NATIONAL CYBERSECURITY ASSOCIATION OF UKRAINE (NCAU) · ANALYTICAL CENTER

When Systems Trust Attackers

The Binance incident of October 29, 2026 and the hidden risks of machine identities

Research Report 02/2026 Identifier: **NCAU-RR-2026-02** 30.10.2026 Data as of **10:00 UTC, 30.10.2026**
English / Ukrainian

Prepared by: the Analytical Center of the National Cybersecurity Association of Ukraine, based on open-source analysis, public statements by affected organizations, technical reports by researchers and available blockchain data. Once Binance publishes its technical report, NCAU will update the findings and test the hypotheses.

Abstract

On October 29, 2026, assets that blockchain analytics firm TRM Labs valued at $6.36 billion were moved out of wallets belonging to the crypto exchange Binance. According to Binance's preliminary account, the incident may have involved a compromised work laptop belonging to a DevOps engineer and subsequent access to an internal service that generates withdrawal requests. The company stated that it had found no evidence of private key leakage.

This raises a fundamental question: is it enough to protect cryptographic keys if an attacker can gain control of a system that is legitimately entitled to use them? NCAU examines the incident in the wider context of attacks on engineers' workstations, privileged accounts, vendors and machine identities, compares it with 14 documented cases, and proposes three original analytical tools: a trust compromise matrix, a defensive barrier map and a method for assessing the risk of a single workstation.

Key conclusion: a valid digital signature does not always mean that the operation was authorized by the rightful owner of the assets. The security of modern infrastructure depends not only on protecting keys and devices, but also on independent verification of the authority, context and consequences of critical actions.

1. Key Findings

1. **Scale.** Three independent analytics firms estimate the theft at $5.9–6.4 billion: TRM Labs $6.36 billion [1], Elliptic $6.43 billion [75], Chainalysis $5.912 billion [10]. That is almost four times the previous record, the roughly $1.5 billion Bybit hack of 2025 [25], and more than was stolen from crypto services in all of 2025 (over $3.4 billion according to Chainalysis) [47]. C
2. **Mechanism.** Binance states there is no evidence of private key leakage [2] B. According to TRM, the attacker likely gained control of the hot wallet signing infrastructure on ten networks [1] C. If confirmed, this was a compromise of the decision to sign, not of the key itself.
3. **Point of entry.** According to Binance's preliminary account, the chain began with a compromised DevOps engineer's laptop and a service container that generates withdrawal requests [2] B. Under NCAU's current classification, including the preliminary assessment for Binance, initial access was gained through one person's device in 9 of the 15 incidents in our dataset, and partially so in one more (Section 7). This describes NCAU's purposive sample, not the prevalence of the method across all cyberattacks.
4. **Frozen and remaining funds.** Within roughly four hours, stablecoin issuers and individual networks froze between $2.7 billion (TRM, 00:30 UTC) and $2.84 billion (Elliptic, 08:00 UTC) on-chain [1][75] A; Binance

puts the figure at about $3 billion [2]. Addresses that analysts link to the attacker still held between $2.4 billion (TRM, ETH and BTC only) and $3.3 billion (Elliptic, all non-freezable assets) [1][75] C.

5. **Detection gap.** The first outflow occurred at 20:05 UTC, the first public signal from an independent researcher appeared at 20:32 [86], issuers began freezing funds at 20:57–21:01 UTC, and Binance officially suspended withdrawals at about 22:15 UTC, roughly 2 hours and 10 minutes after the attack began [1][4][76]. As of 30.10 there is no government attribution [12]; blockchain analytics firms attribute the attack to the North Korean group TraderTraitor [1][11] C; Elliptic considers this likely but not certain [75].
6. **Containment gap.** According to Bitquery, the EIP-7702 delegation through which the attacker's code controlled Binance's busiest Ethereum hot wallet stayed active for 3 hours 50 minutes and was revoked at 00:10:35 UTC, more than 90 minutes after withdrawals were suspended [76] A / C. Suspending a service and revoking authority the system has already granted are different operations.

Scope limitations

This is an independent open-source (OSINT) analysis, not a forensic examination of Binance devices or systems. NCAU had no access to the company's logs, disk images or internal infrastructure and did not receive its comment. Binance's technical report had not been published at the time of writing. Facts, statements by the parties, analyst assessments and hypotheses are separated using an evidence scale (Section 2).

2. Methodology

2.1. NCAU evidence scale

Level	Meaning	Example in this report
A Observed fact	Data available for independent verification (blockchain transactions, a public document)	Transfer of 18,270 BTC at 20:20 UTC; freeze of USDT at the attacker's address
B Primary statement	A statement by an organization with direct access to the information: the affected party, an issuer, a government body	Binance's preliminary statement about the DevOps engineer's laptop; an FBI publication
C Analytical assessment	A conclusion by outside specialists based on data	TraderTraitor attribution by TRM Labs; the $5.912 billion estimate by Chainalysis
D Hypothesis	A possible explanation without sufficient confirmation	The specific method by which the laptop was infected

Level A does not mean we know who controlled an address or why a transfer was made: observation and interpretation are kept separate. On-chain figures are taken from the reconstructions by TRM Labs and Blockaid; anyone can verify them using the addresses and hashes in those reports. Where an organization's statement is known only through media or a social media post, it is marked B with a reference to the source that recorded it. Level A applies only to the fact of a transaction or freeze; attributing addresses to the attacker and the criminal nature of the operations are analytical assessments, so such claims are marked A/C.

2.2. Sources and verification rules

Data collection period: 29.10.2026, 20:00 UTC – 30.10.2026, 10:00 UTC. The report uses 86 sources: statements by the companies involved; independent blockchain analytics (TRM Labs, Elliptic, Bitquery, Chainalysis, Blockaid, Arkham, CryptoQuant); official documents (FBI, CISA, US Department of the Interior Inspector General, SEC, EU, CERT-UA); and standards and specifications (NIST, ISO, MITRE, C4, Ethereum). A key figure is treated as established if it is confirmed by a primary source or by two independent analytics

firms. Discrepancies are not averaged but shown separately (Section 5.4). Three independent blockchain reconstructions (TRM Labs, Elliptic, Bitquery) are compared in Section 5.5. NCAU could not locate a dedicated page about the incident on Binance's official websites; the company's statements are reproduced from identical quotations in several independent outlets [2][19][79]. NCAU opened the TRM Labs, Elliptic and Bitquery pages and checked the key figures against them on 30.10.2026; Binance's post on X is not accessible for automated retrieval. Claims that could not be confirmed by a primary source are not included in the report. All times are UTC (Kyiv is UTC+2); amounts are in US dollars at prices at the time of transfer.

2.3. Definitions

- **Machine identity:** the credentials of services, containers, scripts and bots (tokens, API keys, certificates) through which systems trust each other without human involvement.
- **Signing infrastructure:** the set of systems that construct, approve and sign transactions, including hardware security modules and signing policies.
- **Entry through one person's device:** initial access gained by compromising (malware, stolen credentials or session) a device or personal account used by a specific individual. Excluded: deceiving a person without compromising a device, insider actions, hiring an impostor, and perimeter vulnerabilities.

3. Timeline

Funds began leaving at 20:05 UTC on the XRP Ledger, not on Ethereum, which most monitoring systems watch. Arkham gives a later start, 20:30 UTC [8]; this report relies on TRM's more detailed reconstruction.

