I più grandi attacchi informatici alle criptovalute del 2024 □□

Maria Cattini | 12/03/2025 | Sicurezza digitale

Attacchi informatici alle criptovalute: Il 2024 è stato un anno difficile per il mondo delle criptovalute. Gli hacker hanno affinato le loro strategie, prendendo di mira piattaforme di scambio, servizi finanziari decentralizzati e persino giochi basati su blockchain. Sebbene le perdite economiche siano diminuite del **15%** rispetto al 2023, il numero di attacchi è aumentato. In totale, sono stati sottratti circa **1,5 miliardi di dollari**.

Come agiscono gli hacker?

Le tecniche di attacco più comuni includono:

• Email ingannevoli (phishing) per rubare dati di accesso.
• Virus e malware che infettano computer e telefoni.
• Bug nei programmi (smart contract) che permettono agli hacker di rubare fondi.
• Furto di password e chiavi di accesso.
• Truffe psicologiche (ingegneria sociale) per convincere gli utenti a rivelare informazioni sensibili.
• Attacchi con prestiti istantanei (flash loan attacks) per manipolare il valore delle criptovalute.

I bersagli principali sono stati:

• Exchange centralizzati (CEX): piattaforme di scambio di criptovalute.
• Finanza decentralizzata (DeFi): servizi finanziari basati su blockchain.
• Progetti di gaming (GameFi): giochi che utilizzano criptovalute e NFT.

I tre attacchi informatici alle criptovalute più grandi del 2024

1. DMM Bitcoin – 308 milioni di dollari rubati

Gli hacker hanno ottenuto l’accesso a una chiave segreta che controllava i fondi della piattaforma giapponese DMM Bitcoin. Secondo le autorità, il gruppo TraderTraitor sarebbe dietro l'attacco.

2. WazirX – 235 milioni di dollari sottratti

Un attacco complesso ha permesso agli hacker di manipolare le transazioni utilizzando un virus. Hanno approfittato di un errore nel sistema di sicurezza della piattaforma per trasferire i fondi senza autorizzazione.

3. Munchables – 62,5 milioni di dollari scomparsi (ma poi recuperati)

Un membro interno del team ha abusato della sua posizione per prendere i fondi della piattaforma. Fortunatamente, dopo un’indagine, i fondi sono stati restituiti.

© 2026 Coondivido — Tutti i diritti sono riservati

Altri attacchi importanti

• BtcTurk: hacker rubano 55 milioni di dollari sfruttando una chiave privata compromessa.
• Radiant Capital: un virus infetta i dispositivi di amministratori e utenti, causando perdite per 53 milioni di dollari.
• Thala (Aptos): un errore nel codice permette a un hacker di prelevare 25,5 milioni di dollari, in gran parte recuperati.
• UwU Lend: un attacco con prestiti istantanei porta alla perdita di 19 milioni di dollari.
• PlayDapp: gli hacker riescono a generare e rubare token per un valore di 290 milioni di dollari.
• Bittensor: un attacco alla catena di fornitura porta alla perdita di 8 milioni di dollari.
• Pump.fun (Solana): un hacker combina furto di chiavi private e prestiti istantanei, sottraendo 2 milioni di dollari.

Come proteggersi dagli attacchi?

Se hai investito in criptovalute o utilizzi piattaforme di scambio, ecco alcuni consigli per migliorare la tua sicurezza:

• Proteggi le tue password e chiavi di accesso. Meglio usare dispositivi sicuri come gli hardware wallet invece di lasciare i fondi su un sito web.
• Verifica la sicurezza delle piattaforme. Se un servizio non ha mai effettuato controlli indipendenti sul proprio codice (audit), potrebbe essere rischioso.
• Diffida delle email e dei messaggi sospetti. Se ricevi una richiesta inaspettata di accesso o verifica, controlla sempre l'indirizzo del mittente.
• Limita i permessi di accesso. Non concedere mai il pieno controllo dei tuoi fondi a un'applicazione o un sito web di cui non ti fidi al 100%.
• Mantieni aggiornati i tuoi software e dispositivi. Aggiornamenti e patch di sicurezza proteggono da virus e attacchi.

Il futuro della sicurezza nelle criptovalute

Gli attacchi informatici sono una minaccia costante nel mondo delle criptovalute, ma le soluzioni per difendersi stanno migliorando. Con l'adozione di misure di sicurezza più robuste e maggiore consapevolezza da parte degli utenti, si spera che i furti possano diminuire nei prossimi anni.

