THREAT ADVISORY | NOVEMBER 1, 2026 · VERSION 1.0

# Binance Has the ISO Certificate. North Korea Has the Money.

On October 29, 2026, $6.36 billion disappears from Binance, the world's largest crypto exchange. Most of it in 31 minutes. The perpetrators have a name and a case number, and their method has been in an FBI advisory since April 2022. Binance is ISO 27001 certified and supervised in several countries. This text is about what a certificate proves. And about what a warning is worth when it is read but not acted on.

Author

**Daniel Thomas Heessel, CISO of the Year 2026, ISO 27001 Lead Auditor**

Audience

**CISOs, management, financial and crypto companies, SOC**

Classification

**TLP:CLEAR, sharing permitted**

As of

**November 1, 2026, version 1.0**

Sources

**TRM Labs, Elliptic, Bitquery, BitOK, Binance, CNBC, FBI, CISA, US Treasury, Mandiant, GitHub, Palo Alto Networks Unit 42, Wiz, xorl**

EIGHT ACTIONS

**1**

### Name the adversary

Not “cybercriminals” but TraderTraitor, with the reports from CISA, GitHub, Mandiant, the FBI and Unit 42 on the table.

Foundation for all seven acts

**2**

### Measure your own defense against its techniques

The seven acts are an audit program: what would we detect, what would we stop, where would we be blind?

Acts 1 to 7

**3**

### Protect technicians with privileged access like crown jewels

Hardened devices, no third-party code, short cloud sessions. A fake recruiter has to fail at the device, not at the employee’s vigilance.

Acts 1 to 3

**4**

### Separate the signature from the screen

Whatever is signed is verified on a device the adversary does not control.

Act 6: The Grab

**5**

### Limit the withdrawal path

Limits and emergency brakes. A wallet that releases billions in three minutes is a design flaw.

Act 6: The Grab

**6**

### Hunt for the adversary’s behavior

Freshly funded wallets, test transactions, signatures stockpiled in advance: all visible hours beforehand.

Act 5: The Dress Rehearsal

**7**

### Factor in the supply chain

Ginco, Safe, LayerZero, JumpCloud: every second entry point was at a service provider.

Acts 1 to 4 at the service provider

**8**

### Practice

Against this adversary’s documented chain, not against a phishing simulator.

Acts 1 to 7

# Management Summary

### What happened?

On October 29, 2026, $6.36 billion flowed out of Binance, the world’s largest crypto exchange, spread across ten blockchains, most of it in 31 minutes. According to the exchange, the incident may have started with the laptop of a DevOps engineer; TRM Labs assumes the adversary controlled the signing system for withdrawals. Tether, Circle and other issuers froze $2.7 billion, and $2.4 billion is out of reach.

### What does it mean?

TRM Labs attributes the attack with high confidence to the North Korean group TraderTraitor, and the FBI confirms North Korean perpetrators. The FBI, CISA and the US Treasury have described its approach since April 2022: fake recruiters, rigged hiring tests, stolen sessions, manipulated signatures. Binance has been ISO 27001 certified since 2019. The certificate measures whether processes exist, not whether they work against this adversary.

### What do we need to do?

Name the adversary and test your own defense against its seven acts: what would we detect, what would we stop, where would we be blind? Harden the devices of technicians with privileged access, verify signatures on a device the adversary does not control, limit withdrawals and hunt for the adversary's behavior instead of working through the control catalog.

### Why this advisory matters for regulation

With control A.5.7, ISO 27001:2022 requires threat intelligence, that is, the analysis of information about adversaries. DORA requires large financial entities to run tests that replicate the techniques of real adversaries against their own organization. This advisory provides a named adversary with a documented technique chain mapped to MITRE ATT&CK.

## The Binance hack: $6.36 billion in one night

The actual attack on Binance begins one day before the theft of $6.36 billion. On October 28, the adversary sets up a wallet and, via a service that conceals where money comes from, sends it about one ether, a little over $2,000. On October 29, the adversary tests the attack code against third-party wallets. Four hours after the last test, the code sits on a Binance hot wallet, a wallet that is constantly online because the exchange uses it to process customer withdrawals.

At 8:05 p.m. UTC, 9:05 p.m. in Frankfurt, the outflow begins, first on the XRP Ledger. All further times are UTC. Within 20 minutes, Solana, Optimism, Bitcoin and Tron follow, then Ethereum, where most of the money sits. There, the adversary had obtained 50 signatures from the Binance wallet in advance. One of them is enough to bring the wallet under the adversary's control. Three minutes later it is empty: 167,464 ether and 1.6 billion Tether in a single transaction. Until midnight, the adversary comes back six times and sweeps whatever customers have deposited in the meantime. Ten blockchains, one adversary, half an hour for what matters.