Time (UTC)	Event	Level	Source
Oct 28, 05:55–07:00	Scheduled maintenance of Binance's Ethereum wallets with deposits and withdrawals suspended, announced on Oct 27; no link to the attack has been established	B	[83]
Oct 28, morning	An address that TRM links to the attack operator receives three withdrawals from the Tornado Cash mixer to pay for fees (Bitquery records funding of about 1 ETH at 14:54 on Oct 29)	A / C	[1][76]
Oct 29, daytime	According to TRM, the code is tested on two wallets and rehearsed on a third; about four hours before the attack it is installed on a Binance hot wallet	C	[1]
20:05–20:09	Five Binance wallets on the XRP Ledger send 233.46 million XRP	A	[1]
after 20:10	Wallets on Solana and Optimism are drained	A	[1]
20:20	18,270 BTC in a single transfer; a transaction carrying 50 EIP-7702 authorizations on Ethereum (20:20:59); within two minutes, 612.7 million USDT and 46.4 million TRX on Tron	A	[1][5]
20:24:23	The Ethereum hot wallet is drained: 167,464 ETH, 1.615 billion USDT and about 60 other tokens	A	[1][5]
20:57	World Liberty Financial freezes WLFI at the main receiving address: the first freeze	A	[76]
20:32	Independent researcher Spreek publicly reports a possible hack on X: the first public signal	B	[86]
20:41 / 20:59	Through calls from Binance 14, 780 million and then a further 43 million USDC (823 million in total) are withdrawn from the Hot Wallet 34 smart account, which Binance 14 owned	A	[5][84] [85]
21:01–21:04	Tether freezes 971.1 million USDT; Circle freezes 823 million USDC	A	[1]
21:15	Changpeng Zhao (CZ): "User funds are safe! It does look like a hack on Binance"	B	[3]
21:16–21:29	Binance edits its first statement twice: it removes the line about no impact on funds and adds "User funds are completely safe"	B	[3]

Time (UTC)	Event	Level	Source
21:44	A repeat sweep of Binance 14 after Binance's first statement: about 200 million USDT and 370 ETH reach the already frozen address	A	[84]
22:01–22:10	Ripple freezes 40.5 million RLUSD; World Liberty Financial freezes 27.8 million USD1	A	[1]
about 22:15	Binance officially suspends withdrawals (TechCrunch records confirmation at 22:27)	B	[4][9]
23:05–23:56	Second wave: wallets on Avalanche and Polygon; final sweep at 23:56	A	[1]
Oct 30, 00:08	The Arbitrum Security Council locks about $30 million (8,426 ETH and 74.6 million ARB)	A	[1]
00:10:35	Binance revokes the EIP-7702 delegation; until then the attacker's code had controlled the wallet for 3 h 50 min and been called seven times	A / C	[76]
00:36	Binance co-founder Yi He: "Binance will cover all hacking losses"	B	[7]
about 02:25	Binance's preliminary statement: a DevOps engineer's laptop, a service container, unauthorized withdrawals; about $6.3 billion affected and about $3 billion frozen; no evidence of key leakage (other sources record 02:21–02:36)	B	[2][5]
04:17	Yi He: withdrawals are expected to resume within 48 hours; the withdrawal service and address controls are being rebuilt	B	[6]
about 08:37	Binance reports finding "additional points of breach" beyond the engineer's laptop; withdrawals are expected to resume in about 45 hours	B	[77][78]
about 09:00	Withdrawals remain suspended; deposits are operating	B	[20]

About a day and a half passed between the first anonymous funding from Tornado Cash and the first withdrawal (NCAU calculation based on TRM data). This points to a planned operation with testing, not opportunistic use of accidental access.

4. Technical Reconstruction

4.1. The attack chain

Link	What is known	Level	Source
A DevOps engineer's work laptop	The point of entry according to Binance's preliminary account; the infection method has not been disclosed; Binance later reported additional points of breach	B	[2][77]
Service container	An internal service that generates withdrawal requests; unauthorized requests were submitted through it	B	[2]
Signing infrastructure	Besides Ethereum, wallets on nine other networks were drained through ordinary, correctly signed transfers; TRM concludes that the signing infrastructure was likely compromised; Blockaid records simultaneous signing by 11 hot wallet keys; according to Elliptic, a second Ethereum hot wallet signed nine transfers worth $174 million directly to the attacker	C	[1][5] [75]
Ten networks	XRP Ledger, Solana, Optimism, Bitcoin, Tron, Ethereum, Arbitrum, Base, Avalanche, Polygon	A	[1]

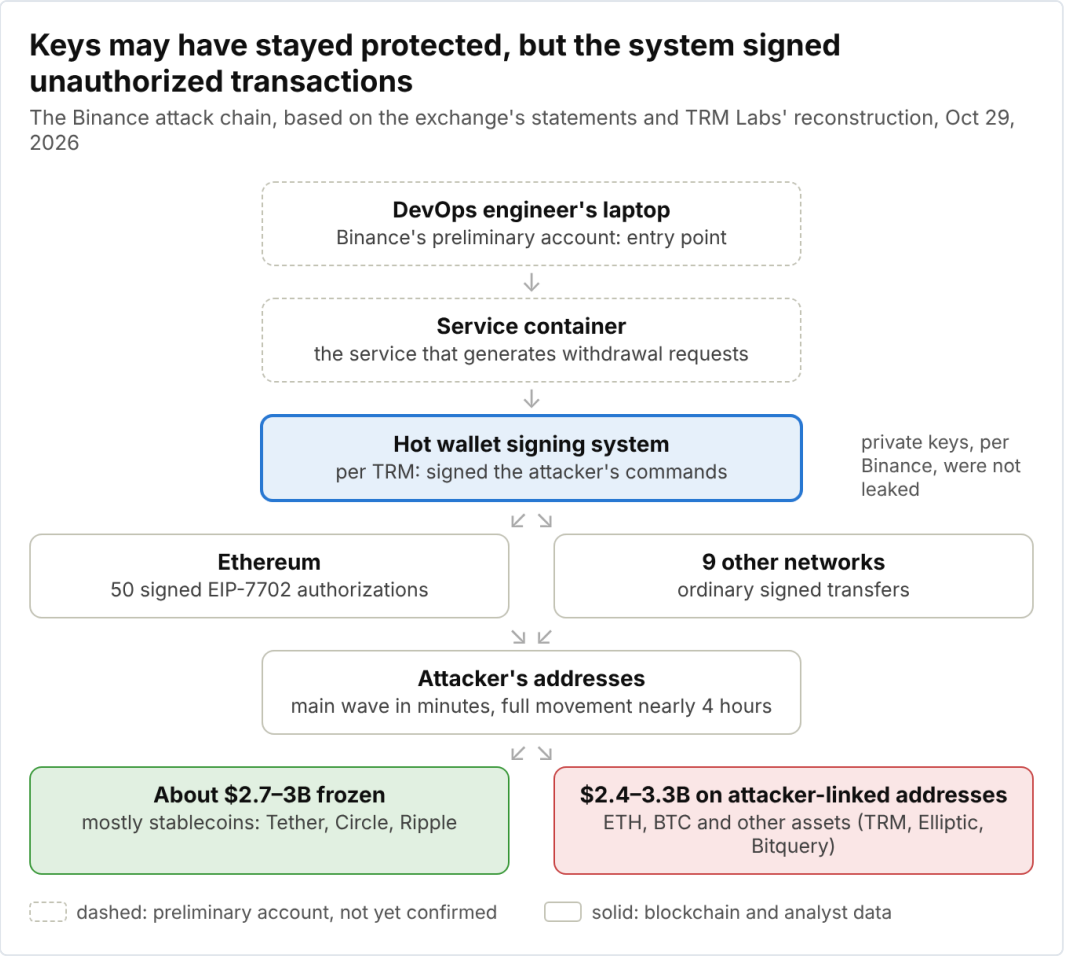


Figure 1. The Binance attack chain based on the exchange's statements and TRM Labs' reconstruction. Dashed: Binance's preliminary account; solid: blockchain and analyst data.

Binance CEO Richard Teng said the attack was "not a single click" and did not rely on the permissions of one engineer [5] B. The laptop was the way in, but the scale of the loss was determined by the internal architecture of trust.

4.2. The key and the authority to use it

The likely scenario is that compromising the transaction-initiation service allowed the attacker to influence the signing process D. Which internal checks were bypassed has not been publicly established. Binance's first measures after the attack, revoking the authorizations of compromised addresses and rebuilding the withdrawal service and address controls [2][6], are consistent with this scenario but do not prove it. Elliptic reads the nine transfers signed directly by the second hot wallet as a sign that the attacker could instruct the signing infrastructure directly [75] C.

