FALLANALYSE · BINANCE, 29. OKTOBER 2026

Binance hat das ISO-Zertifikat. Nordkorea hat das Geld.

Wie Nordkorea in einer Nacht **6,36 Milliarden Dollar** von der größten Kryptobörse der Welt holte, obwohl der Angriffsweg seit **April 2022** in einem Papier des FBI stand. Was ein Zertifikat beweist, was eine Warnung wert ist, und was daraus für jede Bank, jedes Krankenhaus und jeden Energieversorger folgt.

DIE BEFEHLSKETTE

Von der Staatsspitze bis zur Binance-Wallet, rekonstruiert aus öffentlichen Quellen



Verortung nach xorl (DPRK Cyber Operations Groups), Mandiant (Assessed Cyber Structure of North Korea, 2023) und US-Finanzministerium (2019: Lazarus im 110. Forschungszentrum des 3. Büros). Zuordnung des Binance-Angriffs zu TraderTraitor: TRM Labs; das FBI bestätigt nordkoreanische Täter.

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

threat-informed.de

AUF EINEN BLICK

Am 29. Oktober 2026 verschwinden 6,36 Milliarden Dollar von der größten Kryptobörse der Welt, der Großteil in 31 Minuten. Die Täter haben einen Namen und ein Aktenzeichen, ihre Methode steht seit April 2022 in einem Papier des FBI. Binance ist nach ISO 27001 zertifiziert und in mehreren Ländern beaufsichtigt. Dieser Text handelt davon, was ein Zertifikat beweist. Und was eine Warnung wert ist, die gelesen, aber nicht umgesetzt wird.

6,36 Mrd. $
in einer Nacht gestohlen, der Großteil in 31 Minuten; 2,7 Mrd. eingefroren, 2,4 Mrd. außer Reichweite

31 Minuten
vom ersten Abfluss bis zur leeren Ethereum-Wallet; die erste große Sperre kam nach 37 Minuten, von Tether

4,5 Jahre
zwischen der Warnung des FBI vom April 2022 und dem Angriff; dazwischen DMM Bitcoin, Bybit, Drift, KelpDAO

0 Lücken
in Software ausgenutzt: ein Laptop, ein falscher Recruiter, eine gestohlene Sitzung, eine manipulierte Signatur

Das Wichtigste in Kürze

- Am 29. Oktober 2026 verliert Binance, die größte Kryptobörse der Welt, 6,36 Milliarden Dollar. TRM Labs ordnet den Angriff der nordkoreanischen Staatseinheit TraderTraitor zu, das FBI bestätigt nordkoreanische Täter.
- Der Einstieg, so Binance, war der Laptop eines DevOps-Technikers. Genau diesen Weg beschrieb das FBI im April 2022. Seitdem hat die Gruppe mit demselben Muster DMM Bitcoin, Bybit, Drift und KelpDAO getroffen.
- Binance ist seit 2019 nach ISO 27001 zertifiziert, hat einen SOC-2-Bericht und wird in mehreren Ländern beaufsichtigt. Das Zertifikat beweist, dass Prozesse vorhanden sind. Ob sie gegen diesen Gegner wirken, prüft kein Audit.
- Der Fall ist kein Erkennungsproblem allein, sondern eine Architekturentscheidung: Nichts hat eine Wallet angehalten, die in drei Minuten mehr auszahlte als sonst in Wochen.
- Die Lehre reicht über Krypto hinaus: Dieselben Techniker, Signatursysteme und Cloud-Sitzungen gibt es in jeder Bank, jeder Versicherung, jedem Krankenhaus. Kapitel 9 nennt acht Maßnahmen, Kapitel 10 zehn Prüffragen.

ZIELGRUPPE
Vorstände und Geschäftsführung, CISOs, ISMS-Verantwortliche, interne und externe Auditoren, Aufsicht

REGULATORISCHER BEZUG
ISO/IEC 27001:2022 (A.5.7, A.8.1, A.8.2, A.8.16, A.5.21) · DORA Art. 9, 25, 26, 28 · NIS2 Art. 21 · MiCA

KLASSIFIZIERUNG
TLP:CLEAR, Weitergabe erlaubt

STAND
1. November 2026, Version 1.0. Binance hat einen technischen Abschlussbericht angekündigt; dieses Advisory wird danach aktualisiert.

QUELLEN
TRM Labs, Elliptic, Bitquery, Binance (Richard Teng, Yi He), FBI, CISA, US-Finanzministerium, Mandiant, Unit 42, Google GTIG, Sygnia, Safe, xorl, UN-Expertengremium

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

INHALT

1 20:05 Uhr 4
2 Der Riese 6
3 Zurück an den Anfang: ein Papier aus Washington 7
4 Ein Raub in sieben Akten 9
5 Die Chronik: Seit April 2022 ging jedem Opfer eine Warnung voraus 11
6 Der Befund: zertifiziert, geprüft, ausgeräumt 14
7 Die Rechnung: wer zahlt, wer kassiert 15
8 Das Plädoyer: Wer seine Angreifer nicht kennt, verteidigt ins Leere 16
9 Was jetzt zu tun ist: acht Maßnahmen 17
10 Zehn Fragen für das nächste Audit 18
A Anhang: Techniken, Quellen, Vorbehalte 19

Methodik und Vorbehalte zur Faktenlage (Stand 1. November 2026)

Der Einstieg über den DevOps-Laptop stammt bisher allein von Binance; ein technischer Abschlussbericht ist angekündigt. Die Einschätzung zur Signaturinfrastruktur ist eine Bewertung von TRM Labs. Die Attribution zu TraderTraitor trifft TRM mit hoher Konfidenz, das FBI bestätigt nordkoreanische Akteure; die Verbindung zu Bitget, die das Analysehaus BitOK zieht, ist eine analytische Zuordnung, keine bewiesene Identität. Drift wird von Drift und SEAL 911 dem Cluster UNC4736 zugeordnet, nicht TraderTraitor; die Nordkorea-Zuordnung von Bitget ist unbestätigt. Die Zertifizierungsangaben beruhen auf Binance-Pressemitteilungen von 2019 und 2023; ob sie 2026 gültig sind und die Wallet-Infrastruktur umfassen, ist nicht veröffentlicht. Alle Schadenssummen sind Bewertungen zum Zeitpunkt des Abflusses.

Lesehinweis

Die Kapitel 1 bis 8 erzählen den Fall, von der Nacht des Angriffs über den Akteur und seine Angriffskette bis zur Rechnung. Wer wenig Zeit hat, liest das Kapitel „Auf einen Blick“, Kapitel 6 (der Befund) und die Kapitel 9 und 10 (Maßnahmen und Prüffragen). Alle Uhrzeiten in Weltzeit (UTC), Frankfurt liegt eine Stunde voraus. Schadenssummen in US-Dollar zum Zeitpunkt des Abflusses.