### Chronology

| | |
|---|---|
| **Oct. 28** | Three withdrawals from the mixing service Tornado Cash fund a fresh wallet for the adversary |
| **Oct. 29, 2:28 a.m. to 4:47 p.m.** | Two test runs of the attack code against third-party wallets |
| **8:05 p.m.** | The outflow begins on the XRP Ledger: 233 million XRP |
| **8:10 p.m.** | Solana and Optimism |
| **8:20 p.m.** | Bitcoin: 18,270 BTC |

| | |
|---|---|
| **8:21 p.m.** | Ethereum: the adversary uses one of 50 signatures (authorizations) obtained in advance |
| **8:22 p.m.** | Tron: 612 million USDT |
| **8:24 p.m.** | Ethereum wallet emptied: 167,464 ether and 1.6 billion Tether in one transaction |
| **8:32 p.m.** | The analyst Spreek makes the case public |
| **8:41 p.m.** | First sweep: 823 million USDC |
| **8:57 p.m.** | World Liberty is the first issuer to freeze funds |
| **9:01 p.m.** | Tether freezes 971 million USDT, the first major freeze |
| **9:04 p.m.** | Circle freezes 823 million USDC |
| **10:01 p.m.** | Ripple freezes RLUSD |
| **10:33 p.m.** | Binance pauses withdrawals |
| **11:56 p.m.** | Last sweep |
| **Oct. 30, 12:10 a.m.** | Binance revokes the authorization |
| **2:25 a.m.** | Binance reports first findings |

The adversary is slowed down not by Binance but by the companies that issue stablecoins such as Tether and USD Coin. They can freeze their tokens at the push of a button. At 9:01 p.m., Tether freezes $971 million, 37 minutes after the big outflow, and Circle freezes $823 million three minutes later. The adversary sees the freezes coming and sells whatever can still be sold, at a discount of more than ten percent. Binance halts withdrawals at around 10:33 p.m. and reports first findings at 2:25 a.m.

By morning, $6.36 billion is gone. $2.7 billion of it sits frozen at the adversary's addresses, and $2.4 billion in ether and bitcoin is out of reach. One question remains: how does someone get Binance wallets on ten blockchains to sign their transactions?

**$6.36B**
stolen in one night

**31 min**
for most of it, across ten blockchains

**$2.7B**
frozen by issuers

**4.5 years**
between the FBI warning and the Binance hack

Binance answers the next day, cautiously. The incident may have started with the laptop of a DevOps engineer, meaning a technician who runs the exchange's systems. Through this laptop, the adversary is said to have reached an internal system and triggered withdrawals from there. It was

not a one-click attack, there were further entry points, and private keys had not been leaked. TRM Labs goes a step further: the adversary had probably taken control of the system Binance uses to sign its withdrawals.

A laptop. Anyone who has understood that sentence knows the rest of the story. This attack path had been in an FBI advisory for four and a half years.

## Binance: systemically important, certified, controversial

Binance was founded in 2017 and has been the world's largest crypto exchange ever since. In early 2026, the exchange held reserves of around $155 billion and turned over $2.1 trillion in one month, 2.6 times as much as the next competitor. Depending on how it is counted, between a quarter and almost 40 percent of global spot trading runs through Binance. That is where the price of bitcoin is set. When Binance wobbles, the market wobbles: after the attack, bitcoin lost five percent within hours, and shares in Coinbase and Robinhood fell. Binance is to crypto what a systemically important bank is to the money market, only without deposit insurance, without published financial statements and, for a long time, without a headquarters.

The doubts are almost as old as the exchange. In 2019, Binance lost 7,074 bitcoin from a hot wallet because adversaries had collected user credentials through phishing; the alarms went off when the money was already gone. In 2022, an adversary stole around $570 million from the blockchain that Binance itself operates. The exchange then simply halted the entire network, which should not even be possible on a supposedly decentralized blockchain. On top of that came the corporate structure: dozens of companies, no audited financial statements. A proof of reserves from the auditor Mazars at the end of 2022 lasted only days, then Mazars withdrew from the crypto business. In 2023, the US Securities and Exchange Commission accused Binance of commingling customer funds worth billions. In November 2023, Binance and founder Changpeng Zhao pleaded guilty to failing to maintain an effective anti-money laundering program: a $4.3 billion penalty, a compliance monitor in-house, four months in prison for Zhao. President Trump pardoned Zhao in 2025, and Zhao remained the largest shareholder. Since then, Richard Teng, a former financial regulator, and co-founder Yi He have run the business.