Hierarchy between wallets. Binance 14 was the owner of the Hot Wallet 34 smart account, so once the attacker took control of Binance 14, calls through it pulled a further 823 million USDC out of Hot Wallet 34 [84] [85] A / C. An ownership hierarchy between hot wallets turns the compromise of one wallet into the compromise of several.

Whatever the details of this incident, the scenario illustrates a general problem with machine identities: service accounts, containers and bots often have broader permissions than people and are verified less strictly. A person is authenticated with a password, a second factor and a device; a service is often trusted by default. NCAU's conclusion: protecting the key without protecting the decision to sign does not guarantee the protection of assets. A signing policy must verify the substance of a transaction (address, amount, frequency, new or known destination) regardless of who initiated it.

4.3. The 50 EIP-7702 authorizations technique

Ethereum's Pectra upgrade (May 7, 2025) introduced EIP-7702: an ordinary wallet can sign an authorization that delegates its behavior to a smart contract [68]. An authorization is valid only with the wallet's current transaction sequence number (nonce). An active exchange hot wallet changes its nonce constantly, so the attacker submitted a single transaction with 50 pre-signed authorizations for 50 consecutive nonces (18,914,775–18,914,824) [5][13] A. One of them matched, and 3 minutes and 24 seconds later the wallet was empty [1]. According to Bitquery, the delegation stayed active for 3 hours 50 minutes, the attacker's code was called seven times, and the delegation was revoked at 00:10:35 UTC, more than 90 minutes after withdrawals were suspended [76].

The specification explicitly warns that a poorly designed delegate can take near complete control of a wallet [68]. TRM suggests that a batch of 50 signatures indicates either time-limited access or that the signatures were obtained from the exchange's own system [1] C. Abuse of EIP-7702 is not new: in 2025 Wintermute reported that more than 80% of EIP-7702 delegations pointed to the same copy-pasted attacker "sweeper" contract [69].

4.4. MITRE ATT&CK mapping

Stage	What is known	Level	ATT&CK v20 techniques
Preparation	Funding via Tornado Cash; tests and rehearsal on third-party wallets [1]	C	Not represented in Enterprise
Initial access	A DevOps engineer's laptop [2]. Method unknown; a possible scenario is a fake job interview or "test assignment", as in the Contagious Interview campaign, whose attacks Binance reported repelling two days before the incident [18]	D	T1566.003 Spearphishing via Service; T1204.002 Malicious File; T1195.001 Compromise Software Dependencies and Development Tools
Credentials	Not disclosed. By analogy with UNC4899 [55], CircleCI [36] and Bybit/Safe [26]: theft of sessions and tokens	D	T1539 Steal Web Session Cookie; T1550.004 Web Session Cookie; T1552.001 Credentials In Files
Lateral movement	Access to the withdrawal request service container [2]; specific techniques not disclosed	B / D	T1078.004 Cloud Accounts; T1609 Container Administration Command; T1552.007 Container API
Signing abuse	Signed transfers on 10 networks; 50 EIP-7702 authorizations [1][5]	A	No corresponding technique
Impact	Withdrawal of $6.36 billion [1]	A	T1657 Financial Theft
Laundering	DEX swaps, Aave, JustLend, THORChain [1][17][75]	A / C	Outside ATT&CK scope

MITRE tracks Contagious Interview as group G1052 and associates it with T1566.003, T1204 and T1195.001 [58]. MITRE has no dedicated page for TraderTraitor (UNC4899, Jade Sleet, Slow Pisces); its activity is documented by CISA, Google Cloud and Palo Alto Networks Unit 42 [51][55][56].

5. The Financial Picture

5.1. How much was stolen, and why there are several estimates

Estimate	By	Basis	Level
$6.36 billion	TRM Labs [1]	Prices at time of transfer	C
$6.23 billion	TRM Labs [1]	Current prices after the market decline	C

Estimate	By	Basis	Level
about $6.3 billion	Binance [2]	"Affected assets"	B
$6.43 billion	Elliptic [75]	At time of theft	C
$5.912 billion; later $6.4 billion	Chainalysis [10][81]	At time of theft; CEO's updated estimate	C
over $5.7 billion (peak)	Arkham [8]	Attacker wallet balances	C

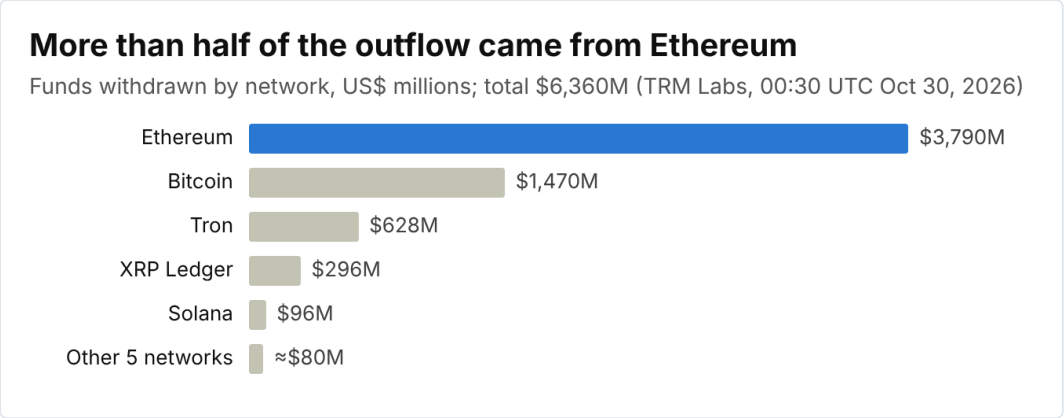


Figure 2. Funds withdrawn by network, US$ millions (TRM Labs, 00:30 UTC, 30.10.2026) [1].

5.2. Frozen and not frozen

Who froze	Asset	Amount	Source
Tether	USDT	about $1.77 billion on-chain (TRM); $1.567 billion per Tether's CEO	[1][21]
Circle	USDC	about $825 million (TRM); "over $800 million in coordination with law enforcement" per Circle's CEO	[1][22]
Ripple	RLUSD	$40.5 million confirmed on-chain; Yi He's claim of about $200 million is unconfirmed	[1]
Arbitrum Security Council	ETH, ARB	about $30 million	[1]
World Liberty Financial	USD1	$27.8 million	[1]
Total		**about $2.7 billion (TRM, 00:30 UTC; Bitquery); $2.84 billion (Elliptic, 08:00 UTC); about $3 billion (Binance)**	[1][2] [75][76]

According to Bitquery, six of Tether's 11 freezes hit wallets that were already empty, and about $729 million of USDT was swapped into ETH and TRX before the freezes reached it [76]; according to Elliptic, Tether froze the attacker's main Ethereum wallet after 37 minutes, locking 1.18 billion USDT [75].

The attacker rapidly converted stablecoins into assets that cannot be frozen: about 325 million USDT was swapped on decentralized exchanges for 122,300 ETH at more than 10% below market; 60 million USDT was deposited into Aave as collateral for a loan of about 19,760 ETH; 300 million USDT was moved into the JustLend protocol on Tron; and about 48 million of 88.5 million RLUSD was sold before the freeze [1] A / C. Elliptic counts the swaps more broadly: 434 million USDT for 160,451 ETH at a 12–26% loss against market; Aave froze the affected markets after the loan [75]. The balance on attacker-linked addresses is estimated at about $2.4 billion (TRM, 00:30 UTC, ETH and BTC), $3.2 billion (Bitquery, 06:43 UTC) and $3.33 billion (Elliptic, about 07:00 UTC, 43 addresses) [1][75][76].

Frozen does not mean returned. Recovery requires separate legal proceedings: a year and a half after its 2025 hack, Bybit obtained a preliminary injunction in a US court restraining the disposal of assets, having recovered about $48.4 million and frozen more than $30.5 million [27].

