Riciclaggio, truffe e furti: così i criminali sfruttano il mondo delle criptovalute

Chainalysis e scenari

Scambi tra token e passaggi tra le diverse blockchain per fare perdere le tracce

I ricavi da attività illecite nel 2023 sono scesi rispetto al record storico del 2022

Vittorio Carlini

Nel 2023 i crimini legati al mondo delle cripto sono calati. La riprova la offre Chainalysis: lo scorso anno il giro d'affari illegale si è assestato a 24,2 miliardi di dollari (0,34% delle transazioni totali), a fronte dei 39,6 miliardi del 2022. Sennonché, al di là del fatto che – in scia alla scoperta di nuovi illeciti oggi non individuati - il dato può aumentare, l'inchiesta di Chainalysis pone l'accento sulle diverse attività *contra legem*: dal riciclaggio alla truffa fino ai Darknet e il Ransomware.

I software malevoli

Proprio quest'ultimo, a ben vedere, è uno dei crimini che sono andati in contro tendenza. L'attacco informatico, per nascondere informazioni o bloccare l'accesso alle medesime, nel 2023 ha fruttato ai cripto pirati 1,1 miliardi (erano 567 milioni due anni fa). In generale gli assalti sono stati compiuti da soggetti più diversificati che nel passato: non solo grandi gruppi organizzati, ma anche – e sempre di più - singoli soggetti. Un contesto dove il numero di nuove varanti di Ransomware è salito a 538. L'andamento – spiegano gli esperti – è dovuto ad un mix di cause.

Il piede di porco in prestito

Tra queste, *in primis*, c'è il Ransomware as a Service (RaaS). In altre parole, similmente a quanto accade nell' industria informatica legale, c'è chi fornisce – come fosse un normale servizio - la tecnologia per compiere l'illecita intrusione a chi non ha gli strumenti. Poi, se il colpo riesce, una parte del malloppo serve a pagare il servizio. Non solo. Chainalysis sottolinea che c'è anche chi (cosiddetti "Initial access broker") è specializzato nell'ottenere, e vendere, l'accesso non autorizzato a reti e sistemi. Di nuovo, un meccanismo che aiuta a commettere il reato. In un simile contesto, le competenze tecnologiche per diventare un cyber pirata giocoforza calano, e di molto. Quindi non stupisce come il mondo del Ransomware sia pervaso non da geniali criminali, bensì da "ladri di cripto polli" hi tech. I quali rischiano, però, di farla franca.

I mercati oscuri

Così come rischia di riprendere quota il mondo dei darknet market. Cioè: dei mercati online illegali, creati nelle pieghe del "web oscuro", dove non di rado si fa uso delle cripto valute. Nel 2023 il fatturato di queste piattaforme è stato di 1,7 miliardi di dollari, in rialzo rispetto al 2022. La crescita, va sottolineato, è anche e soprattutto l'effetto dell'onda lunga - nel 2022 - della chiusura del darknet market Hydra. Nel passato queste piattaforme illegali avevano un business generalizzato e diversificato: dal traffico di droga al riciclaggio fino all'attività legata all'uso di software malevoli. Così è sempre accaduto che, quando la polizia, ha tirato giù la "serranda elettronica" di un mercato oscuro, questo è stato sostituito da un altro marketplace generalista. Sennonché, dopo l'intervento su Hydra il nuovo Re non si è fatto avanti. Anzi! Si sono rafforzati singoli, minori luoghi di scambio per specifici illeciti. In tal senso, può ricordarsi che Mega Market è diventato il leader per la domanda ed offerta di stupefacenti. Kraken market (che nulla ha che fare con la nota Borsa Usa), invece, è tra i luoghi virtuali dove è possibile "offuscare" i flussi di denaro. In un simile scenario, è normale che i ricavi generali dei darknet market siano scesi.