In Europe, the MiCA regulation with its licensing requirement has applied since the end of 2024. Binance did not get a license, withdrew its application and largely discontinued its offering for EU customers in July 2026. Teng then criticized Brussels: 70 percent of the affected users had moved their money into self-custody wallets, where the risk was higher. That sentence is worth remembering.

Yet on paper, Binance is a model student. The exchange has been ISO 27001 certified since 2019, one of the first crypto platforms to be so. In 2023, certificates for France, the Emirates, Bahrain and Turkey followed, along with a SOC 2 report for the global platform. The then head of security spoke of proven effective controls. Binance has not published whether the certificates are still valid in

2026 and cover the wallet systems. For this text, that does not matter. The question is not whether a certificate was missing but what a certificate proves. The supervisory rules surrounding Binance deal with money laundering, client assets and transparency. None of them asks how to protect a technician's laptop against a North Korean adversary posing as a recruiter.

## TraderTraitor: who is behind the Binance hack

Who did it is considered settled. TRM Labs attributes the attack with high confidence to the North Korean group TraderTraitor, and the FBI confirms North Korean perpetrators. To understand this group, you have to go back to the beginning: to a paper from Washington.

On April 18, 2022, the FBI, the cybersecurity agency CISA and the US Treasury publish a joint paper, 14 pages, readable by anyone. It describes a North Korean campaign against crypto companies and gives it the name TraderTraitor. The entry point, according to the paper: employees of crypto companies, often system administrators and DevOps technicians, are offered highly paid jobs via job portals and messengers and are asked to install software for them that takes over the computer. The paper lists the names of the programs, the checksums of the files and the addresses of the servers. It can still be downloaded today.

The group has since acquired many names: UNC4899 at Google and Mandiant, Jade Sleet at Microsoft, Slow Pisces at Palo Alto Networks. Mandiant assigns it to the Reconnaissance General Bureau, North Korea's foreign intelligence service. Its goal is not espionage but foreign currency.

Where it sits in the state apparatus can be reconstructed from public sources. Since 2021, the security researcher xorl has maintained a map of North Korea's cyber units, built on Mandiant's analyses, US indictments and defector reports. According to it, the chain of command runs from Kim Jong Un through the General Staff to the intelligence service, there to the 3rd Bureau and on to Lab 110, the core of what the world calls "Lazarus." TraderTraitor is the line in this network that specializes in crypto assets. The US Treasury placed Lazarus exactly there in 2019: in the 110th Research Center of the 3rd Bureau.

### Place in the state apparatus

| Level | Unit | Classification |
|---|---|---|
| **State leadership** | **Kim Jong Un**<br>***Chain of command*** | Supreme Leader. At the top of the chain of command, which according to xorl runs through the General Staff to the intelligence service and on to the cyber units. |
| | **State Affairs Commission**<br>***Chain of command*** | State leadership |

| | | |
|---|---|---|
| **Military** | **General Staff of the Korean People's Army**<br>***Chain of command*** | Military command |
| **Intelligence service** | **Reconnaissance General Bureau (RGB)**<br>***Chain of command*** | Foreign intelligence service. Formed in 2009, sanctioned by the United Nations since 2016. The RGB runs almost all of North Korea's cyber operations; Mandiant assigns TraderTraitor to it. |
| **RGB bureaus** | 1st Bureau | Operations |
| | 2nd Bureau | Reconnaissance |
| | **3rd Bureau**<br>***Chain of command*** | Foreign intelligence and cyber. This is where the US Treasury has placed the Lazarus unit since 2019. There is no 4th Bureau; four is considered an unlucky number in Korea. |
| | 5th Bureau | Inter-Korean affairs and cyber |
| | 6th Bureau | Technology |
| | 7th Bureau | Support |
| **Cyber unit** | Bureau 325 | Since 2021, assignment uncertain |
| | **Lab 110**<br>***Chain of command*** | 110th Research Center. Expanded successor to "Bureau 121" and the core of what the world calls "Lazarus." The US Treasury placed Lazarus exactly here in 2019: in the 110th Research Center of the 3rd Bureau. |
| | Kimsuky | 5th Bureau: espionage, think tanks |
| **Activity clusters** | TEMP.Hermit | Espionage, government, defense. Attributed: Sony 2014, WannaCry 2017. |
| | APT38 · BlueNoroff | Bank heists, SWIFT, financial institutions. Attributed: Bangladesh central bank 2016. |
| | Andariel | Military, government agencies, defense industry. Espionage plus side income. |
| | **TraderTraitor**<br>***Chain of command*** | Digital assets, active since 2020. The line specializing in crypto assets. Also known as UNC4899 (Google, Mandiant), Jade Sleet (Microsoft) and Slow Pisces (Palo Alto Networks). Attributed: DMM Bitcoin, Bybit, KelpDAO and, according to TRM Labs with high confidence, Binance. |