5.3. Market impact

Over the evening of 29.10, bitcoin fell 4.8% to below $77,000, ether 5.7%, BNB 8% and the Aave token 11% [8]. In one hour, $629 million in leveraged positions were liquidated, of which $607 million were longs [14]; over 24 hours, about $1.54 billion, 84% of it longs, affecting about 239,000 traders [15]. The market had begun falling before the first signs of the hack, so the entire sell-off cannot be attributed to the incident [14]. Before the incident Binance held about $144 billion in assets according to DefiLlama, so the loss is about 4% [8]; the SAFU insurance fund is estimated at about $1 billion in bitcoin [8]. Fundstrat analysts do not consider the incident a solvency event [16].

5.4. Data discrepancies

Metric	Discrepancy	NCAU interpretation
Start of attack	20:05 UTC (TRM) vs 20:30 UTC (Arkham)	20:05: TRM records the XRP Ledger; Arkham counts from movement on Ethereum
USDC	780 million (Blockaid) vs 823 million (TRM)	Two transfers from Hot Wallet 34: 780 million at 20:41 and 43 million at 20:59; 823 million in total [84]
BTC wallet	"Hot" (TRM) vs "cold" (CryptoQuant)	Not established until Binance's technical report D
Total frozen	$2.54 billion (early Binance statement), $2.7 billion (TRM), about $3 billion (later Binance statement)	Figures grew overnight; $2.7 billion is confirmed on-chain
Bitget	$350–388 million across sources	About $387.5 million per the company's revised estimate [45]
Tornado Cash funding	Three withdrawals on the morning of Oct 28 (TRM) vs about 1 ETH at 14:54 on Oct 29 (Bitquery)	Possibly different addresses or stages; not established D
Number of networks	10 (TRM), 11 (Elliptic), 9 (Bitquery)	Different treatment of minor networks and tokens
USDT-to-ETH swaps	325 million at a discount of more than 10% (TRM) vs 434 million at a 12–26% loss (Elliptic)	Different snapshot times and swap coverage
Bridges and mixers	Funds commingled with Bitget via THORChain (ZachXBT); about $1.9 million of TRX via THORChain (Elliptic); none found by 06:43 UTC (Bitquery)	Movement through bridges was minimal as of the morning of 30.10

5.5. Three independent reconstructions

NCAU does not pick a convenient number; it compares three public blockchain reconstructions. The differences come from snapshot time, network coverage and valuation method.

Metric	TRM Labs [1]	Elliptic [75]	Bitquery [76]
Data snapshot	00:30 UTC	about 08:00 UTC	06:43 UTC
Total amount	$6.36 billion	$6.43 billion	about $6.3 billion
Networks	10	11	9 (17 hot wallets)
Frozen	about $2.7 billion	$2.84 billion (44%)	about $2.7 billion

Metric	TRM Labs [1]	Elliptic [75]	Bitquery [76]
On attacker-linked addresses	about $2.4 billion (ETH and BTC)	about $3.33 billion (43 addresses)	about $3.2 billion
Exchanges, mixers, bridges	Bridges and OTC brokers expected next	Almost nothing beyond about $1.9 million of TRX via THORChain	None found
Attribution	TraderTraitor, high confidence	North Korea likely, with caveats	No own attribution

6. Attribution

TRM Labs attributes the attack with high confidence to the North Korean group TraderTraitor [1]; Chainalysis CEO Jonathan Levin named the same group [11] C. Binance has not named a perpetrator. As of 30.10 there is no government attribution: the US Department of Justice and the FBI did not respond to requests for comment [12]; a Binance spokesperson said the company is working with law enforcement to identify the criminals [11]. Analytical attribution is not a final identification of the perpetrators.

Elliptic also considers North Korean involvement likely but not certain, and lists caveats: the address shared with Bitget received only about $39,000 of Binance funds and may indicate a shared launderer rather than the same perpetrator; stablecoins were held for 37–46 minutes, which is atypical for North Korea; and the laundering methods (market makers, DeFi lending) differ from the pattern after the Bybit hack [75] C.

Context. According to Chainalysis, more than $3.4 billion was stolen from crypto services in 2025, of which at least $2.02 billion (about 59%) is attributed to North Korea [47]. In 2026, before the Bitget hack, $1.73 billion was stolen in 333 incidents [48]; according to DefiLlama, hack losses in 2026 up to October 26 totaled $2.369 billion across 312 incidents, so the Binance incident alone is about 2.7 times larger than all 2026 hack losses before it [80]. According to TRM, North Korea's cumulative crypto thefts exceeded $6 billion by April 2026 [49]; if the attribution is confirmed, the single incident of October 29 roughly doubles that figure. The Multilateral Sanctions Monitoring Team (MSMT) estimated North Korean thefts at no less than $2.84 billion between January 2024 and September 2025 [50].

Methods. In 2022 the US government described TraderTraitor as a campaign targeting system administrators and DevOps engineers at crypto companies through "recruitment" messages and trojanized applications [51]. In 2024 the FBI warned about job interview "test assignments" that run malicious packages [52]. In 2025 Google Cloud described UNC4899 attacks in which victims ran malicious Docker containers on work machines after approaches on LinkedIn and Telegram, and the attackers used stolen session cookies in AWS [55]. This is the closest public precedent to the chain described by Binance.

7. Comparative Analysis

NCAU compiled 15 publicly documented incidents, including Binance, in which one person, one device or one human process played the decisive role. The criterion "entry through one person's device" is defined in Section 2.3 and shown in a separate column so that the classification can be checked.

Table 7a. Losses and attribution

Incident	Date	Losses	Attribution	Attribution type	Source
Binance	10.2026	$6.36B (TRM)	TraderTraitor (North Korea)	Analytical	[1][11]
Bitget	09.2026	about $387.5M	North Korea	Analytical; CEO statement	[45][46]
Bybit (via Safe)	02.2025	about $1.5B	TraderTraitor	Government (FBI)	[25][26]

Incident	Date	Losses	Attribution	Attribution type	Source
Radiant Capital	10.2024	about $50M	UNC4736 / AppleJeus	Analytical (Mandiant)	[28]
DMM Bitcoin (via Ginco)	05.2024	4,502.9 BTC, $308M	TraderTraitor	Government (FBI, Japan NPA)	[29][30]
Okta	10.2023	files of 134 customers	not disclosed		[43]
MGM Resorts	09.2023	about $100M (EBITDAR)	Scattered Spider / ALPHV	Attacker claims	[40]
CircleCI	12.2022	customer secrets and tokens	not disclosed		[36]
LastPass	2022	customer vault backups	not disclosed		[34][35]
Uber	09.2022	access to internal systems	Lapsus$	Company statement	[44]
Ronin / Axie Infinity	03.2022	about $620M	Lazarus	Government (FBI)	[31][33]
Arup	01.2024	$25.6M	not established		[38][39]
KnowBe4	07.2024	no data lost	North Korea	Company statement	[42]
Coinbase	05.2025	costs of $180–400M (estimate)	not disclosed		[41]
USGS (US)	2018	not quantified	not applicable		[37]

Table 7b. Point of entry and classification

Incident	Point of entry	Lure or method	Entry through one person's device
Binance	DevOps engineer's laptop (preliminary)	Not disclosed	yes (preliminary)
Bitget	Zero-day in two third-party security appliances, then the wallet server	Technical vulnerability	no
Bybit (via Safe)	A Safe{Wallet} developer's MacBook	A Docker "investment simulator" project; hijacked AWS sessions	yes
Radiant Capital	A developer's device, then several devices	A ZIP "PDF report" via Telegram from a "former contractor"	partially
DMM Bitcoin (via Ginco)	A vendor employee's computer	A "test assignment" from a LinkedIn "recruiter"; session cookies	yes
Okta	A personal Google profile on a work laptop	Saved service account credentials	yes
MGM Resorts	Help desk	A call impersonating an employee (details from attackers)	no
CircleCI	An engineer's laptop	Malware missed by antivirus; stolen 2FA-backed SSO session	yes
LastPass	A DevOps engineer's home computer	Vulnerable third-party media software; keylogger	yes