KAPITEL 1 · DIE NACHT

20:05 Uhr

Der Angriff beginnt einen Tag vor dem Diebstahl. Am 28. Oktober richtet der Angreifer eine Wallet ein und schickt ihr über einen Dienst, der die Herkunft von Geld verschleiert, rund einen Ether, gut 2.000 Dollar. Das reicht für Transaktionsgebühren. Am 29. Oktober testet er seinen Angriffscode an fremden Wallets. Vier Stunden nach dem letzten Test läuft der Code gegen eine Hot Wallet von Binance, eine Wallet, die ständig am Netz hängt, weil die Börse daraus Kundenauszahlungen bedient.

Um 20:05 Uhr Weltzeit, 21:05 Uhr in Frankfurt, beginnt der Abfluss, zuerst auf dem XRP Ledger. Alle weiteren Zeiten in Weltzeit. Binnen 20 Minuten folgen Solana, Optimism, Bitcoin und Tron, dann Ethereum, wo das meiste Geld liegt. Dort hat sich der Angreifer vorab 50 Signaturen der Binance-Wallet beschafft. Eine davon genügt, um die Wallet unter seine Kontrolle zu bringen. Drei Minuten später ist sie leer: 167.464 Ether und 1,6 Milliarden Tether in einer einzigen Transaktion. Bis Mitternacht kommt er sechsmal zurück und räumt ab, was Kunden inzwischen eingezahlt haben. Zehn Blockchains, ein Angreifer, eine halbe Stunde für das Wesentliche.

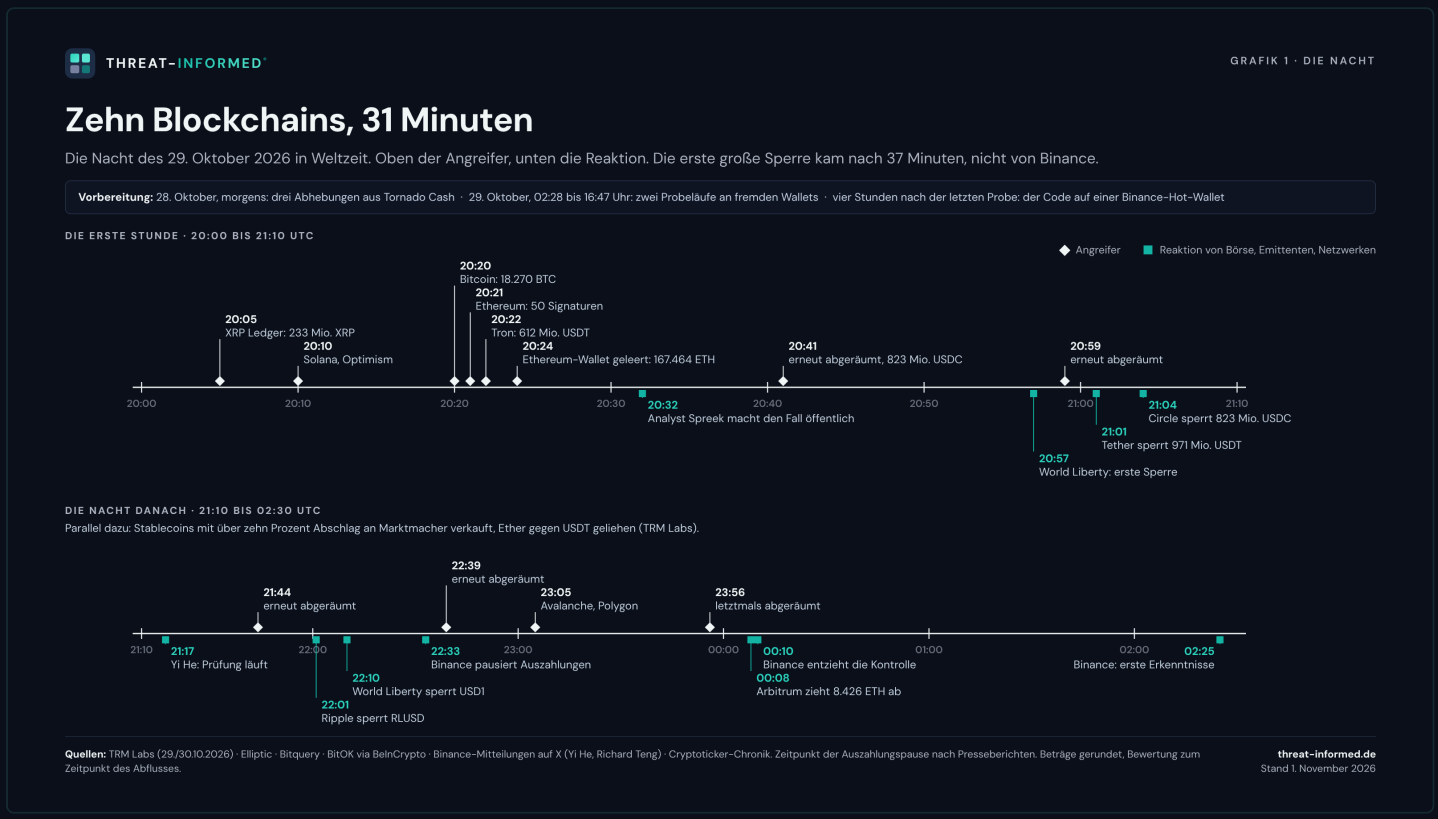
Gebremst wird der Angreifer nicht von Binance, sondern von den Firmen, die Stablecoins wie Tether und USD Coin herausgeben. Sie können ihre Token per Knopfdruck sperren. Tether sperrt um 21:01 Uhr 971 Millionen Dollar, 37 Minuten nach dem großen Abfluss, Circle drei Minuten später 823 Millionen. Der Angreifer sieht die Sperren kommen und verkauft, was sich noch verkaufen lässt, mit mehr als zehn Prozent Abschlag. Binance hält Auszahlungen gegen 22:33 Uhr an und meldet um 02:25 Uhr erste Erkenntnisse.

Am Morgen sind 6,36 Milliarden Dollar weg. 2,7 Milliarden davon liegen eingefroren auf Adressen des Angreifers, 2,4 Milliarden in Ether und Bitcoin außer Reichweite. Eine Frage bleibt: Wie bringt jemand Binance-Wallets auf zehn Blockchains dazu, seine Transaktionen zu unterschreiben?

