> BACKGROUND REPORT FOR PROFESSIONALS

Binance: the biggest crypto heist in history, about $6 billion, through one engineer's laptop

They didn't crack the vault, they cracked a laptop

Event: 29 October 2026
Closed: 30 October 2026 (research revision: v1)
Made with the AI crew, reviewed by Péter
English version of the Hungarian original

Summary

On 29 October 2026, the Binance crypto exchange suffered a theft affecting about $6.3 billion in assets according to the company (about $5.9 billion according to Chainalysis), the largest crypto heist ever. According to the preliminary investigation, the attackers got from a DevOps engineer's compromised laptop to an internal service container and submitted unauthorised withdrawals from there; the company says no private key leaked, about $3 billion has been frozen, the loss will be covered from the SAFU fund and its own funds, and withdrawals are temporarily paused. Analysts (TRM Labs) attribute the heist to the North Korean TraderTraitor group; there is no official confirmation yet. The most important action for individuals: don't respond to the fake “Binance support”, compensation and fund recovery approaches expected after the heist, and never transfer funds to a “safe wallet”; for organisations: protect key people's machines and the processes that start withdrawals as carefully as the keys.

KEY FINDINGS

- According to Binance, about $6.3 billion in assets were affected (Chainalysis: about $5.9 billion), the largest crypto theft ever, roughly four times the 2025 Bybit case.
- According to the preliminary investigation, a DevOps engineer's compromised laptop was the starting point; unauthorised withdrawals were launched from an internal service container; according to the company, private keys did not leak.
- About $3 billion has been frozen (Tether 1.57 billion USDT, Circle 800 million+ USDC); Binance pledged to cover the loss from the SAFU fund and its own funds; withdrawals are temporarily paused.
- Analysts attribute it to the North Korean TraderTraitor group, which previously robbed DMM Bitcoin and Bybit through developers' machines; there is no official confirmation yet.
- No Hungarian impact is known; the main domestic risk is the second wave riding the news: fake customer support, compensation and fund recovery scams.

What happened

On 29 October 2026 (Thursday), assets began flowing out en masse from the wallets of **Binance**, the world's largest crypto exchange. Users and blockchain watchers flagged the unusual outflow first; then founder Changpeng Zhao (CZ) wrote on X that the exchange had probably been hacked; Binance then confirmed it was handling a security incident. (TechCrunch; Fortune) – **confirmed**

Key facts (status on the morning of 30 October 2026):

- **Size:** according to Binance, the estimated total impact of the incident is about **$6.3 billion**. Chainalysis revised its estimate for the moment of theft to about **$5.9 billion** ($5.912 billion); according to the firm, this is nearly four times the previous second-largest crypto heist. Both figures make it the largest crypto theft ever, ahead of the Bybit case of February 2025 (about $1.5 billion). (Binance Square – Binance News; CoinDesk; The Hacker News) – **confirmed** (the two figures are estimates using different methods, see Open questions)
- **What was taken:** according to Arkham data, the attacker wallets at one point held more than $5.7 billion, including about $1.5 billion in bitcoin, $0.9 billion in ether, about $1.5 billion in USDT and more than $0.8 billion in USDC. (CoinDesk; Fortune) – **reported** (two press sources citing a blockchain analytics firm)
- **How (preliminary investigation):** according to Binance, the starting point of the incident was most likely the **compromised laptop of a DevOps engineer** (someone who both develops and operates systems). From that machine, the attacker gained access to a **service container** (one of the exchange's internal, running software components) and submitted **unauthorised withdrawal transactions** from there. The company says there is **no sign that the wallets' private keys leaked**. Binance also said that several factors contributed and that it is still investigating the full path; it has not disclosed how the laptop was compromised, the container's role or which controls failed. (Binance Square – Binance News; CyberInsider; The Hacker News) – **confirmed** (the company's primary statement; preliminary result)
- **Freezes:** according to Binance, about **$3 billion** of affected assets were frozen on-chain together with partners; this is not the same as recovered money. Tether froze more than 1.57 billion USDT, Circle more than 800 million USDC; Ripple about $200 million in assets. (Binance Square; CoinDesk; Portfolio (in Hungarian); Cyber Security News) – **confirmed** (Tether, Circle) / **reported** (Ripple)
- **Arbitrum's** security council froze about $30.5 million linked to the "Binance Exploit", according to The Hacker News. (The Hacker News) – **reported** (single source)
- **The attacker moves the money:** according to reports, part of the assets were swapped on a decentralised exchange (Uniswap), and at least 20,000 WETH (about $44 million) were borrowed on Aave using stolen USDT as collateral, which may indicate an attempt to move funds out before the stablecoins were frozen. (CoinDesk; Fortune) – **reported**
- **Who bears the loss:** Binance says it will cover all losses from the **SAFU fund** (Secure Asset Fund for Users, a reserve set aside to protect users, reportedly about $1 billion in bitcoin) and **its own funds**; the company and CZ say user funds are safe. (Binance Square; CoinDesk; Cyber Security News) – **confirmed** (pledge; no detailed compensation plan)
- **Service:** as a precaution, Binance suspended deposits and withdrawals and revoked the affected address's permissions. According to a later update, **deposits have resumed** and **withdrawals remain paused** while the withdrawal service and related addresses are rebuilt; the company estimates they may resume within 48 hours. (CyberInsider; The Week; Portfolio (in Hungarian)) – **confirmed** (the 48-hour estimate)

