaggio e furti con cui fa cassa. Solo nel 2025, secondo Chainalysis, gli *hacker* nordcoreani hanno sottratto criptovalute per circa 2 miliardi.

Circa metà del «bottino» rubato è già stata congelata: si trattava di *stablecoin*, le criptovalute ancorate al dollaro i cui emittenti - Tether, Circle, Ripple e World Liberty Financial, la società della famiglia Trump - possono bloccare gli indirizzi sospetti. Congelate, però, non significa restituite: le monete restano bloccate, ma non tornano automaticamente nelle casse della piattaforma. Sui restanti 3,3 miliardi Binance non si pronuncia.

Per bitcoin ed ether, invece, non esiste un emittente in grado di intervenire. Il portale di notizie specializzato *CoinDesk* ha seguito sulla *blockchain* il percorso dei 18.270 bitcoin sottratti, pari a circa 1,4 miliardi di dollari controvalore: in pochi minuti i ladri li hanno suddivisi in 19 *wallet*, 17 dei quali contengono esattamente mille bitcoin. Poi più nulla. Ieri mattina, sempre secondo *CoinDesk*, nessuno dei 19 indirizzi aveva ancora mosso un solo bitcoin. Ogni trasferimento, rileva la testata, aveva l'aspetto di un normale prelievo, con tanto di firma valida di Binance.

L'anello debole

Che fine faranno quelle monete e che uso se ne potrà fare? Lo abbiamo chiesto a Michele Ficara Manganelli, direttore esecutivo di Swiss Blockchain Consortium di Lugano e fondatore di Datamoney.ch. «Nel caso Binance non è stata violata la *blockchain* - chiarisce subito - . È stato violato un computer (secondo la stessa Binance anzitutto il portatile di un ingegnere) e da lì i ladri hanno ordinato i prelievi dai portafogli online dell'*exchange*, quelli che servono a pagare in tempo reale i clienti. L'anello debole è stato l'essere umano, non la tecnologia».

Il bottino comprende un po' di tutto, spiega l'esperto: «Ether, bitcoin, *token* minori e perfino oro *tokenizzato*. La voce più pesante è sulla rete Ethereum, circa 3,8 miliardi». Di ciò che non è stato bloccato, circa 2,4 miliardi in ether e bitcoin si trovano in portafogli già individuati e restano sotto osservazione. «Con software di analisi come Chainalysis ogni movimento viene seguito e, anche passando da un cosiddetto "mixer", servizio che rimescola le monete per nasconderne l'origine, quei fondi restano marchiati: banche e piattaforme regolamentate rifiutano di cambiarli. Potranno quindi essere spesi solo nei circuiti "sporchi", dove non si passa dai dollari ma si pagano altre attività illecite. E a caro prezzo: per svendere parte delle *stablecoin*, il ladro ha già accettato di perdere oltre il 10%».

Quanto alla tenuta del mercato, per l'esperto di IA agentica «la tecnologia ha retto e proprio la tracciabilità ha fermato quasi metà del bottino in una notte». Per Binance, osserva, la perdita vale circa il 4% di quanto custodisce. «Va difeso l'anello umano e qui l'IA agentica diventa decisiva: agenti che analizzano ogni movimento in tempo reale e bloccano in pochi secondi quelli anomali, prima che il denaro esca».

Lo «scudo» svizzero

Lontano dall'epicentro - ma non troppo - c'è Sygnum Bank. Nel gennaio 2024 il «Financial Times» aveva riferito che Binance consentiva ai grandi *trader* di custodire i propri averi crittografici presso banche indipendenti, tra cui la criptobanca zurighese (che collabora con diversi istituti in Svizzera, fra questi BancaStato e PKB Private Bank in Ticino). Da lì è nato Sygnum Protect, il servizio di custodia esterna lanciato con Binance quella primavera. Ed è proprio lì che la banca registra il primo effetto del furto: «Dall'incidente abbiamo visto aumentare gli afflussi verso Sygnum Protect», riferisce al *CdT* un portavoce, precisando che «i patrimoni dei clienti, i sistemi di sicurezza e l'infrastruttura bancaria non sono stati toccati e funzionano normalmente». Il consiglio dell'istituto zurighese è di «scegliere con cura piattaforme e custodi, tenendo conto di vigilanza, giurisdizione, sicurezza informatica e *audit*, e se gli averi dei clienti siano detenuti dentro o fuori bilancio».