About a third of North Korea's foreign currency earnings in 2024 came from cyber theft (MSMT). According to the UN, the FBI and OFAC, the money flows into the missile and nuclear program.

Reconstructed from xorl (v2.2, 2023), Mandiant (2022, 2023) and the US Treasury (OFAC designation of Lazarus, 2019). "Lazarus Group" is the media's umbrella term for the clusters. Outside the RGB operate the Ministry of State Security (APT37), the United Front Department and the IT worker programs. Since 2023, Mandiant has described a blurring of the units with shared tools and targets. Confidence: high at cluster level (FBI, Mandiant), medium at bureau level (defectors, OSINT).

This organization is no phantom. It has bureau numbers, front companies in China, employees indicted by name and a mission. In 2024, the UN Panel of Experts estimated that North Korea had stolen more than three billion dollars in crypto assets since 2017; a successor body puts the share of cyber loot in the country's foreign currency earnings for 2024 at around one third. According to the UN and the US government, the money flows into the missile and nuclear program. Whoever empties Binance finances warheads.

## TraderTraitor's TTPs: a heist in seven acts

The 2022 paper describes the first act. The group has performed the other six in plain sight since then. Each one is documented and carries numbers from MITRE ATT&CK, the technique catalog that is the industry's common language.

### The attack chain in seven acts

| Act | Approach | Techniques (MITRE ATT&CK) | Described since |
|---|---|---|---|
| **1 The First Contact** | A recruiter, an investor or a developer gets in touch on LinkedIn, Telegram or Slack. The targets are people with keys: DevOps and wallet technicians. Sometimes the adversary writes from a hijacked real profile. | T1585 Establish Accounts<br>T1566.003 Spearphishing via Service<br>T1593.001 Social Media | FBI/CISA 04/2022 · GitHub 07/2023 |
| **2 The Bait** | A hiring test, a coding assignment, a Docker container. The code looks harmless because the malicious part is only loaded later, and only for the right victim. It is only loaded if address, location and time of day match the expected victim. At Bybit, the Docker project posed as a stock simulator. | T1204.002 Malicious File<br>T1195.001 Compromise Software Dependencies and Development Tools<br>T1027 Obfuscated Files or Information | CISA 04/2022 · Unit 42 04/2025 |

| | | | |
|---|---|---|---|
| **3 The Stolen Identity** | The malware collects whatever is on the laptop: SSH keys, cloud credentials, session data. With stolen sessions, multi-factor authentication comes to nothing, and the adversary appears as the employee. At DMM Bitcoin, the session data of an employee at the service provider Ginco was enough. | T1552.001 Credentials In Files<br>T1552.004 Private Keys<br>T1539 Steal Web Session Cookie<br>T1528 Steal Application Access Token | FBI 12/2024 (DMM) · Unit 42 04/2025 |
| **4 Time in the System** | At Bybit, the adversaries moved through the cloud of the wallet provider Safe for twelve days, during the working hours of the developer whose identity they had assumed. Access via VPN, admin rights identified, the MFA requirement switched off, roles scouted. | T1078.004 Cloud Accounts<br>T1556.006 Multi-Factor Authentication<br>T1087.004 Cloud Account<br>T1090 Proxy | Mandiant 07/2023 · Sygnia 02/2025 · Google 07/2025 |
| **5 The Dress Rehearsal** | Files swapped, code tested, signatures stockpiled. At Drift, the technical preparation began three weeks before the grab. At Bybit, files in the cloud were swapped for manipulated versions. At Binance, the adversary rehearsed the code on third-party wallets and stockpiled 50 signatures. | T1195.002 Compromise Software Supply Chain<br>T1565.001 Stored Data Manipulation<br>T1608 Stage Capabilities | Safe/Mandiant 03/2025 · TRM 04/2026 |
| **6 The Grab** | The wallet key is never stolen. What gets manipulated is what gets signed. The outflow takes 12 minutes (Drift), 20 (Bitget) or 31 (Binance). At Bybit, the signers saw a genuine transaction, but a different one was executed. At Binance, the signing system signed for ten blockchains. | T1565 Data Manipulation<br>T1657 Financial Theft<br>T1557 Adversary-in-the-Middle | FBI 12/2024 · Sygnia 02/2025 |
| **7 The Getaway with the Loot** | Tracks are covered, and the tools delete themselves. The loot is collected in ether and laundered through traders. At Bybit, the manipulated files were replaced again two minutes after the transaction. Bitcoin is broken up into small pieces. | T1070.003 Clear Command History<br>T1070 Indicator Removal<br>T1485 Data Destruction | Safe/Sygnia 03/2025 · TRM 10/2026 |