- **Who is behind it:** Binance has not named a perpetrator. Blockchain analytics firm TRM Labs attributes it "with high confidence" to the North Korean state-backed **TraderTraitor** group, which it also links to the Bybit heist; Blockaid and investigator ZachXBT also point to North Korea (the Lazarus group). No evidence has been published. (CoinDesk; CyberInsider; HVG (in Hungarian); Fortune) – **reported** (analyst attribution, no official confirmation)
- **Market:** bitcoin fell 2–5%, ether 4–6%, Binance's own token (BNB) about 5–8%; according to Fortune, the reaction was relatively muted. (CoinDesk; The Week; Portfolio (in Hungarian)) – **confirmed** (the differences come from the time of measurement)
- **Next steps:** Binance promises a detailed technical post-mortem and an updated Proof of Reserves after damage control. (Binance Square; CyberInsider) – **confirmed**

Same day, separate case: the Polymarket prediction market briefly went down due to the compromise of an external software provider; the damage is about $2–3 million. According to the sources, there is no connection to the Binance case. (TechCrunch; CoinDesk)

Timeline

Date	Event	Source
March–May 2024	TraderTraitor compromises the machine of an employee at a Japanese wallet software company with a job-offer coding test; DMM Bitcoin loses $308 million (confirmed, FBI)	BleepingComputer
21 February 2025	Bybit: about $1.5 billion; a Safe{Wallet} developer's machine was compromised; the FBI attributes it to TraderTraitor (confirmed)	The Hacker News
26 February 2025	Fake SMS to Binance customers using a "Lazarus attack" pretext, urging transfers to a "safe wallet" (reported)	ForkLog
29 October 2026	Mass outflow from Binance wallets; CZ signals a probable hack; Binance confirms the incident and suspends deposits and withdrawals (confirmed)	TechCrunch; Fortune
29 October 2026	Tether (1.57 billion USDT) and Circle (800 million+ USDC) freeze funds; TRM Labs attributes the heist to TraderTraitor (confirmed / reported)	CoinDesk
Night of 29–30 October 2026	Binance states: about $6.3 billion impact, about $3 billion frozen, DevOps laptop as the preliminary starting point, no private key leaked, compensation from SAFU and own funds (confirmed)	Binance Square
30 October 2026	Deposits resume, withdrawals paused, estimate: within 48 hours; Chainalysis puts the theft at about $5.9 billion (confirmed)	CyberInsider; The Hacker News