Binance antwortet am Tag danach, vorsichtig. Der Vorfall habe möglicherweise mit dem Laptop eines DevOps-Engineers begonnen, also eines Technikers, der die Systeme der Börse betreibt. Über diesen Laptop sei der Angreifer in ein internes System gelangt und habe von dort Auszahlungen ausgelöst. Es sei kein Angriff mit einem Klick gewesen, es gebe weitere Einfallstore, und private Schlüssel seien nicht abgeflossen. TRM Labs geht einen Schritt weiter: Der Angreifer habe wahrscheinlich das System unter Kontrolle gebracht, mit dem Binance seine Auszahlungen signiert.

> **Ein Laptop. Wer diesen Satz verstanden hat, kennt den Rest der Geschichte. Dieser Angriffsweg stand seit viereinhalb Jahren in einem Papier.**

Zehn Blockchains, ein Angreifer, eine halbe Stunde für das Wesentliche.



Grafik 1 Die Nacht des 29. Oktober 2026 in Weltzeit, oben der Angreifer, unten die Reaktion. Die erste große Sperre kam nach 37 Minuten, nicht von Binance.

KAPITEL 2 · BINANCE

Der Riese

Binance wurde 2017 gegründet und ist seither die größte Kryptobörse der Welt. Anfang 2026 verwahrte die Börse Reserven von rund 155 Milliarden Dollar und setzte in einem Monat 2,1 Billionen Dollar um, das 2,6-Fache des nächsten Wettbewerbers. Je nach Zählung läuft ein Viertel bis knapp 40 Prozent des weltweiten Spot-Handels über Binance. Dort entsteht der Preis für Bitcoin. Wankt Binance, wankt der Markt: Nach dem Angriff verlor Bitcoin binnen Stunden fünf Prozent, die Aktien von Coinbase und Robinhood gaben nach. Binance ist für Krypto, was ein systemrelevantes Institut für den Geldmarkt ist, nur ohne Einlagensicherung, ohne veröffentlichte Bilanz und lange ohne Hauptsitz.

Die Zweifel sind fast so alt wie die Börse. 2019 verlor die Börse 7.074 Bitcoin aus einer Hot Wallet, weil Angreifer mit Phishing Zugangsdaten von Nutzern gesammelt hatten; die Alarme kamen, als das Geld weg war. 2022 wurde die Brücke der hauseigenen BNB Chain um 570 Millionen Dollar erleichtert. Dazu kam die Konzernstruktur: Dutzende Gesellschaften, keine geprüften Abschlüsse. Ein Reservenachweis des Prüfers Mazars Ende 2022 hielt nur Tage, dann zog sich Mazars aus dem Kryptogeschäft zurück. 2023 warf die US-Börsenaufsicht Binance vor, Kundengelder in Milliardenhöhe vermischt zu haben. Im November 2023 bekannten sich Binance und Gründer Changpeng Zhao schuldig, kein wirksames Geldwäscheprogramm betrieben zu haben: 4,3 Milliarden Dollar Strafe, ein Compliance-Monitor im Haus, vier Monate Haft für Zhao. Präsident Trump begnadigte ihn 2025, Zhao blieb größter Anteilseigner. Seither führen Richard Teng, ein früherer Finanzaufseher, und Mitgründerin Yi He das Geschäft.

In Europa gilt seit Ende 2024 die MiCA-Verordnung mit Lizenzpflicht. Binance bekam keine Lizenz, zog seinen Antrag zurück und stellte das Angebot für EU-Kunden im Juli 2026 weitgehend ein. Teng kritisierte daraufhin Brüssel: 70 Prozent der betroffenen Nutzer hätten ihr Geld in eigene Wallets verschoben, und dort sei das Risiko höher. Man sollte sich den Satz merken.

Dabei ist Binance auf dem Papier ein Musterschüler. Seit 2019 ist die Börse nach ISO 27001 zertifiziert, als eine der ersten Kryptoplattformen überhaupt. 2023 kamen Zertifikate für Frankreich, die Emirate, Bahrain und die Türkei hinzu sowie ein SOC-2-Bericht für die globale Plattform. Der damalige Sicherheitschef sprach von nachgewiesenen wirksamen Kontrollen. Ob die Zertifikate 2026 noch gelten und die Wallet-Systeme abdecken, hat Binance nicht veröffentlicht. Für diesen Text spielt das keine Rolle. Es geht nicht darum, ob ein Zertifikat fehlte, sondern darum, was ein Zertifikat beweist. Die Aufsichtsregeln, die Binance umgeben, handeln von Geldwäsche, Kundenvermögen und Transparenz. Keine davon fragt, wie man den Laptop eines Technikers gegen einen Angreifer schützt, der sich als Recruiter ausgibt.

KAPITEL 3 · DER AKTEUR

Zurück an den Anfang: ein Papier aus Washington

Wer es war, gilt als geklärt. TRM Labs schreibt den Angriff mit hoher Sicherheit der nordkoreanischen Gruppe TraderTraitor zu, das FBI bestätigt nordkoreanische Täter. Um diese Gruppe zu verstehen, muss man zurück ins Frühjahr 2022.

Am 18. April 2022 veröffentlichen das FBI, die Cybersicherheitsbehörde CISA und das US-Finanzministerium ein gemeinsames Papier, 14 Seiten, für jedermann lesbar. Es beschreibt eine nordkoreanische Kampagne gegen Kryptofirmen und gibt ihr den Namen TraderTraitor. Der Einstieg, so das Papier: Mitarbeiter von Kryptofirmen, oft Systemadministratoren und DevOps-Techniker, bekommen über Jobportale und Messenger hoch bezahlte Stellen angeboten und sollen dafür eine Software installieren, die den Rechner übernimmt. Das Papier listet die Namen der Programme, die Prüfsummen der Dateien und die Adressen der Server. Man kann es bis heute herunterladen.

Die Gruppe hat seither viele Namen bekommen: UNC4899 bei Google und Mandiant, Jade Sleet bei Microsoft, Slow Pisces bei Palo Alto Networks. Mandiant ordnet sie dem Reconnaissance General Bureau zu, dem nordkoreanischen Auslandsgeheimdienst. Ihr Ziel ist nicht Spionage, sondern Devisen.

Wo sie im Staat sitzt, lässt sich aus öffentlichen Quellen rekonstruieren; Grafik 2 zeigt das Ergebnis. Der Sicherheitsforscher xorl pflegt seit 2021 eine Karte der nordkoreanischen Cyber-Einheiten, aufgebaut auf Mandiants Analysen, US-Anklageschriften und Überläuferberichten. Demnach läuft die Befehlskette von Kim Jong Un über den Generalstab zum Geheimdienst, dort zum 3. Büro und weiter zum Lab 110, dem Kern dessen, was die Welt „Lazarus“ nennt. TraderTraitor ist die auf Kryptowerte spezialisierte Linie in diesem Geflecht. Das US-Finanzministerium hat Lazarus 2019 genau dort verortet: im 110. Forschungszentrum des 3. Büros.