Test question for every act: what would we detect, what would we stop, where would we be blind?

Four things make this play so successful, and none of them is a software vulnerability: a person with privileged access; multi-factor authentication that does not detect stolen sessions; service providers as the entry point; patience that ends in a single strike.

## Since April 2022, every victim was preceded by a warning

None of this was secret. The chain of warnings begins in April 2022 and becomes more precise every year.

| Date | Publisher | What was documented |
|---|---|---|
| **April 2022** | FBI, CISA, US Treasury (AA22-108A) | Spearphishing against employees of crypto companies, often in system administration or DevOps, disguised as recruiting for highly paid jobs; the malicious code is hidden in trojanized crypto apps |
| **June and July 2023** | Phylum, GitHub | Fake developer and recruiter profiles on GitHub, LinkedIn, Slack and Telegram; invitations to collaborate on repositories with malicious npm dependencies, disguised as media players or trading tools |
| **July 2023** | Mandiant | Entry via the identity provider JumpCloud, execution of a Ruby script via its agent at customers in the crypto industry; attribution to UNC4899 after an operational security slip revealed a North Korean IP address |
| **August and September 2023** | FBI | Alphapo, CoinsPaid, Atomic Wallet, Stake; call on the industry to read the TraderTraitor warning |
| **December 2024** | FBI, DC3, Japanese police | DMM Bitcoin: LinkedIn recruiter, Python script as a hiring test on GitHub, stolen session cookies, manipulated transaction request |
| **February and March 2025** | FBI, Sygnia, Mandiant, Safe | Bybit: compromised developer Mac, AWS session tokens to bypass MFA, twelve days of reconnaissance, manipulated JavaScript files |
| **April 2025** | Palo Alto Networks Unit 42 | Campaign with coding assignments, documented down to hash level: PDF job description, questionnaire, malicious code only for selected victims, YAML deserialization, RN Loader and RN Stealer |
| **July 2025** | Google Threat Intelligence Group | Freelance lures via LinkedIn and Telegram, malicious Docker containers, disabling of the MFA requirement in Google Cloud, swapped JavaScript files |

In March 2024, a supposed recruiter contacted an employee of the Japanese wallet company Ginco and sent a hiring test on GitHub. Two months later, the adversaries used the employee's session data to manipulate a transaction of the customer DMM Bitcoin: $308 million. In February 2025,

a developer at the wallet company Safe launched a Docker project that posed as a stock simulator. Twelve days later, Bybit was $1.5 billion poorer. In April 2026, Drift and KelpDAO followed, and in September, Bitget. And in October, Binance, four and a half years after the FBI had named DevOps technicians at crypto companies as a preferred target. In April 2025, Unit 42 had noted that the group's approach had remained the same for months. Why change anything? It worked.