Actors and background

- **Binance:** the world's largest crypto exchange; according to 2025 data, about 335 million registered users and around $160 billion in customer assets. According to DefiLlama, the stolen amount is roughly 4% of the exchange's approximately $144 billion in assets. Its current leaders include co-CEO Yi He; founder CZ no longer runs the company but is its largest shareholder. (CoinDesk; The Week; TechCrunch)
- **TraderTraitor (also known as Jade Sleet, UNC4899, Slow Pisces):** a group the FBI classifies among North Korean state hackers, specifically targeting crypto companies. The FBI attributes the attacks on DMM Bitcoin (2024, $308 million) and Bybit (2025, $1.5 billion) to it. (BleepingComputer; The Hacker News)
- **Blockchain analytics firms (Chainalysis, TRM Labs, Arkham, Blockaid) and stablecoin issuers (Tether, Circle):** they trace the money and can freeze their own tokens. This is where the crypto

world "can" react much like a bank: centrally issued stablecoins can be frozen, bitcoin and ether cannot. (CoinDesk)

The pattern isn't new: the developer's machine is the gateway. - **DMM Bitcoin, 2024:** the attacker posed as a recruiter on LinkedIn, ran malware on the machine of a wallet software company employee via a "pre-employment coding test", entered internal systems with stolen session cookies and manipulated a legitimate transaction request. (BleepingComputer) – **confirmed** (FBI) - **Bybit, 2025:** a Safe{Wallet} developer's machine was compromised; from there, malicious code was planted in the wallet provider's web interface, which hijacked Bybit's next transaction. (The Hacker News) – **confirmed** - **The Security Alliance (SEAL) 2025 advisory** says the group typically approaches staff with production or IT access using fake recruiter identities, delivers malware to their machines through a "technical interview" involving a code repository download, then spends days to months mapping from the inside where the keys are and who can access them. (SEAL Radar – DPRK advisory) – **confirmed** (professional community advisory)

Important: Binance has not yet disclosed the specific entry method in this case (phishing, fake job offer, supply chain or other); the cases above show the group's known methods, not the proven course of this incident. – **assumption** (pattern similarity)

How it works

> `RED // ATTACKER'S VIEW`

The most important lesson of the case is conceptual: **they didn't break the vault door, they picked the key holder's pocket.** Exchanges protect funds with keys, and according to Binance the keys didn't leak. The attacker didn't need to steal them: it was enough to get to where the system *by itself* signs and sends withdrawals.

1. **A human in the chain.** A DevOps engineer has access to production infrastructure because of the job. That machine is therefore worth more to the attacker than any customer account. Groups like this typically spend months preparing to approach a key person (fake job offer, test task, a "partner's" message). – **assumption** (known pattern, not the confirmed course of this case)
2. **From the machine to the engine room.** From the compromised laptop, the attacker reached an internal service container, i.e. a software component that "has the right" to start withdrawals. (Binance Square)
3. **Using the system's own hands.** Withdrawals submitted from the container were official requests from the system's point of view: the keys stayed in place, only someone else told them what to sign. That's why "no private key leaked" is both good news and a warning: protecting the key alone isn't enough if the process using the key can be hijacked.
4. **Speed and getaway.** The money was immediately spread out, swapped and posted as collateral, moving it from freezable stablecoins into assets that are harder to catch. (CoinDesk)

Which weaknesses does it exploit? - **Too much trust in one machine:** if an employee's laptop is enough for someone to reach the withdrawals, the laptop is the key to the bank branch. - **Machine privileges without checks:** an automated service can start large withdrawals; without independent human or separate-channel approval, an unusual request goes through too. - **Missing amount limits and throttling:** a multi-billion outflow is only possible if no limit stops or delays unusual volumes. What failed at Binance is not yet known. – **assumption**

The second wave (the scammers' side): after big heists, criminals ride the news. In February 2025, days after the Bybit heist, Binance customers received messages appearing to come from Binance's real SMS

sender saying "someone from North Korea logged into your account"; the "support line" they called back asked them to move their funds to a new, "safe" wallet the scammers controlled. (ForkLog; NCSC Switzerland) The other recurring form is the "fund recovery" scam: someone poses as an authority, law firm or investigator and asks for an upfront fee for "recovery". According to the FBI, authorities don't charge for investigations, and private companies cannot order seizures. (FBI IC3) In the first hours of the incident, Binance already warned users to beware of unofficial links and requests for account details. (TechCrunch)