Incident	Point of entry	Lure or method	Entry through one person's device
Uber	A contractor's personal device	Malware, stolen password, "MFA fatigue"	yes
Ronin / Axie Infinity	A Sky Mavis employee	Fake job, offer in a PDF (per The Block's sources [32])	yes
Arup	A finance employee	A video call with deepfaked "colleagues"; 15 transfers	no
KnowBe4	A newly hired "employee"	A North Korean IT worker using a stolen identity	no
Coinbase	Several support agents	Bribery, followed by a $20M ransom demand	no
USGS (US)	A government laptop	More than 9,000 adult web pages, including Russian sites carrying malware	yes

What the dataset shows

- Under NCAU's current classification, including the preliminary assessment for Binance, in 9 of the 15 cases initial access was gained through one person's device, and partially so in one more (Radiant). In two (Arup, MGM), a person was deceived without any device compromise; in two (KnowBe4, Coinbase), the threat came from inside the company; and in one (Bitget), a technical perimeter vulnerability was decisive. These ratios describe NCAU's purposive sample, drawn from incidents where the role of a person or device was already known, and are not an estimate of the method's prevalence across all cyberattacks.
- In five cases (Bybit, DMM, Okta, LastPass, Uber), the compromise occurred at a vendor, on a personal device or through a personal account, outside the victim's formal perimeter.
- Seven of the 15 incidents are linked to North Korea: three by government attribution (Bybit, DMM, Ronin), three by analytical attribution (Binance, Bitget, Radiant) and one by a statement from the affected organization (KnowBe4). In at least three of them (DMM, Ronin, KnowBe4), the way in was tied to hiring: a job offer, a test assignment or a fake employee.
- In no case was the cryptography broken. Two-factor authentication did not stop attacks in which an already active session was stolen (CircleCI, Bybit/Safe, DMM).

8. Trust Compromise Matrix

NCAU's first analytical tool shows exactly what authority the attacker obtained in the seven best-documented incidents. It helps explain why losing a device is dangerous not in itself, but because of how much the system trusts it.

Incident	Human credentials or session	Access via a vendor	Machine identity	Authority to initiate or sign transactions	Deception of a verification procedure
Binance	○	·	●	●	○
Bybit / Safe	●	●	·	·	●
DMM / Ginco	●	●	·	●	●
Radiant Capital	●	·	·	●	●
CircleCI	●	·	●	·	·
LastPass	●	·	●	·	·
KnowBe4	·	·	·	·	●

Column criteria. Human credentials or session: the attacker used a specific person's password, cookie or token, or malware on that person's device. Access via a vendor: the compromise occurred at an organization providing a service to the victim. Machine identity: the attacker used the credentials of a service, container or integration. Authority to initiate or sign transactions: the attacker was able to create or sign a financial transaction using the victim's system. Deception of a verification procedure: a person or process approved an action because information or identity was falsified.

● confirmed by a primary source or analytics; ○ likely, level D; · not applicable or not established. Binance: only access to the service container and submission of unauthorized withdrawal requests are confirmed, per the company's statement [2]; control over the signing mechanism remains an analytical assessment [1][75]. Bybit/Safe: hijacked AWS sessions, Safe as Bybit's vendor, malicious JavaScript showed signers legitimate transactions [25][26]. DMM/Ginco: session cookies, vendor Ginco, manipulation of a legitimate transaction request [29][30]. Radiant: malware on signers' devices, which displayed legitimate transactions [28]. CircleCI: SSO session, stolen customer tokens and secrets [36]; the affected organization was CircleCI itself, so the vendor column is not marked. LastPass: master password via keylogger, access keys to backups [34][35]. KnowBe4: deception of the hiring procedure [42].

Conclusion. In four of the seven cases (Bybit, DMM, Radiant, KnowBe4) the attacker deceived a verification procedure rather than breaking it technically, and likely did so in one more (Binance); in three (Binance, CircleCI, LastPass), the attacker obtained machine credentials. The largest losses (Binance, Bybit, DMM) occurred where the attacker could influence the transaction itself: initiate it, sign it, or alter what the signers saw.

9. Defensive Barrier Map

NCAU's second tool separates three tasks that are often conflated: preventing an attack, limiting the damage and accelerating detection.

Incident	Prevent	Limit damage	Accelerate detection
Binance	Dedicated workstations for privileged access; third-party code only in disposable VMs; short, device-bound sessions	Independent signing policy; hot wallet limits on every network; delays on large withdrawals to new addresses; revoking EIP-7702 delegations at the same time as suspending withdrawals; no ownership hierarchy between hot wallets	Real-time monitoring of all networks, including the XRP Ledger; alerts on batched EIP-7702 authorizations

Incident	Prevent	Limit damage	Accelerate detection
Bybit / Safe	Isolated development environments with no access to production cloud; short, device-bound AWS sessions	Independent verification of the transaction hash by signers on a hardware device	Integrity monitoring of client-side code (JavaScript) on the server
DMM / Ginco	Test assignments only in disposable VMs; security requirements in the vendor contract	Transaction policy: address allowlists and limits	Anomalies in vendor session use
Radiant	No opening of archives from messaging apps on signers' devices	Signers on separate clean devices; independent transaction simulation; hardware wallets with readable displays	Monitoring of changes to multisig owners and thresholds
CircleCI	EDR beyond antivirus; binding sessions to devices	Short-lived tokens instead of long-lived secrets	Session anomalies by location and time
LastPass	No privileged access from personal devices; control of third-party software	Production keys kept out of personal password vaults; separate backup keys	Alerts on bulk access to backups
KnowBe4	Candidate identity verification	Gradual granting of access (it worked: no data lost)	EDR on new devices (it worked: about 25 minutes to isolation)

The preventive measures for Binance are NCAU's inference by analogy with other incidents; the actual method of intrusion has not been disclosed. KnowBe4's response time was calculated by NCAU from the company's timestamps [42].

10. A Method for Assessing the Risk of a Single Workstation

NCAU's third tool answers a question every board should ask: what exactly could an attacker do if a specific engineer's or executive's laptop were compromised tomorrow? The method produces no numeric score: it is reproducible and yields a qualitative risk profile across six dimensions.

Dimension	Key questions	Signs of high risk	Example
1. Reach	Which systems can be accessed from this workstation without additional authentication: production cloud, CI/CD, signing, payments?	Direct access to production systems or to services that initiate transactions	Binance, Bybit/Safe
2. Persistence of privileges	Are privileges standing or granted per task? How long do sessions and tokens live? Are there secrets in files?	Standing administrator rights; long sessions; API keys on disk	CircleCI, LastPass
3. Independent confirmation	Which critical actions require confirmation by another person on another device or by an independent policy?	One person or one service can complete a critical action	Radiant, Arup
4. Environment hygiene	Is third-party code run? Are there personal profiles, email, browsing, administrator rights?	Test assignments, personal accounts and work access on one device	DMM, Okta
5. Detection	Is there EDR and telemetry? Are there alerts on anomalous sessions? How long until detection?	Antivirus only; no alerts on new sign-in locations	CircleCI, KnowBe4

Dimension	Key questions	Signs of high risk	Example
6. Revocation and containment	How quickly can sessions, tokens and keys be revoked and the device isolated? What limits cap the damage in that window?	Revocation takes hours; no limits on amount or frequency	Binance (delegation active 90+ min after suspension), KnowBe4

How to apply it. (1) List the workstations with privileged access. (2) For each, answer the questions in all six dimensions and rate each dimension as low, medium or high risk. (3) Describe the worst case in the window before access is revoked: which actions are possible and what damage they cause. (4) For each high-risk dimension, assign a control from Section 11 and an owner. (5) Repeat the assessment after changes in roles, systems or vendors.

11. Controls and Framework Mapping

The table links controls to attack stages and to the requirements of recognized frameworks. This is NCAU's analytical mapping to ease implementation, not an official conformity assessment or certification. ISO/IEC 27001:2022 control numbers follow the ISO/IEC 27002:2022 mapping [62]; formal references should be checked against the text of the standard.