Diese Organisation ist kein Phantom. Sie hat Büronummern, Tarnfirmen in China, namentlich angeklagte Mitarbeiter und einen Auftrag. Das UN-Expertengremium schätzte 2024, dass Nordkorea seit 2017 mehr als drei Milliarden Dollar in Kryptowerten gestohlen hat; ein Nachfolgegremium beziffert den Anteil der Cyberbeute an den Deviseneinnahmen des Landes für 2024 auf rund ein Drittel. Das Geld fließt nach Einschätzung von UN und US-Regierung in das Raketen- und Nuklearprogramm. Wer Binance ausräumt, finanziert Sprengköpfe.

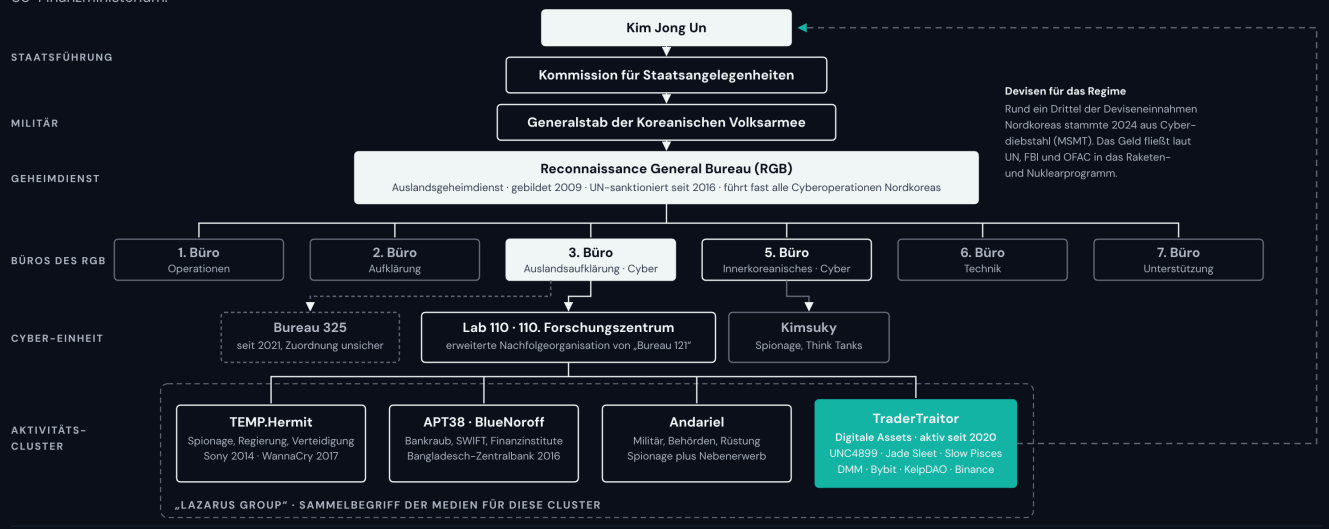
Wer Binance ausräumt, finanziert Sprengköpfe.

THREAT-INFORMED®

GRAFIK 2 · DER AKTEUR

Kein Phantom: Wo TraderTraitor im Staat sitzt

Die Befehlskette vom Obersten Führer bis zur Einheit, die Binance ausgeräumt hat. Rekonstruiert nach xorl (v2.2, 2023), Mandiant (2022, 2023) und dem US-Finanzministerium.



Quellen: xorl, North Korea (DPRK) Cyber Operations Groups, v2.2 (10/2023) · Mandiant, Not So Lazarus (03/2022) und Assessed Cyber Structure of North Korea (2023) · US-Finanzministerium, OFAC-Designation Lazarus (2019): „subordinate to the 110th Research Center, 3rd Bureau of the RGB" · FBI/CISA/Treasury AA22-108A (2022) · CCDCOE, The All-Purpose Sword (2019) · HRNK, The Reconnaissance General Bureau (2026).
Ein 4. Büro gibt es nicht; die Vier gilt in Korea als Unglückszahl. Außerhalb des RGB operieren das Ministerium für Staatssicherheit (APT37), die Einheitsfrontabteilung (Propaganda) und die IT-Worker-Programme. Mandiant beschreibt seit 2023 eine Verwischung der Einheiten mit geteilten Werkzeugen und Zielen. Konfidenz: auf Clusterebene hoch (FBI, Mandiant), auf Büroebene mittel (Überläufer, OSINT).

threat-informed.de
Stand 1. November 2026

Grafik 2 Kein Phantom: Wo TraderTraitor im nordkoreanischen Staatsapparat sitzt, rekonstruiert nach xorl, Mandiant und US-Finanzministerium.