Il riciclaggio

Analogamente a quelli del riciclaggio che però, nel mondo cripto, rimane tra le attività illegali più diffuse. Nel 2019 il totale della cryptocurrency "lavate" - a detta di Chainalysis – era stato di 11,1 miliardi di dollari. La cifra è via via aumentata fino ad arrivare al record storico di 31,5 miliardi nel 2022. Poi lo scorso anno, per fortuna, la frenata. L'ammontare del "crypto laundering" è valso 22,2 miliardi di dollari. Cosa è successo? Anche in questo caso le motivazioni sono differenziate. Gli analisti, oltre a rimarcare come il 2023 sia stato – nonostante la ripresa del bitcoin - un con prezzi deboli e poco invitanti per il riciclaggio – puntano l'attenzione sul fatto che le strette normative, un po' in tutto il mondo, hanno dato i loro frutti. Un effetto positivo riguardo ad un illecito il quale, peraltro, è mutato nella sua esecuzione, diventando molto sofisticato.

I numeri delle attività illegali

Fonte: Chainalysis

> FURTO A NOLEGGIO
> **È diffusa l'offerta, quale servizio, di software malevoli finalizzati a realizzare attacchi hacker**

> MERCATI OSCURI
> **Dopo la chiusura di Hydra, sono cresciuti darknet market specifici per droga e riciclaggio**

Un'infinita rete

Per rendersene conto, è utile rammentare un caso concreto: l'attacco hacker Harmony. Qui il bottino realizzato è stato trasferito dalla blockchain del Bitcoin a quella di Avalanche attraverso un protocollo brigde. Cioè: detto in parole semplici, una tecnologia che consente di spostare informazioni od asset da una catena di blocco all'altra senza intermediario. Successivamente i cripto asset sono stati, dapprima "scambiati" (con uno swap) in stablecoin. E poi, sfruttando un altro bridge, ulteriormente portati dall'ecosistema di Avalanche alla blockchain di TRON. Insomma: un giro infinito che, come in molti altri casi, consente di fare perdere le tracce. Ma non è solo questione di riciclaggio.

Attenzione ai furti

Altro fronte, da sempre caldo nel cripto mondo, è rappresentato dai furti. In particolare, nella Finanza decentralizzata (DeFi). Nel 2022, attraverso 203 attacchi hacker, il malloppo portato via era stato di oltre 3 miliardi. Lo scorso anno si è scesi a 1,1 miliardi. Il motivo del crollo? Essenzialmente uno: il focus sulla sicurezza dei protocolli. Fino ad un po' di tempo fa, gli sviluppatori guardavano essenzialmente alla crescita del business e al guadagno. Dopo numerosi furti, e polemiche, la musica è cambiata: è stata data molta più importanza a controlli e test, ad esempio, sugli smart contract. Un innalzarsi delle barriere che ha ridotto l'efficacia degli attacchi.

Le truffe romantiche

Fin qua alcune considerazioni su DeFi, riciclaggio o Ransomware. Ci sono però, sempre secondo Chainalysis, da ricordare altri due mondi. Il primo è costituito dalle cripto truffe. Queste sono valse 4,6 miliardi (6,5 nel 2022). In particolare, è andata diffondendosi la cosiddetta "romance scam". Vale a dire: il raggiro romantico. No! Non si tratta di una questione tra innamorati, bensì di una situazione dove il delinquente si conquista la fiducia di una persona, spesso emotivamente debole, e lo raggira. Come? Ad esempio attraverso l'approval phishing. In altre parole: il membro della cripto Banda Bassotti induce il malcapitato a sottoscrivere una transazione malevola su una blockchain. Questa dà al ladro la possibilità di operare nel portafoglio digitale del truffato. Il quale, dopo un po', si trova nelle più tradizionali "cripto mutande". Infine: il secondo mondo. Quello, per intenderci, del finanziamento al terrorismo. La narrazione comune dice che i terroristi fanno grande uso di cryptocurrencies. Per gli esperti, però, il tema, assolutamente allarmante e da monitorare, non costituisce un parte rilevante nel mondo dei cripto reati.

© RIPRODUZIONE RISERVATA