Control	Stage	NIST CSF 2.0	ISO/IEC 27001:2022	Other frameworks
Dedicated "sterile" workstations for privileged access	Initial access	PR.AA, PR.PS	8.1, 8.2, 8.18	Microsoft PAW [70]
Test assignments and third-party code only in disposable VMs	Initial access	PR.AT, PR.PS	6.3, 8.7	FBI [52], Microsoft [54]
Short, device-bound sessions; re-authentication for production systems	Credentials	PR.AA	8.5	NIST SP 800-207 [61]
Least privilege for service accounts and containers; segmentation	Lateral movement	PR.AA, PR.PS	5.15, 5.18, 8.22	Zero Trust [61]
Independent signing policy: address, amount, frequency, new destinations	Signing	PR.PS, DE.AE	8.24, 8.32	CCSS 1.05.8.1, 1.05.2.2 [63]
Multiple signers on separate devices held by different operators	Signing	PR.AA	8.2	CCSS 1.02.1.1, 1.02.4.1, 1.05.9.1 [63]
Hot wallet limits; delays on large withdrawals to new addresses	Impact	GV.RM, PR.PS	8.32	Timelock mechanisms
Real-time blockchain monitoring with automatic suspension	Impact	DE.CM, DE.AE	8.15, 8.16	CCSS 2.02.3, 2.02.4.1 [63]
Vendor and contractor risk management	All stages	GV.SC	5.19, 5.20, 5.21	CCSS 2.03 [63]; DORA [66]
Incident response plan with issuer and law enforcement contacts; pre-drafted statements	Response	RS.MA, RS.CO	5.24–5.27	DORA: 4/24 h, 72 h, 1 month [67]

12. The Regulatory Dimension

European Union. Since December 30, 2024, the MiCA Regulation (2023/1114) has required crypto-asset service providers to maintain resilient ICT systems in line with DORA (Article 68) and has made them liable for the loss of clients' crypto-assets resulting from an incident attributable to them, capped at market value at the time of the loss (Article 75(8)) [64][65]. The transitional period for existing operators ended on July 1, 2026 [65]. DORA (2022/2554) has applied since January 17, 2025 [66]; for major ICT-related incidents, the initial notification is due within 4 hours of classification and no later than 24 hours after detection, the intermediate report within 72 hours and the final report one month later [67]. Whether these rules apply to a specific legal entity depends on its licence and jurisdiction; NCAU has not analyzed the status of individual Binance group companies. The recommendations below are general guidance for the market.

Group structures. Binance.US, a separate company, said it was not affected by the incident [82]. For regulators, this is an argument for assessing not only the legal but also the operational separation of local licensees that belong to international groups: whether they have their own keys, signing infrastructure and hot wallets, or share them with the group.

Ukraine. The Law "On Virtual Assets" No. 2074-IX was adopted in 2022 but has not entered into force. Draft law No. 10225-d passed its first reading on September 3, 2025 [74]; on July 31, 2026, the second reading was postponed to the autumn because agencies had not agreed on the division of powers between the National Bank of Ukraine and the National Securities and Stock Market Commission [71]. NCAU found no evidence of a vote by 30.10.2026. Ukrainian IT professionals are already targeted by fake recruiters: in August 2026, CERT-UA warned of campaign UAC-0145 (a Sandworm sub-cluster) that distributed a trojanized VPN client under the guise of job offers [72][73].

13. NCAU Recommendations

13.1. Exchanges, custodians and fintech

1. Separate the right to initiate a withdrawal from the right to sign it: the signing system must apply its own policy rather than trust the initiating service.
2. Keep only the minimum necessary balances in hot wallets; introduce per-transaction and per-period limits, and delays for large withdrawals to new addresses.
3. Do not make one hot wallet the owner of others: an ownership hierarchy between wallets spreads a compromise from one wallet to several [84][85].
4. Monitor all networks, not only Ethereum: this attack began on the XRP Ledger.
5. Agree an emergency freeze protocol in advance with stablecoin issuers and network operators, with contacts available around the clock.
6. Review the use of EIP-7702 and prohibit signing delegation authorizations outside a controlled process.
7. Include revocation of authority already granted (delegations, approvals, sessions) in the response plan, not just suspension of the service: in this incident the EIP-7702 delegation stayed active more than 90 minutes after withdrawals were suspended [76].
8. Undergo an independent CCSS v9 assessment and publish the level achieved.

13.2. Any business and public bodies

1. Apply the method in Section 10 to the workstations of everyone with privileged access, starting with the CIO and the CFO.
2. Assign dedicated devices for privileged access; prohibit personal profiles and third-party code on them.
3. Verify payments and access resets through an independent channel, regardless of who appears on a video call.

4. Include security requirements in contractor agreements and extend access monitoring to contractors.
5. Introduce a "report within five minutes, no blame" rule and test it in exercises.

13.3. Regulators, including in Ukraine

1. Require mandatory reporting of major incidents in virtual asset legislation, on timelines comparable to DORA.
2. Establish custodian liability for the loss of client assets and segregation requirements modeled on Article 75 of MiCA.
3. Reference recognized standards (ISO/IEC 27001, CCSS) as minimum requirements for licensees.
4. Require licensees that belong to international groups to disclose whether keys, signing infrastructure and hot wallets are shared with the group, and to demonstrate that they can contain a group-level incident.
5. Create a mechanism for rapid cooperation with stablecoin issuers and international law enforcement to freeze assets.

13.4. IT professionals and developers

1. Do not run test assignments, archives or repositories from recruiters on a work device; use a disposable virtual machine.
2. Be wary if an interview quickly moves to Telegram or requires installing an application, a VPN or a package.
3. Report suspicious approaches to your security team: information about one campaign protects the whole industry.

13.5. Citizens and investors

1. A balance on an exchange is the exchange's liability, not coins at your disposal: long-term savings are better kept in a hardware wallet.
2. Leverage turns someone else's incident into your loss: in the first hours, positions worth hundreds of millions of dollars were liquidated.
3. Fraud rises after high-profile hacks: no exchange asks you to "verify your account" via a link or move funds to a "safe address".
4. Stablecoins can be frozen by their issuer, and this applies not only to thieves.

14. Open Questions and Indicators

Indicator	Why it matters	Expected timing
Resumption of Binance withdrawals	The main indicator of liquidity and trust	per Binance's latest estimate, about 05:47 UTC, 01.11.2026 [78]
Binance technical report and updated Proof of Reserves	Will confirm or refute the hypotheses on the point of entry, infection method and role of the signing infrastructure	Promised, no date given [2]
Details of the "additional points of breach"	Will show whether the laptop was the only way in, and may change the assessment of the "one device" model	Unknown [77]
Government attribution	Moves attribution from level C to level B	Unknown
Movement of the $2.4 billion in ETH and BTC	Bridges, swap services and OTC brokers as possible interception points	Ongoing
Link to the Bitget hack	If confirmed, this is a series of attacks on exchanges	Unknown [17]

Indicator	Why it matters	Expected timing
Return of frozen funds	Will show how effective freezing really is as a defensive tool	Months
Response of EU and Ukrainian regulators	A test of MiCA and DORA; the fate of draft law No. 10225-d	2026–2027

Questions for the exchange's security architects. Why could a single service role initiate withdrawals on ten networks at once? What exactly does "no evidence of key leakage" mean if signing was carried out on the commands of a compromised service? Were there signals in the access logs for October 28–29? How was the laptop infected, and is it connected to the fake job interview campaign? Is the scheduled maintenance of Ethereum wallets on October 28 connected to the preparation of the attack?

15. Limitations and Disclaimers

- The report was prepared within 14 hours of the start of the incident; some data are preliminary and may change.
- Statements by Binance and by the heads of Tether, Circle and other companies are recorded from social media posts and media reports; NCAU did not open the posts directly, and the text of Binance's statement is reproduced from identical quotations in several independent outlets [2][19][79].
- Blockchain data are as of 00:30 UTC (TRM Labs), 06:43 UTC (Bitquery) and about 08:00 UTC (Elliptic), 30.10.2026.
- Attribution to North Korea was made by private analytics companies; there is no government attribution. Mention of a company or person is not an accusation.
- This report is not investment or legal advice.