| Victim | Date | Loss (USD) | Entry point | Attribution |
|---|---|---|---|---|
| **Ronin / Sky Mavis** | March 2022 | 625 million | Social engineering | FBI: Lazarus, APT38 |
| **Atomic Wallet, Alphapo, CoinsPaid** | June and July 2023 | 197 million | CoinsPaid: an employee downloaded software with malicious code via phishing | FBI: TraderTraitor |
| **JumpCloud customers** | June 2023 | no theft proven | Identity provider as supply chain | Mandiant: UNC4899 |
| **DMM Bitcoin via Ginco** | May 2024 | 308 million | LinkedIn recruiter, hiring test on GitHub, session cookies | FBI, Japanese police |
| **Bybit via Safe{Wallet}** | February 2025 | 1.5 billion | Developer Mac, AWS session tokens, manipulated signing interface | FBI |
| **Drift Protocol** | April 2026 | 285 million | Six months of social engineering posing as a trading firm, in-person meetings at conferences, pre-signed transactions | Drift, SEAL: North Korea (cluster UNC4736) |
| **KelpDAO via LayerZero** | April 2026 | 292 million | Compromised verifier nodes, config-uration with a single verifier (1-of-1) | LayerZero: TraderTraitor |
| **Bitget** | September 2026 | 387.5 million | Backend wallet system, signing logic subverted, third-party security product | unconfirmed; fund flows overlap with Binance |
| **Binance** | October 2026 | 6.36 billion | DevOps laptop, service container, signing infrastructure | TRM: TraderTraitor; FBI: North Korea |

Since April 2022, every victim was preceded by a report describing the entry point it would be hit with shortly afterwards. This is not a story about vulnerabilities. It is a story about what comes after reading.

## Certified, audited, emptied: what ISO 27001 proves and

## what it does not

For years, I have audited information security management systems as a lead auditor, and I have built four myself. An ISO 27001 certificate proves that an organization operates such a system: that it assesses risks, implements controls and audits itself internally. The auditor sees this in samples, a few days a year. The standard even explicitly requires threat intelligence, that is, the analysis of information about adversaries. The auditor checks whether this process exists. Whether a technician's laptop withstands a fake recruiter is not something the auditor checks. That does not fit into any audit program.

Binance had threat intelligence. For years, the exchange has tracked down North Korean loot, and it employs one of the largest security teams in the industry. The knowledge was there. It was not translated into architecture and detection. That is the difference between threat intelligence and Threat-Informed Defense, and this night proves it.

The architecture: whoever gets the signing system for wallets on ten blockchains to sign within half an hour hits no limit. Nothing stopped a wallet that paid out more in three minutes than it normally does in weeks. $6.36 billion in one night is not just a detection problem. It is an architecture decision.

Detection: this attack announced itself. A freshly funded wallet, test runs on the day of the attack, then 15 minutes between the first outflow and the access to Ethereum, then 37 minutes until the first major freeze by Tether. Whoever hunts for the adversary's behavior has hours of lead time that evening. Whoever only works through the control catalog sees nothing until the outflow. The attack was discovered not by Binance's own detection but from the outside. The pattern is familiar from Germany: in the Berlin state network, a data exfiltration went unnoticed for five days, and there, too, it was discovered from the outside.

The human factor: the laptop of a technician with access to withdrawal systems is not an office computer. It deserves as much protection as a company's central directory service. No code from a recruiter's repository is run on such a device. That rule is not in any certificate. It is in the reports on DMM Bitcoin and Bybit.

And the certificate itself: it is not worthless. It proves that Binance operates a management system. It proves nothing about the question that decided this evening: whether an organization knows its adversary and has built and tested its defense against the adversary's techniques. Certificates measure whether processes exist. Adversaries measure whether they work. Binance went through both measurements. It passed the first in 2019. The second took 31 minutes.

## Who bears the loss and where the money goes

Binance bears the loss, not its customers. The day after, Richard Teng said the company had set aside $6.34 billion in corporate funds. On October 31, the exchange reported that 90 percent of the stolen holdings had been replaced, from three pots: the emergency fund SAFU, an insurance fund for derivatives trading and the group's treasury. Withdrawals are resuming in stages, and a new proof of reserves has been announced.

Nobody outside can verify this; Binance does not publish financial statements. Teng says the group holds its profits in crypto assets and can absorb the loss. With two trillion dollars in monthly trading volume, that is plausible, and so the question of whether the biggest bankruptcy in crypto history is looming comes too early. FTX did not collapse in 2022 because of a hack but because customer funds were gambled away. Binance insists that its customer funds sit untouched in cold wallets that are not connected to the internet. The test comes when all withdrawals are open again.

Frozen is not recovered. The $2.7 billion that Tether, Circle, Ripple and others have frozen is stuck at the adversary's addresses; getting it back takes courts and time. What stands out is who acted: no regulator, not the exchange, but private companies that can freeze their tokens at the push of a button. The crypto world, which cultivates freedom from censorship as its founding myth, was saved from the worst by exactly the kind of central intervention it rejects.