KAPITEL 4 · DIE ANGRIFFSKETTE

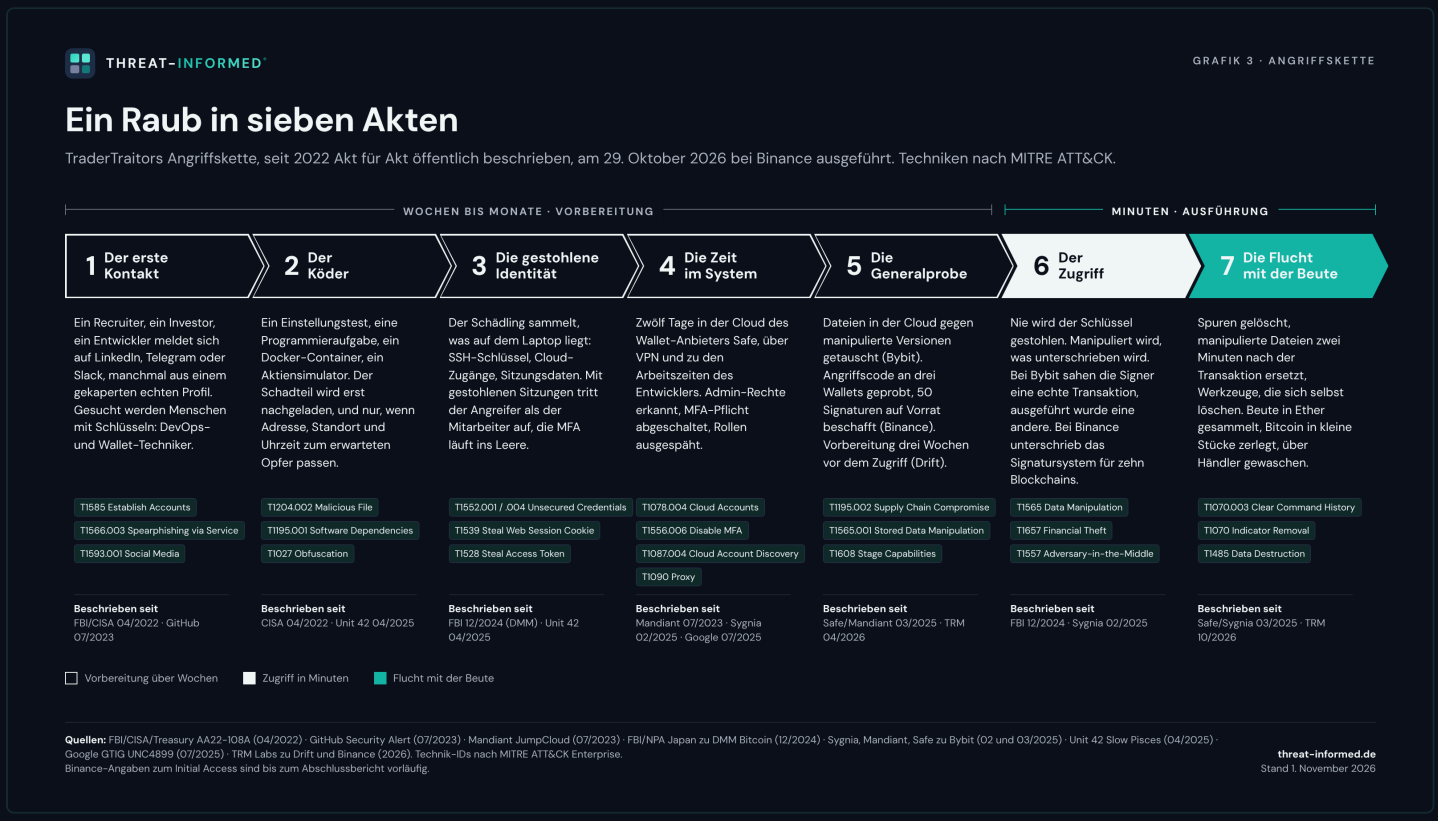
Ein Raub in sieben Akten

Das Papier von 2022 beschreibt den ersten Akt. Die übrigen sechs hat die Gruppe seither vor aller Augen aufgeführt. Jeder ist dokumentiert. Grafik 3 ordnet ihm die Nummern aus MITRE ATT&CK zu, dem Technikkatalog der Branche.

1. **Der erste Kontakt.** Ein Recruiter, ein Investor oder ein Entwickler meldet sich auf LinkedIn, Telegram oder Slack. Gesucht werden Menschen mit Schlüsseln: DevOps- und Wallet-Techniker.
2. **Der Köder.** Ein Einstellungstest, eine Programmieraufgabe, ein Docker-Container. Der Code wirkt harmlos, weil der Schadteil erst nachgeladen wird, und das nur beim richtigen Opfer.
3. **Die gestohlene Identität.** Der Schädling sammelt, was auf dem Laptop liegt: SSH-Schlüssel, Cloud-Zugänge, Sitzungsdaten. Mit gestohlenen Sitzungen läuft die Mehrfaktor-Authentifizierung ins Leere, der Angreifer tritt als der Mitarbeiter auf.
4. **Die Zeit im System.** Bei Bybit bewegten sich die Angreifer zwölf Tage in der Cloud des Wallet-Anbieters Safe, zu den Arbeitszeiten des Entwicklers, dessen Identität sie trugen.
5. **Die Generalprobe.** Dateien ausgetauscht, Code getestet, Signaturen auf Vorrat beschafft. Bei Drift begann die technische Vorbereitung drei Wochen vor dem Zugriff.
6. **Der Zugriff.** Nie wird der Schlüssel der Wallet gestohlen. Manipuliert wird, was unterschrieben wird. Der Abfluss dauert 12 Minuten (Drift), 20 (Bitget) oder 31 (Binance).
7. **Die Flucht mit der Beute.** Spuren werden verwischt, die Werkzeuge löschen sich selbst. Die Beute wird in Ether gesammelt und über Händler gewaschen.

Vier Dinge machen dieses Stück so erfolgreich, und keines ist eine Softwarelücke: ein Mensch mit privilegiertem Zugang; eine Mehrfaktor-Authentifizierung, die gestohlene Sitzungen nicht erkennt; Dienstleister als Einstieg; Geduld, die in einem einzigen Schlag endet.

Vier Dinge machen dieses Stück so erfolgreich, und keines ist eine Softwarelücke.



Grafik 3 Ein Raub in sieben Akten: die Angriffskette von TraderTraitor mit den Techniknummern aus MITRE ATT&CK und dem Jahr, seit dem jeder Akt öffentlich beschrieben ist.

KAPITEL 5 · WARNUNGEN UND OPFER

Die Chronik: Seit April 2022 ging jedem Opfer eine Warnung voraus

Nichts davon war geheim. Die Warnkette beginnt im April 2022 und wird mit jedem Jahr präziser.

Tabelle 1 Öffentliche Berichte zum Vorgehen von TraderTraitor

DATUM	HERAUSGEBER	WAS DOKUMENTIERT WURDE
April 2022	**FBI, CISA, US-Finanzministerium (AA22-108A)**	Spearphishing an Mitarbeiter von Kryptofirmen, oft in Systemadministration oder DevOps, getarnt als Recruiting mit hoch bezahlten Jobs; Schadcode in gefälschten Krypto-Apps
Juni und Juli 2023	**Phylum, GitHub**	Falsche Entwickler- und Recruiter-Profile auf GitHub, LinkedIn, Slack und Telegram; Einladung zur Zusammenarbeit an Repositories mit bösartigen npm-Abhängigkeiten, getarnt als Mediaplayer oder Trading-Tools
Juli 2023	**Mandiant**	Einstieg über den Identity-Provider JumpCloud, Ausführung eines Ruby-Skripts über dessen Agent bei Kunden aus der Kryptobranche; Attribution zu UNC4899 nach einem Fehler bei der Tarnung, der eine nordkoreanische IP-Adresse preisgab
August und September 2023	**FBI**	Alphapo, CoinsPaid, Atomic Wallet, Stake; Aufforderung an die Branche, die TraderTraitor-Warnung zu lesen
Dezember 2024	**FBI, DC3, japanische Polizei**	DMM Bitcoin: LinkedIn-Recruiter, Python-Skript als Einstellungstest auf GitHub, gestohlene Session-Cookies, manipulierte Transaktionsanfrage
Februar und März 2025	**FBI, Sygnia, Mandiant, Safe**	Bybit: kompromittierter Entwickler-Mac, AWS-Session-Tokens gegen MFA, zwölf Tage Erkundung, manipulierte JavaScript-Ressourcen
April 2025	**Palo Alto Networks Unit 42**	Coding-Challenge-Kampagne bis auf Hash-Ebene: PDF-Stellenbeschreibung, Fragebogen, Schadcode nur für ausgewählte Opfer, YAML-Deserialisierung, RN Loader und RN Stealer
Juli 2025	**Google Threat Intelligence Group**	Freelance-Lockangebote über LinkedIn und Telegram, bösartige Docker-Container, Abschaltung der MFA-Pflicht in Google Cloud, ausgetauschte JavaScript-Dateien