How to Cite

NCAU Analytical Center. When Systems Trust Attackers: The Binance Incident of October 29, 2026 and the Hidden Risks of Machine Identities. Research Report 02/2026 (NCAU-RR-2026-02). National Cybersecurity Association of Ukraine, 30.10.2026. ncaua.vercel.app/en/research/binance-hack-machine-identity-trust-2026

Corrections and comments: via the contact form on the NCAU website.

Sources

The Binance incident

1. TRM Labs. North Korea steals $6.36 billion from Binance in the largest hack in history. 29.10.2026. https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history
2. Binance. Preliminary statement on the security incident, 30.10.2026 (X); summary: PANews. https://x.com/binance/status/2115993361517891592 · https://panews.io/articles/01a18aa0-7624-71d3-95c4-901bde2cba87
3. FinanceFeeds. Binance edited hack statement twice. 30.10.2026. https://financefeeds.com/binance-hack-statement-edited-user-funds-safe/
4. FinanceFeeds. Binance halts withdrawals. 29.10.2026. https://financefeeds.com/binance-halts-withdrawals-suspected-hack/
5. FinanceFeeds. Eleven keys signed, no leak (Blockaid data; statement by R. Teng). 30.10.2026. https://financefeeds.com/binance-hack-eleven-keys-signed-no-leak/
6. FinanceFeeds. Binance withdrawals to resume within 48 hours. 30.10.2026. https://financefeeds.com/binance-withdrawals-resume-48-hours/
7. CoinDesk. Live updates. 29–30.10.2026. https://www.coindesk.com/business/2026/10/29/live-updates-bitcoin-clings-to-usd80-000-as-strategy-s-cushion-thins-before-earnings

8. CoinDesk. Potential multi-billion Binance hack hitting crypto markets. 29.10.2026. https://www.coindesk.com/business/2026/10/29/potential-multi-billion-binance-hack-hitting-crypto-markets
9. TechCrunch. Binance pauses withdrawals. 29.10.2026. https://techcrunch.com/2026/10/29/binance-pauses-withdrawals-as-hackers-suspected-of-stealing-billions-in-crypto/
10. investingLive. Chainalysis estimates $5.9B stolen. 30.10.2026. https://investinglive.com/cryptocurrency/chainalysis-estimates-5-9b-stolen-in-suspected-binance-hack-nearly-4-times-bybit/
11. Associated Press (WFSB). North Korea-linked $6.3 billion hack, blockchain intelligence firms say. 30.10.2026. https://www.wfsb.com/2026/10/30/north-korea-linked-63-billion-hack-binance-blockchain-intelligence-firms-say/
12. Euronews / AFP. Binance confirms major hack. 30.10.2026. https://euronews.com/2026/10/30/crypto-platform-binance-confirms-major-hack-with-more-than-25bn-frozen
13. crypto.news. Binance hack: EIP-7702 wallet attack. 30.10.2026. https://crypto.news/binance-hack-eip-7702-wallet-attack/
14. PANews (CoinGlass data). One-hour liquidations. 29.10.2026. https://panews.io/articles/01a18974-b901-703b-9d7e-a863192210e2
15. crypto.news (CoinGlass data). Bitcoin price falls, liquidations. 30.10.2026. https://crypto.news/bitcoin-price-falls-binance-hack-liquidations/
16. Yahoo Finance. Bitcoin drops to $76,000 as Binance hack spooks investors (Fundstrat comment). 30.10.2026. https://finance.yahoo.com/markets/article/bitcoin-drops-to-76000-as-binance-hack-spooks-investors-tether-circle-freeze-assets-083406383.html
17. PANews. ZachXBT: Binance and Bitget funds consolidated via THORChain. 30.10.2026. https://panews.io/articles/01a18b2f-d427-707d-a6ae-55777882372c
18. TokenPost. Binance blocked North Korea-linked attacks (Contagious Interview). 27.10.2026. https://www.tokenpost.com/news/technology/41876
19. The Hacker News. Binance suffers security breach. 30.10.2026. https://thehackernews.com/2026/10/binance-suffers-security-breach.html
20. The Cryptonomist. Binance hacking update: withdrawals. 30.10.2026. https://en.cryptonomist.ch/2026/10/30/binance-hacking-update-withdrawal/
21. Paolo Ardoino (Tether), post on the USDT freeze. 29.10.2026. https://x.com/paoloardoino/status/2115918000373346709
22. Jeremy Allaire (Circle), post on the USDC freeze. 29.10.2026. https://x.com/jerallaire/status/2115916207463481846
23. ChainCatcher. Bybit: systems operating normally. 29.10.2026. https://www.chaincatcher.com/en/article/2300138
24. Forbes. Binance's $6.3 billion hack started with one engineer's laptop. 30.10.2026. https://www.forbes.com/sites/digital-assets/2026/10/30/binances-63-billion-hack-started-with-one-engineers-laptop/

Comparative incidents

25. FBI. PSA I-022625-PSA: North Korea responsible for $1.5 billion Bybit hack. 26.02.2025. https://ic3.gov/psa/2025/psa250226
26. The Hacker News. Safe{Wallet} confirms North Korean TraderTraitor hackers (Mandiant findings). 07.03.2025. https://thehackernews.com/2025/03/safewallet-confirms-north-korean.html
27. NK News. Crypto exchange sues North Korean government over $1.5B heist. 08.2026. https://www.nknews.org/2026/08/crypto-exchange-sues-north-korean-government-and-hackers-over-1-5b-heist/
28. Radiant Capital. Incident Update. 06.12.2024. https://medium.com/@RadiantCapital/radiant-capital-incident-update-e56d8c23829e
29. FBI. FBI, DC3 and NPA identification of North Korean cyber actors tracked as TraderTraitor. 23.12.2024. https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom
30. BleepingComputer. FBI links North Korean hackers to $308 million crypto heist. 24.12.2024. https://www.bleepingcomputer.com/news/security/fbi-links-north-korean-hackers-to-308-million-crypto-heist
31. Sky Mavis. Back to Building: Ronin Security Breach. 2022. https://roninchain.com/blog/posts/back-to-building-ronin-security-breach-6513cc78a5edc1001b03c364
32. The Block. How a fake job offer took down the world's most popular crypto game. 06.07.2022. https://www.theblock.co/post/156038/how-a-fake-job-offer-took-down-the-worlds-most-popular-crypto-game
33. BleepingComputer. FBI links largest crypto hack ever to North Korean hackers. 14.04.2022. https://www.bleepingcomputer.com/news/security/fbi-links-largest-crypto-hack-ever-to-north-korean-hackers
34. LastPass. Security Incident Update and Recommended Actions. 01.03.2023. https://blog.lastpass.com/posts/2023/03/security-incident-update-recommended-actions
35. LastPass. Incident 2: Additional details of the attack. 2023. https://support.lastpass.com/help/incident-2-additional-details-of-the-attack
36. CircleCI. CircleCI incident report for January 4, 2023 security incident. 12.01.2023. https://circleci.com/blog/jan-4-2023-incident-report

37. U.S. Department of the Interior, Office of Inspector General. Management Advisory: USGS IT Security Vulnerabilities. 17.10.2018. https://www.oversight.gov/sites/default/files/oig-reports/ManagementAdvisory%20_USGSITSecurityVulnerabilities_101718_0.pdf
38. CNN. Arup revealed as victim of $25 million deepfake scam. 16.05.2024. https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk
39. The Standard (Hong Kong). HK's first deepfake video conference scam. 04.02.2024. https://www.thestandard.com.hk/news/article/213122/HKs-first-deepfake-video-conference-scam-involving-HK200-million
40. MGM Resorts International. Form 8-K. 05.10.2023. https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm
41. Coinbase Global. Form 8-K. 14.05.2025. https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm
42. KnowBe4. How a North Korean fake IT worker tried to infiltrate us. 23.07.2024. https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
43. Okta. Unauthorized access to Okta's support case management system: root cause and remediation. 03.11.2023. https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause/
44. Uber. Security update. 2022. https://uber.com/newsroom/security-update
45. BleepingComputer. Bitget hacked via zero-day in third-party security products. 30.09.2026. https://www.bleepingcomputer.com/news/security/bitget-hacked-via-zero-day-in-third-party-security-products/amp/
46. The Defiant. Chainalysis links $387 million Bitget hack to North Korea. 02.10.2026. https://thedefiant.io/news/hacks/chainalysis-links-387-million-bitget-hack-to-north-korea