Impact and Hungarian relevance

- **Damage:** about $5.9–6.3 billion, of which about $3 billion is frozen; the final loss will become clear over the coming days. Binance pledged that users won't lose money; if that holds, the exchange bears the loss. (Binance Square; Fortune)
- **Affected groups:** directly, Binance; indirectly, customers who temporarily can't access their funds because withdrawals are paused, and everyone approached by scammers riding the news.
- **Wider impact:** if the analyst attribution is correct, the stolen money increases the revenue of a sanctioned state; the FBI previously attributed the Bybit and DMM heists to the same group. (The Hacker News – Bybit; BleepingComputer) – **assumption** (for this case)

Hungarian relevance: - **No impact in Hungary is known.** Hungarian media (Portfolio, HVG, Fintech.hu, Cryptofalka) reported on the case on 30 October but published no information on Hungarian users, Hungarian authorities or domestic impact. (Portfolio (in Hungarian); HVG (in Hungarian)) - As of 30 October 2026, we found no related warning from the MNB (the Hungarian central bank and financial supervisor), the NBSZ NKI (Hungary's national cyber security centre) or the Hungarian police. - The risk in Hungary, too, is the second wave: Hungarian crypto holders may receive Hungarian-language calls, texts and ads using "Binance support", "compensation" or "fund recovery" as a pretext. No specific Hungarian case is known yet. – **assumption** (based on earlier international patterns)

What to do

> BLUE // WHAT TO DO NOW

Individuals (if you hold crypto, on Binance or elsewhere): - **Don't move anything to a "safe wallet"**, no matter who asks. A real exchange never asks you to move your money to a wallet it provides or one just created. (NCSC Switzerland) - **Don't call back numbers received by SMS or email**, and don't click links in the message; check notifications in the exchange's app or on the official address typed by hand. A fake SMS can appear in the same thread as the genuine ones. (NCSC Switzerland) - **You don't need to do anything to be compensated.** Binance pledged to cover the losses from SAFU and its own funds; anyone asking for data or money for "compensation registration", an "unlock fee" or "verification" is a scammer. (Binance Square) - **Don't pay "fund recovery" companies.** Authorities don't charge, and private companies can't order seizures. (FBI IC3) - **Never give anyone remote access** to your computer or phone, and never reveal your recovery phrase (seed phrase), password or 2FA code. - **Don't panic:** a temporary pause in withdrawals doesn't mean your money is lost; follow updates on official channels, not figures circulating on social media. (Cyber Security News) - **Longer term:** don't keep on an exchange what you don't use for trading; if you use your own wallet, keep the recovery phrase offline.

Small business (if you work with developers or operators): - **Machines with admin or production access are a separate category:** no personal browsing, unknown test tasks or running downloaded code repositories. (SEAL Radar) - **Raise awareness** of the fake job offer trick among staff: anyone asking to run

code as a "recruitment test" is suspicious. (BleepingComputer) - **Two keys for moving money:** large transfers or payouts shouldn't start on the decision of a single person or machine; set an amount limit and a second approver on a separate channel.

Organisation: - **Treat key people's endpoints as crown jewels:** EDR, software and browser extension inventory, regular review; check whether suspicious "recruiters" have approached staff with production access. (SEAL Radar) - **Protecting the key isn't enough; protect the process that uses the key too:** services that start withdrawals need independent approval, amount and velocity limits, and an automatic stop on unusual patterns. - **No direct path from developer machines to production:** dedicated, isolated admin workstations, short-lived, task-bound privileges, protection of session cookies and tokens. (BleepingComputer) - **Independent verification when signing:** approvers should also check transaction data on a separate device (e.g. a hardware wallet), not only in the browser interface; test with unusual trial transactions whether approvers notice. (SEAL Radar) - **Prepare for the second wave:** after a major incident, pre-written customer communication ("this is how we contact you, and this is how we never do"), clear naming of official channels, and repetition of warnings already issued. (TechCrunch)