The $2.4 billion out of reach is more than any single earlier crypto heist. It is moving via bridges, exchange services and traders toward Pyongyang, like the loot from Bybit, Drift, KelpDAO and Bitget. With $6.36 billion, a state under comprehensive sanctions captured more in one night than the UN panel attributed to it for six years in total. Without exploiting a single vulnerability in any software.

And regulation? Binance left Europe in July, so EU customers were hardly affected. Teng's sentence from July sounds different now: this time, the higher risk was not in customers' wallets but in a hot wallet of the exchange. Experts told CNBC that US regulators would not have prevented this incident either, because it started with a laptop. Rules on money laundering, client assets and transparency produce audit reports. They do not produce resilience.

## Whoever does not know their adversaries defends against nothing

Every major incident is followed by calls for more rules, more certificates, more evidence. The Binance case refutes this reflex. Binance was certified, audited and supervised. The perpetrator was known by name, its techniques cataloged. None of that mattered in the 31 minutes when it counted. Compliance alone does not stop adversaries.

The mistake lies in the order. Whoever starts with the control catalog defends against the standard. Whoever starts with the adversary defends against the adversary.

Threat-Informed Defense answers three questions: Who is attacking us? How do we detect them? What do we do to make them fail? Binance could answer the first. It failed at the other two, like Bybit, DMM, Drift, KelpDAO and Bitget before it. What this requires is laid out in this case; the eight actions that follow from it are at the start of this advisory, each assigned to one act of the attack chain.

The lesson reaches beyond crypto. The same technicians, signing systems and cloud sessions exist in every bank and every insurer. The difference lies not in the number of rules but in what they test: existence or effectiveness. European financial supervisors have understood this: DORA requires large financial entities to run tests that replicate the techniques of real adversaries against their own organization. That is Threat-Informed Defense with the force of law.

Binance knew who was coming. It knew how. It was certified. And in one night it lost $6.36 billion to an adversary the FBI had warned about four and a half years earlier. Binance still has the certificate. North Korea has the money.

# What this advisory is based on

Caveats on the facts (as of November 1, 2026). The entry via the DevOps laptop has so far come from Binance alone; a technical post-incident report has been announced. The assessment of the signing infrastructure is an evaluation by TRM Labs. TRM makes the attribution to TraderTraitor with high confidence, and the FBI confirms North Korean actors. The link to Bitget drawn by BitOK is an analytical attribution, not a proven identity. Drift and SEAL 911 attribute Drift to the cluster UNC4736, not TraderTraitor; the North Korea attribution of Bitget is unconfirmed. The certification information is based on Binance press releases from 2019 and 2023; whether the certificates are valid in 2026 and cover the wallet infrastructure has not been published. All loss amounts are valuations at the time of the outflow. The times of the night come from TRM Labs, Elliptic, Bitquery, BitOK and Binance's statements, the time of the withdrawal pause from press reports. Technique IDs per MITRE ATT&CK Enterprise.

### On the Binance hack

- TRM Labs: North Korea Steals USD 6.36 Billion From Binance
  https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history
- Elliptic: The largest theft in history
  https://www.elliptic.co/insights/binance-largest-hack-in-history/
- Bitquery: Binance hack investigation
  https://www.bitquery.io/investigations/binance-hack

- BeInCrypto / BitOK: How did the Binance hack happen? (German)
  https://de.beincrypto.com/wie-binance-hack-passierte/
- Richard Teng on X, October 30, 2026
  https://x.com/_RichardTeng/status/2116072080525656150
- Decrypt: Binance Sets Aside $6.34B
  https://decrypt.co/382237/binance-sets-aside-6-34b-to-cover-hack-losses-ceo-says-your-assets-are-safe
- CNBC: Binance resumes withdrawals, 90% covered
  https://www.cnbc.com/2026/10/31/binance-hack-asset-coverage-withdrawals.html
- CNBC: Hack raises questions about wallet safety
  https://www.cnbc.com/2026/10/31/binance-hack-crypto-wallet-safety.html
- Axios: Binance halts trading
  https://www.axios.com/2026/10/29/binance-cyberattack-crypto-heist