Statistics and context

47. The Record (Chainalysis data). Over $3 billion in crypto stolen in 2025. 18.12.2025. https://therecord.media/over-3-billion-crypto-stolen-2025-north-korea
48. PYMNTS (TRM Labs data). Bitget suffers year's largest crypto hack. 09.2026. https://www.pymnts.com/cryptocurrency/2026/bitget-suffers-years-largest-crypto-hack-as-losses-top-387-million/
49. Decrypt (TRM Labs data). North Korean hackers have stolen $6 billion in crypto. 30.04.2026. https://decrypt.co/366241/north-korean-hackers-stolen-6-billion-crypto-trm
50. WorldECR. North Korea stole $2.84B in crypto over 21 months, monitoring team reports. 30.10.2025. https://www.worldecr.com/news/north-korea-stole-2-84b-in-crypto-over-21-months-allied-monitoring-team-reports/

Threat intelligence and official advisories

51. CISA, FBI, U.S. Treasury. AA22-108A: TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies. 18.04.2022. https://www.cisa.gov/ncas/alerts/aa22-108a
52. FBI. PSA I-090324-PSA: North Korea aggressively targeting crypto industry. 03.09.2024. https://www.ic3.gov/PSA/2024/PSA240903
53. FBI. PSA I-012325-PSA: North Korean IT workers conducting data extortion. 23.01.2025. https://www.ic3.gov/PSA/2025/PSA250123
54. Microsoft Threat Intelligence. Contagious Interview: malware delivered through fake developer job interviews. 11.03.2026. https://microsoft.com/en-us/security/blog/2026/03/11/contagious-interview-malware-delivered-through-fake-developer-job-interviews
55. Google Cloud. Threat Horizons Report H2 2025 (UNC4899). 2025. https://services.google.com/fh/files/misc/cloud_threat_horizons_report_h22025.pdf
56. Palo Alto Networks Unit 42. Slow Pisces targets developers with coding challenges. 14.04.2025. https://unit42.paloaltonetworks.com/slow-pisces-new-custom-malware/
57. Palo Alto Networks Unit 42. Two campaigns by North Korea bad actors target job hunters. 21.11.2023. https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/
58. MITRE ATT&CK. Group G1052: Contagious Interview. https://attack.mitre.org/groups/G1052
59. MITRE ATT&CK. Group G0032: Lazarus Group. https://attack.mitre.org/groups/G0032

Standards, regulation and technical specifications

60. NIST. The NIST Cybersecurity Framework (CSF) 2.0. CSWP 29. 26.02.2024. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final
61. NIST. SP 800-207: Zero Trust Architecture. 2020. https://csrc.nist.gov/pubs/sp/800/207/final
62. NQA. ISO/IEC 27002:2022 mapping (Annex A control numbers of ISO/IEC 27001:2022). https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-27002-Mapping.pdf
63. CryptoCurrency Certification Consortium (C4). CCSS v9.0. 17.12.2024. https://cryptoconsortium.org/ccss-table-v9/
64. Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). https://eur-lex.europa.eu/eli/reg/2023/1114/oj

65. ESMA. Interactive Single Rulebook, MiCA, Articles 68, 75, 143. https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mica/article-75-providing-custody-and
66. Regulation (EU) 2022/2554 on digital operational resilience (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
67. FMA Austria. DORA: ICT-related incidents (reporting timelines under RTS 2025/301). https://www.fma.gv.at/en/dora-ict-related-incidents/
68. Ethereum Improvement Proposals. EIP-7702: Set Code for EOAs. https://eips.ethereum.org/EIPS/eip-7702
69. The Block. Wintermute warns Pectra upgrade leaves Ethereum users at risk of automated attacks. 01.06.2025. https://www.theblock.co/post/356481/wintermute-warns-pectra-upgrade-leaves-ethereum-users-at-risk-of-automated-attacks
70. Microsoft. Privileged access devices. https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-devices

Ukraine

71. Interfax-Ukraine. Second reading of the virtual assets bill postponed. 31.07.2026. https://interfax.com.ua/news/political/1189726.html
72. CERT-UA. Warning on campaign UAC-0145. 12.08.2026. https://cert.gov.ua/article/6318863
73. DOU. Russian hackers attack via fake job offers and a VPN client. 08.2026. https://dou.ua/lenta/news/russian-hackers-attack-vpn/
74. Hromadske. Verkhovna Rada backs cryptocurrency market legalization (first reading of No. 10225-d). 03.09.2025. https://hromadske.ua/en/politics/250673-verkhovna-rada-backs-cryptocurrency-market-legalization-details

Additional independent reconstructions and updates

75. Elliptic. The largest theft in history: North Korea likely behind the $6.4 billion Binance hack. 30.10.2026. https://www.elliptic.co/insights/binance-largest-hack-in-history/
76. Bitquery. Binance Hack: $6.3B Drained on 9 Chains, $2.7B Frozen. 30.10.2026. https://www.bitquery.io/investigations/binance-hack
77. Cointelegraph. Live updates: Binance $6.3B hack linked to North Korea's TraderTraitor (report of additional points of breach, 08:37 UTC). 30.10.2026. https://cointelegraph.com/news/live-updates-binance-63b-hack-linked-to-north-koreas-tradertraitor
78. The Crypto Times. Binance $6.3B Hack Update: More Breach Points, Withdrawals to Restart in 45 Hours. 30.10.2026. https://www.cryptotimes.io/2026/10/30/binance-hack-update-more-breach-points-withdrawals-to-restart-in-45-hours/
79. SecurityWeek. $6 Billion Binance Hack Bears Hallmarks of North Korea's TraderTraitor. 30.10.2026. https://www.securityweek.com/6-billion-binance-hack-bears-hallmarks-of-north-koreas-tradertraitor/
80. DefiLlama. Hacks dashboard (2026 losses as of 26.10.2026). https://defillama.com/hacks
81. Cointelegraph. North Korea's TraderTraitor linked to $6.3B Binance hack (Chainalysis estimate of $6.4 billion). 30.10.2026. https://cointelegraph.com/news/north-korea-linked-to-63b-binance-hack-by-crypto-investigators
82. Reuters (CP24). Binance's possible hack triggers US$3 billion freeze in crypto assets (Binance.US statement). 29.10.2026. https://www.cp24.com/news/money/2026/10/30/binances-possible-hack-triggers-us3-billion-freeze-in-crypto-assets/
83. TokenPost. Binance to Pause Ethereum Deposits and Withdrawals for Wallet Maintenance. 27.10.2026. https://www.tokenpost.com/news/technology/41825
84. Yahoo Finance (Unchained). Binance Says User Funds Are 'Completely Safe' After $3.5 Billion Drains From Its Hot Wallets. 29.10.2026. https://finance.yahoo.com/markets/crypto/articles/binance-says-user-funds-completely-214417766.html
85. ChainCatcher. Discuss the incident of Binance being hacked (Binance 14 as owner of Hot Wallet 34). 30.10.2026. https://www.chaincatcher.com/en/article/2300203
86. CryptoTicker. Binance Hack: Around $2.8 Billion Drained From a Hot Wallet (timeline, Spreek post). 29–30.10.2026. https://cryptoticker.io/en/binance-hack-hot-wallet-drained/

© 2026 National Cybersecurity Association of Ukraine · NCAU Analytical Center · NCAU-RR-2026-02