Technical block

- **CVE:** none; Binance has not named a vulnerability. Based on current knowledge, the case rests on endpoint compromise and abuse of internal access. (CyberInsider)
- **Affected component:** Binance's withdrawal service and an internal service container; the company is rebuilding the withdrawal service and related addresses. (CyberInsider)
- **MITRE ATT&CK (editorial mapping based on the group's known methods and the disclosed chain – assumption):**
- T1566 Phishing / T1204 User Execution (job-offer lure, coding test – the group's known method, not confirmed in this case);
- T1539 Steal Web Session Cookie, T1550 Use Alternate Authentication Material (confirmed in the DMM case);
- T1078 Valid Accounts (use of the engineer's access);
- T1021 Remote Services / T1610 Deploy Container-type movement towards the container environment;
- T1657 Financial Theft (unauthorised withdrawals).
- **Detection ideas (conceptual):**
- withdrawal requests not coming from the usual internal source or schedule; amount and count anomalies in a short time window;
- new, unknown code repositories run on admin endpoints, unusual browser extensions;
- the same session ID from an unusual location or device;
- access to the container environment from a developer machine outside working hours or without a change ticket.
- **Official guidance, background:** FBI statements on TraderTraitor (DMM Bitcoin, Bybit); SEAL's February 2025 DPRK advisory; FBI IC3 warnings on fund recovery scams. (BleepingComputer; SEAL Radar; FBI IC3)
- **Indicators:** by type, attacker blockchain addresses tracked by blockchain analytics firms (Arkham, Chainalysis, TRM Labs) and Binance; no official consolidated IOC list had been published as of 30 October 2026.

Contradictions and open questions

Open questions

- **$6.3 or $5.9 billion?** Binance reports the "estimated total impact", Chainalysis the market value at the moment of theft; early reports ranged from $1.7 billion to $8 billion. This document therefore uses: "about $6 billion, $6.3 billion according to Binance, $5.9 billion according to Chainalysis". (Fortune; The Hacker News)
- **How much is frozen?** Binance reports "about $3 billion"; according to Cyber Security News, the amount Binance had confirmed as frozen in an earlier update was $2.54 billion; the difference may come from the rapidly changing situation. (Cyber Security News)
- **Deposits:** some sources say both deposits and withdrawals are paused (HVG, Binance Square's first statement), others that deposits have already resumed (CyberInsider, The Week, Portfolio). The later status is that deposits have resumed.
- **How was the laptop compromised?** Unknown; Binance promises a post-mortem.
- **Who did it?** TRM Labs' attribution is an analyst assessment; there is no official (e.g. FBI) confirmation as of 30 October, and Binance has not named a perpetrator.
- **Can the unfrozen part be recovered?** Unknown; bitcoin and ether cannot be frozen centrally.
- **When will withdrawals resume?** Binance estimates 48 hours, but itself calls this an estimate.

Source assessment

Source	Type	Reliability	Supports
Binance Square – Binance News	company (primary summary)	high (on its own claims)	$6.3 billion, $3 billion frozen, DevOps laptop, private key, SAFU, post-mortem
CoinDesk	press	high	Chainalysis estimate, Tether/Circle, Arkham balances, Aave, TRM attribution, market
The Hacker News	press	medium–high	Chainalysis $5.912 billion, Arbitrum, attack chain
CyberInsider	press	medium–high	deposits back, withdrawals paused, 48 hours, TraderTraitor (TRM)
Fortune	press	high	early estimates, asset breakdown, open questions
TechCrunch	press	high	first hours, CZ, Binance scam warning, Polymarket
The Week	press	medium	status on 30 Oct, market, background
Cyber Security News	press	medium	$2.54 billion confirmed frozen, SAFU size, Ripple
Portfolio	press (HU)	medium–high	Hungarian media coverage, freezers, 48 hours
HVG	press (HU)	medium–high	Hungarian media coverage, TRM attribution
The Hacker News – Bybit	press	high	Bybit precedent, FBI attribution
BleepingComputer – DMM Bitcoin	press (based on FBI statement)	high	TraderTraitor method: fake recruiter, coding test, session hijacking
SEAL Radar – DPRK advisory	researcher (professional community)	high	DPRK tactics, defensive recommendations
FBI IC3 – PSA230811	authority	high	fund recovery scams, red flags
NCSC Switzerland – Binance SMS scam	authority	high	"safe wallet" scam mechanism, advice
ForkLog	press	medium	post-Bybit "Lazarus"-pretext scam (Feb 2025)