L'IA apre i codici chiusi: «Non esiste sicurezza nell'oscurità»

CIBERSICUREZZA / Al recente Plan B Forum di Lugano Paolo Ardoino (Tether) ha avvertito che con l'intelligenza artificiale anche il «closed source» diventa leggibile

L'hackeraggio a Binance è soltanto l'ultimo di una lunga serie di attacchi *cyber* che ha colpito diverse piattaforme informatiche di recente. E proprio di cibersicurezza ha parlato anche Paolo Ardoino, CEO di Tether - emittente della principale *stablecoin* al mondo - sul palco del Plan B Forum a Lugano lo scorso fine settimana. Dopo aver detto che viviamo in un'epoca in cui le certezze sono sempre meno, Ardoino ha definito interessante il fatto che oggi, con l'arrivo dell'intelligenza artificiale, non esistono più i benefici degli ultimi 50 anni di ogni piattaforma o software che utilizzava codici sorgente chiusi. Ardoino ha portato l'esempio dell'attacco ai prodotti Adobe, azienda di software, dei quali è stato possibile, tramite un *tool* IA, trasformare il codice binario in linguaggio naturale, cioè in inglese, per poi ricostruirlo con un'altra IA per essere compatibile con il prodotto originale.

«

Non si può sperare
che un codice sorgente resti al sicuro solo perché è nascosto
Occultarlo all'IA è sempre più difficile
Denis «Jaromil» Roio
Fondazione Plan B

Ardoino, nella sala principale del Palazzo dei Congressi, ha aggiunto che la certezza che avevano le aziende nel beneficiare di un prodotto chiuso - del quale era molto più difficile scoprire le vulnerabilità rispetto a un software *open source* con il codice sorgente visibile - non esiste più. A oggi anche i software *closed source* possono essere decifrati e resi aperti perché con l'IA è possibile ricostruire il codice sorgente partendo dal codice binario. Quest'ultimo concetto di «ingegneria al contrario», se si dovesse tradurre in parole più comuni, lo si potrebbe paragonare, nel mondo della chimica, all'individuazione degli ingredienti partendo da un prodotto.

Ce l'ha spiegato il direttore scientifico della Fondazione Plan B, Denis «Jaromil» Roio, che abbiamo contattato per capire questa dinamica. Anche Roio, così come Ardoino, crede che la trasparenza del codice dei software o delle piattaforme possa diventare un vantaggio competitivo sul mercato. «Nel mondo della cibersicurezza - ci ha spiegato Roio - l'adagio è che non esiste sicurezza nell'oscurità». In altre parole, «non si può sperare che un codice resti al sicuro solo perché è nascosto». Anzi, «un codice *open source*, trasparente, permette a più occhi di scoprirne le vulnerabilità. E magari prima che sia troppo tardi».

E l'IA, come ci ha spiegato il direttore scientifico, sta velocizzando questo fenomeno in cui ci sono più occhi che guardano in luoghi e fattori che erano rimasti sconosciuti agli sviluppatori. Di fatto, per Roio, non puntare sulla trasparenza porta maggiori rischi, perché occultare un codice all'IA è sempre più difficile. «Allora è piuttosto meglio fare l'opposto, garantire la trasparenza del codice così da permettere a chiunque il rilevamento delle vulnerabilità».

Il direttore scientifico della Fondazione Plan B ha citato anche un recente studio della National Security Agency, l'agenzia di sicurezza nazionale statunitense, che nel maggio di quest'anno ha dichiarato che con lo sviluppo dell'IA ci troviamo in un cambio di paradigma radicale nell'ambito della cibersicurezza, e che l'orizzonte temporale non è «di anni, bensì di mesi». **Andrés Bignasca**

T P