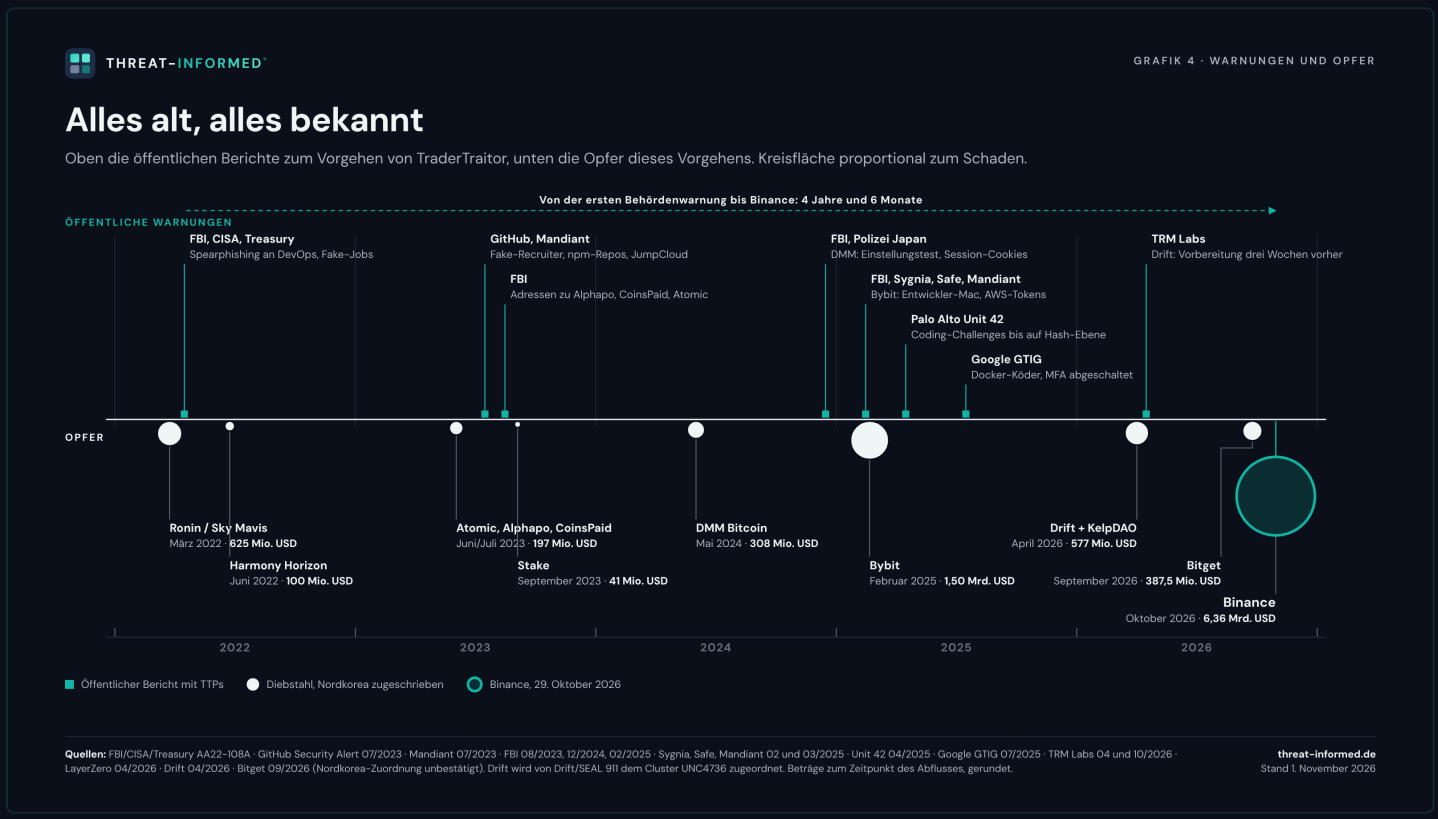
Im März 2024 schrieb ein angeblicher Recruiter einen Mitarbeiter der japanischen Wallet-Firma Ginco an und schickte ihm einen Einstellungstest auf GitHub. Zwei Monate später manipulierten die Angreifer mit seinen Sitzungsdaten eine Transaktion des Kunden DMM Bitcoin: 308 Millionen Dollar. Im Februar 2025 startete ein Entwickler der Wallet-Firma Safe ein Docker-Projekt, das sich als Aktiensimulator ausgab. Zwölf Tage später war Bybit um 1,5 Milliarden Dollar ärmer. Im April 2026 folgten Drift und KelpDAO, im September Bitget. Und im Oktober Binance, mehr als vier Jahre nachdem das FBI DevOps-Techniker von Kryptofirmen als bevorzugtes Ziel benannt hatte. Unit 42 hatte im April 2025 festgehalten, das Vorgehen der Gruppe sei über Monate gleich geblieben. Warum auch etwas ändern? Es funktionierte.

Tabelle 2 Die Opfer, Schaden in US-Dollar zum Zeitpunkt des Abflusses

DATUM	OPFER	SCHADEN	EINSTIEG	ATTRIBUTION
März 2022	**Ronin / Sky Mavis**	**625 Mio.**	Social Engineering	FBI: Lazarus, APT38
Juni und Juli 2023	**Atomic Wallet, Alphapo, CoinsPaid**	**197 Mio.**	CoinsPaid: Mitarbeiter lud per Phishing Software mit Malware	FBI: TraderTraitor
Juni 2023	**JumpCloud-Kunden**	**kein Diebstahl nachgewiesen**	Identity-Provider als Lieferkette	Mandiant: UNC4899
Mai 2024	**DMM Bitcoin über Ginco**	**308 Mio.**	LinkedIn-Recruiter, Einstellungstest auf GitHub, Session-Cookies	FBI, japanische Polizei
Februar 2025	**Bybit über Safe{Wallet}**	**1,5 Mrd.**	Entwickler-Mac, AWS-Session-Tokens, manipulierte Signer-Oberfläche	FBI
April 2026	**Drift Protocol**	**285 Mio.**	Sechs Monate Social Engineering als Trading-Firma, persönliche Treffen auf Konferenzen, vorab signierte Transaktionen	Drift, SEAL 911: Nordkorea (Cluster UNC4736)
April 2026	**KelpDAO über LayerZero**	**292 Mio.**	Kompromittierte Verifier-Nodes, 1-of-1-Konfiguration	LayerZero: TraderTraitor
September 2026	**Bitget**	**387,5 Mio.**	Backend-Wallet-System, Signaturlogik unterlaufen, Drittanbieter-Sicherheitsprodukt	unbestätigt; Geldflüsse überlappen mit Binance
Oktober 2026	**Binance**	**6,36 Mrd.**	DevOps-Laptop, Service-Container, Signaturinfrastruktur	TRM Labs: TraderTraitor; FBI: Nordkorea