## On the actor and its place in the state

- FBI, CISA, US Treasury: AA22-108A TraderTraitor (April 2022)
  https://www.cisa.gov/ncas/alerts/aa22-108a
- xorl: North Korea (DPRK) Cyber Operations Groups, v2.2
  https://xorl.wordpress.com/2021/04/24/north-korea-dprk-cyber-operations-groups/
- Mandiant: Not So Lazarus (2022)
  https://cloud.google.com/blog/topics/threat-intelligence/mapping-dprk-groups-to-government
- Mandiant: Assessed Cyber Structure of North Korea in 2023
  https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023
- Mandiant: JumpCloud supply chain, UNC4899 (July 2023)
  https://cloud.google.com/blog/topics/threat-intelligence/north-korea-supply-chain
- GitHub Security Alert (July 2023)
  https://github.blog/2023-07-18-security-alert-social-engineering-campaign-targets-technology-industry-employees
- FBI: Cryptocurrency funds stolen by DPRK (August 2023)
  https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk
- FBI PSA: North Korea responsible for Bybit hack (February 2025)
  https://ic3.gov/psa/2025/psa250226
- Unit 42: Slow Pisces coding challenges (April 2025)
  https://unit42.paloaltonetworks.com/slow-pisces-new-custom-malware/
- Wiz: TraderTraitor Deep Dive
  https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist
- heise: First investigation details on the Bybit case (German)
  https://heise.de/-10317026
- TRM Labs: Drift Protocol
  https://www.trmlabs.com/resources/blog/north-korean-hackers-attack-drift-protocol-in-285-million-heist
- Security Affairs: Kelp DAO, LayerZero attribution
  https://securityaffairs.com/?p=191092

- Security Affairs: DMM Bitcoin, FBI attribution
  https://securityaffairs.com/?p=172290

### On Binance, certification and regulation

- Decrypt: Binance granted ISO 27001 (2019)
  https://decrypt.co/9562/binance-iso27001-security-standard
- Binance: ISO 27001 and 27701 certifications (June 2023)
  https://www.aap.com.au/aapreleases/cision20230605ae19512
- Binance: SOC 2 Type II (December 2023)
  https://www.aap.com.au/aapreleases/cision20231218ae96171/
- Fortune: Trump pardons Changpeng Zhao
  https://www.fortune.com/crypto/2025/10/23/binance-changpeng-zhao-cz-pardon-president-donald-trump
- BTC-ECHO: Binance takes stock after leaving Europe (German)
  https://www.btc-echo.de/schlagzeilen/binance-zieht-bilanz-nach-europa-aus-risiko-durch-mica-gestiegen-234128/
- TechCrunch: Binance pledges changes after 2019 hack
  https://techcrunch.com/?p=1825646
- Daniel Heessel: Berlin cannot be blackmailed. But it can be plundered. (Security Insider, German)
  https://www.security-insider.de/berlin-hack-2026-rhysida-datenabfluss-kritis-luecke-a-632d35c84df369df3b73627b27e021a3/

## How we can support you with implementation

This advisory shows how TraderTraitor operates and why a certificate alone does not protect against it. Whether your defense holds up against this attack chain can only be answered on your own infrastructure.

We work with you to check which of the seven acts your detection sees today, where you would be blind and which action has the greatest leverage: in an ISMS under ISO 27001, in preparing for threat-led tests under DORA and in getting ready for an incident.

**Contact us for an initial conversation.**
**kontakt@threat-informed.de | www.threat-informed.de**

*This advisory is part of our threat briefings for companies under NIS2, DORA and critical infrastructure rules in Germany, Austria and Switzerland. TLP:CLEAR, sharing permitted. As of: November 1, 2026, version 1.0.*

## Glossary

| Term | Meaning |
|---|---|
| ATT&CK | MITRE knowledge base of adversary tactics and techniques; T numbers denote techniques |
| Attribution | Assigning an attack to an actor, with a statement of confidence |
| Cold wallet | Wallet with no connection to the internet, used to hold large balances |
| DevOps | Teams that develop software and run the systems it runs on; they often have far-reaching privileges |
| Issuer | Company that issues a stablecoin and can freeze its tokens |
| Hot wallet | Wallet that is permanently online so the exchange can process withdrawals from it |
| MFA | Multi-factor authentication |
| RGB | Reconnaissance General Bureau, North Korea's foreign intelligence service |
| Session cookie | Session data after a successful login; whoever steals it needs neither password nor second factor |
| Stablecoin | Token with a fixed value, usually pegged to the US dollar, such as Tether (USDT) or USD Coin (USDC) |
| Threat-Informed Defense | Defense that starts from the known behavior of real adversaries rather than from the control catalog |
| TLP | Traffic Light Protocol: marking that indicates how widely information may be shared |
| TTP | Tactics, Techniques, Procedures: how adversaries operate |