Se investi in cripto, informarti è il primo passo per evitare di finire nel mirino degli hacker. Restare aggiornati sulle minacce più comuni può fare la differenza tra perdere i propri fondi e proteggerli efficacemente.
Attacchi informatici alle criptovalute: Il 2024 è stato un anno difficile per il mondo delle criptovalute. Gli hacker hanno affinato le loro strategie, prendendo di mira piattaforme di scambio, servizi finanziari decentralizzati e persino giochi basati su blockchain. Sebbene le perdite economiche siano diminuite del **15%** rispetto al 2023, il numero di attacchi è aumentato. In totale, sono stati sottratti circa **1,5 miliardi di dollari**.

Come agiscono gli hacker?

Le tecniche di attacco più comuni includono:

• Email ingannevoli (phishing) per rubare dati di accesso.
• Virus e malware che infettano computer e telefoni.
• Bug nei programmi (smart contract) che permettono agli hacker di rubare fondi.
• Furto di password e chiavi di accesso.
• Truffe psicologiche (ingegneria sociale) per convincere gli utenti a rivelare informazioni sensibili.
• Attacchi con prestiti istantanei (flash loan attacks) per manipolare il valore delle criptovalute.

I bersagli principali sono stati:

© 2026 Coondivido — Tutti i diritti sono riservati

• Exchange centralizzati (CEX): piattaforme di scambio di criptovalute.
• Finanza decentralizzata (DeFi): servizi finanziari basati su blockchain.
• Progetti di gaming (GameFi): giochi che utilizzano criptovalute e NFT.

I tre attacchi informatici alle criptovalute più grandi del 2024

1. DMM Bitcoin – 308 milioni di dollari rubati

Gli hacker hanno ottenuto l'accesso a una chiave segreta che controllava i fondi della piattaforma giapponese DMM Bitcoin. Secondo le autorità, il gruppo TraderTraitor sarebbe dietro l'attacco.

2. WazirX – 235 milioni di dollari sottratti

Un attacco complesso ha permesso agli hacker di manipolare le transazioni utilizzando un virus. Hanno approfittato di un errore nel sistema di sicurezza della piattaforma per trasferire i fondi senza autorizzazione.

3. Munchables – 62,5 milioni di dollari scomparsi (ma poi recuperati)

Un membro interno del team ha abusato della sua posizione per prendere i fondi della piattaforma. Fortunatamente, dopo un'indagine, i fondi sono stati restituiti.

Altri attacchi importanti

• BtcTurk: hacker rubano 55 milioni di dollari sfruttando una chiave privata compromessa.
• Radiant Capital: un virus infetta i dispositivi di amministratori e utenti, causando perdite per 53 milioni di dollari.
• Thala (Aptos): un errore nel codice permette a un hacker di prelevare 25,5 milioni di dollari, in gran parte recuperati.
• UwU Lend: un attacco con prestiti istantanei porta alla perdita di 19 milioni di dollari.
• PlayDapp: gli hacker riescono a generare e rubare token per un valore di 290 milioni di dollari.
• Bittensor: un attacco alla catena di fornitura porta alla perdita di 8 milioni di dollari.
• Pump.fun (Solana): un hacker combina furto di chiavi private e prestiti istantanei, sottraendo 2 milioni di dollari.

Come proteggersi dagli attacchi?

Se hai investito in criptovalute o utilizzi piattaforme di scambio, ecco alcuni consigli per migliorare la tua sicurezza:

• Proteggi le tue password e chiavi di accesso. Meglio usare dispositivi sicuri come gli hardware wallet invece di lasciare i fondi su un sito web.
• Verifica la sicurezza delle piattaforme. Se un servizio non ha mai effettuato controlli indipendenti sul proprio codice (audit), potrebbe essere rischioso.
• Diffida delle email e dei messaggi sospetti. Se ricevi una richiesta inaspettata di accesso o verifica, controlla sempre l'indirizzo del mittente.
• Limita i permessi di accesso. Non concedere mai il pieno controllo dei tuoi fondi a un'applicazione o un sito web di cui non ti fidi al 100%.
• Mantieni aggiornati i tuoi software e dispositivi. Aggiornamenti e patch di sicurezza proteggono da virus e attacchi.

Il futuro della sicurezza nelle criptovalute

Gli attacchi informatici sono una minaccia costante nel mondo delle criptovalute, ma le soluzioni per difendersi stanno migliorando. Con l'adozione di misure di sicurezza più robuste e maggiore consapevolezza da parte degli utenti, si spera che i furti possano diminuire nei prossimi anni.

© 2026 Coondivido — Tutti i diritti sono riservati

Se investi in cripto, informarti è il primo passo per evitare di finire nel mirino degli hacker. Restare aggiornati sulle minacce più comuni può fare la differenza tra perdere i propri fondi e proteggerli efficacemente.

© 2026 Coondivido — Tutti i diritti sono riservati