> **Seit April 2022 ging jedem Opfer ein Bericht voraus, der den Einstieg beschrieb, mit dem es wenig später getroffen wurde. Das ist keine Geschichte über Sicherheitslücken. Es ist eine Geschichte darüber, was nach dem Lesen kommt.**

Seit April 2022 ging jedem Opfer ein Bericht voraus.



Grafik 4 Alles alt, alles bekannt: öffentliche Warnungen und Opfer 2022 bis 2026 auf einer Zeitachse, Kreisfläche proportional zum Schaden.

KAPITEL 6 · DER BEFUND

Der Befund: zertifiziert, geprüft, ausgeräumt

Ich prüfe seit Jahren als Lead Auditor Managementsysteme für Informationssicherheit und habe selbst vier aufgebaut. Ein Zertifikat nach ISO 27001 beweist, dass eine Organisation ein solches System betreibt: Risiken bewertet, Maßnahmen umgesetzt, intern geprüft. Der Auditor sieht das in Stichproben, ein paar Tage im Jahr. Die Norm verlangt sogar ausdrücklich Threat Intelligence, also das Auswerten von Informationen über Angreifer. Der Auditor prüft, ob dieser Prozess existiert. Ob der Laptop eines Technikers einem falschen Recruiter standhält, prüft er nicht. Das passt in kein Auditprogramm.

Binance hatte Threat Intelligence. Die Börse spürt seit Jahren nordkoreanische Beute auf und beschäftigt eines der größten Sicherheitsteams der Branche. Das Wissen war da. Es wurde nicht in Architektur und Erkennung übersetzt. Das ist der Unterschied zwischen Threat Intelligence und Threat-Informed Defense, und er lässt sich an dieser Nacht belegen.

Die Architektur: Wer das Signatursystem für Wallets auf zehn Blockchains binnen einer halben Stunde zu Unterschriften bringt, stößt auf keine Grenze. Nichts hat eine Wallet angehalten, die in drei Minuten mehr auszahlte als sonst in Wochen. 6,36 Milliarden Dollar in 31 Minuten sind nicht nur ein Erkennungsproblem. Sie sind eine Architekturentscheidung.

Die Erkennung: Dieser Angriff hat sich angekündigt. Eine frisch finanzierte Wallet, Probeläufe am Tattag, dann 15 Minuten zwischen dem ersten Abfluss und dem Zugriff auf Ethereum, dann 37 Minuten bis zur ersten großen Sperre durch Tether. Wer nach dem Verhalten des Angreifers sucht, hat an diesem Abend Stunden Vorlauf. Wer nur den Kontrollkatalog abarbeitet, sieht erst den Abfluss. Entdeckt wurde der Angriff nicht von der eigenen Erkennung, sondern von außen. Das Muster kennt man aus Deutschland: Im Berliner Landesnetz blieb ein Datenabfluss fünf Tage unbemerkt. Auch dort kam die Entdeckung von außen.

Der Mensch: Der Laptop eines Technikers mit Zugang zu Auszahlungssystemen ist kein Bürorechner. Er ist so schützenswert wie der zentrale Verzeichnisdienst einer Firma. Auf einem solchen Gerät wird kein Code aus einem Recruiter-Repository ausgeführt. Diese Regel steht in keinem Zertifikat. Sie steht in den Berichten über DMM Bitcoin und Bybit.

Und das Zertifikat selbst: Es ist nicht wertlos. Es beweist, dass Binance ein Managementsystem betreibt. Es beweist nichts über die Frage, die an diesem Abend entschied: ob eine Organisation ihren Gegner kennt und ihre Verteidigung gegen dessen Techniken gebaut und geprüft hat. Zertifikate messen, ob Prozesse vorhanden sind. Angreifer messen, ob sie wirken. Binance hat beide Messungen bekommen. Die erste hat es 2019 bestanden. Die zweite dauerte 31 Minuten.

> **Zertifikate messen, ob Prozesse vorhanden sind. Angreifer messen, ob sie wirken.**

KAPITEL 7 · DIE RECHNUNG

Die Rechnung: wer zahlt, wer kassiert

Den Schaden trägt Binance, nicht die Kunden. Richard Teng erklärte am Tag danach, man habe 6,34 Milliarden Dollar an Firmenmitteln reserviert. Am 31. Oktober meldete die Börse, 90 Prozent der gestohlenen Bestände seien ersetzt, aus drei Töpfen: dem Notfallfonds SAFU, einem Versicherungsfonds für den Terminhandel und der Konzernkasse. Auszahlungen laufen gestaffelt wieder an, ein neuer Reservenachweis ist angekündigt.

Prüfen kann das niemand von außen; Binance veröffentlicht keine Bilanz. Teng sagt, der Konzern halte seine Gewinne in Kryptowerten und könne den Schlag absorbieren. Das ist bei zwei Billionen Dollar Handelsvolumen im Monat plausibel. Die Frage, ob hier die größte Pleite der Kryptogeschichte droht, kommt deshalb zu früh. FTX fiel 2022 nicht an einem Hack, sondern daran, dass Kundengelder verspielt waren. Binance beteuert, Kundengelder lägen unberührt in Cold Wallets, die nicht am Netz hängen. Der Test kommt, wenn alle Auszahlungen wieder offen sind.

Eingefroren ist nicht zurück. Die 2,7 Milliarden Dollar, die Tether, Circle, Ripple und andere gesperrt haben, liegen auf Adressen des Angreifers fest; ihre Rückführung braucht Gerichte und Zeit. Bemerkenswert ist, wer gehandelt hat: keine Aufsicht, nicht die Börse, sondern private Firmen, die ihre Token per Knopfdruck sperren können. Die Kryptowelt, die Zensurfreiheit als Gründungsmythos pflegt, wurde von genau den zentralen Eingriffen, die sie ablehnt, vor dem Schlimmsten bewahrt.

Die 2,4 Milliarden Dollar außer Reichweite sind mehr als jeder einzelne frühere Kryptoraub. Sie wandern über Brücken, Tauschdienste und Händler Richtung Pjöngjang, wie die Beute aus Bybit, Drift, KelpDAO und Bitget. Mit 6,36 Milliarden Dollar hat ein Staat unter umfassenden Sanktionen in einer Nacht mehr erbeutet, als das UN-Gremium ihm für sechs Jahre insgesamt zurechnete. Ohne eine einzige Sicherheitslücke in einer Software auszunutzen.

Und die Regulierung? Binance hat Europa im Juli verlassen, EU-Kunden waren deshalb kaum betroffen. Tengs Satz vom Juli klingt seither anders: Das höhere Risiko lag diesmal nicht in den Wallets der Kunden, sondern in einer Hot Wallet der Börse. Fachleute sagten CNBC, auch die US-Aufsicht hätte diesen Vorfall nicht verhindert, weil er mit einem Laptop begann. Regeln zu Geldwäsche, Kundenvermögen und Transparenz erzeugen Prüfberichte. Widerstandsfähigkeit erzeugen sie nicht.

KAPITEL 8 · DAS PLÄDOYER

Das Plädoyer: Wer seine Angreifer nicht kennt, verteidigt ins Leere

Auf jeden großen Vorfall folgt der Ruf nach mehr Regeln, mehr Zertifikaten, mehr Nachweisen. Der Fall Binance widerlegt diesen Reflex. Binance war zertifiziert, geprüft und beaufsichtigt. Der Täter war namentlich bekannt, seine Techniken katalogisiert. Nichts davon spielte in den 31 Minuten eine Rolle, in denen es darauf ankam. Compliance stoppt keine Angreifer.

Der Fehler liegt in der Reihenfolge. Wer mit dem Kontrollkatalog beginnt, verteidigt sich gegen die Norm. Wer mit dem Angreifer beginnt, verteidigt sich gegen den Angreifer und erfüllt die Norm nebenbei. Threat-Informed Defense beantwortet drei Fragen: Wer greift uns an? Wie erkennen wir ihn? Was tun wir, damit er scheitert? Binance konnte die erste beantworten. An den beiden anderen ist es gescheitert, wie Bybit, DMM, Drift, KelpDAO und Bitget vor ihm.

Was das verlangt, steht in diesem Fall:

- **Den Gegner benennen.** Nicht „Cyberkriminelle“, sondern TraderTraitor, mit den Berichten von CISA, GitHub, Mandiant, FBI und Unit 42 auf dem Tisch.
- **Die eigene Verteidigung gegen seine Techniken messen.** Die sieben Akte sind ein Prüfprogramm: Was würden wir erkennen, was stoppen, wo wären wir blind?
- **Techniker mit privilegiertem Zugang schützen wie Kronjuwelen.** Gehärtete Geräte, kein fremder Code, kurze Cloud-Sitzungen. Ein falscher Recruiter muss am Gerät scheitern, nicht an der Wachsamkeit des Mitarbeiters.
- **Die Unterschrift vom Bildschirm trennen.** Was signiert wird, wird auf einem Gerät geprüft, das der Angreifer nicht kontrolliert.
- **Den Auszahlungspfad begrenzen.** Limits und Notbremsen. Eine Wallet, die in drei Minuten Milliarden abgibt, ist ein Konstruktionsfehler.
- **Nach dem Verhalten des Angreifers suchen.** Frisch finanzierte Wallets, Testtransaktionen, Signaturen auf Vorrat: alles Stunden vorher sichtbar.
- **Die Lieferkette mitdenken.** Ginco, Safe, LayerZero, JumpCloud: Jeder zweite Einstieg lag beim Dienstleister.
- **Üben.** Gegen die dokumentierte Kette dieses Gegners, nicht gegen einen Phishing-Simulator.

Die Lehre reicht über Krypto hinaus. Dieselben Techniker, Signatursysteme und Cloud-Sitzungen gibt es in jeder Bank und jeder Versicherung. Der Unterschied liegt nicht in der Zahl der Regeln, sondern darin, was sie prüfen: Vorhandensein oder Wirkung. Die europäische Finanzaufsicht hat das verstanden: DORA verlangt von großen Finanzunternehmen Tests, bei denen die Techniken realer Angreifer gegen die eigene Organisation nachgestellt werden. Das ist Threat-Informed Defense mit Gesetzeskraft.

Binance wusste, wer kommt. Es wusste, wie. Es war zertifiziert. Und es verlor in einer Nacht 6,36 Milliarden Dollar an einen Gegner, vor dem das FBI viereinhalb Jahre zuvor gewarnt hatte. Das Zertifikat hat Binance noch. Das Geld hat Nordkorea.

KAPITEL 9 · HANDLUNGSEMPFEHLUNGEN

Was jetzt zu tun ist: acht Maßnahmen

Die acht Punkte aus Kapitel 8, übersetzt in Maßnahmen für Organisationen außerhalb der Kryptobranche. Jede Maßnahme trägt den Bezug zu ISO/IEC 27001:2022 und, wo einschlägig, zu DORA und NIS2, damit sie im Managementsystem andocken kann. Die Reihenfolge ist die Reihenfolge der Wirkung: Erst den Gegner kennen, dann die eigene Verteidigung gegen ihn messen, dann bauen und üben.

1

Den Gegner benennen

Nicht „Cyberkriminelle", sondern TraderTraitor, Lazarus, die für die eigene Branche relevanten Cluster. Die Berichte von CISA, FBI, Mandiant, Unit 42 und GTIG gehören auf den Tisch des Sicherheitsteams, nicht in den Posteingang.

ISO 27001:2022 A.5.7 · NIS2 Art. 21 Abs. 2

2

Die Verteidigung gegen seine Techniken messen

Die sieben Akte sind ein Prüfprogramm: Welche Technik würden wir erkennen, welche stoppen, wo sind wir blind? Ergebnis als Abdeckung gegen MITRE ATT&CK festhalten, Lücken priorisieren.

ISO 27001:2022 A.5.35, A.8.8 · DORA Art. 25, 26

3

Techniker mit privilegiertem Zugang schützen wie Kronjuwelen

Gehärtete, verwaltete Geräte für alle mit Zugang zu Auszahlungs-, Signatur- und Produktionssystemen. Kein fremder Code aus Repositories oder Einstellungstests auf diesen Geräten. Kurze Cloud-Sitzungen, Token an das Gerät gebunden.

ISO 27001:2022 A.8.1, A.8.2, A.8.19

4

Die Unterschrift vom Bildschirm trennen

Was signiert oder freigegeben wird, wird auf einem Gerät geprüft, das der Angreifer nicht kontrolliert. Für Wallets: Hardware-Signer mit lesbarer Anzeige der Transaktion. Für Banken: dasselbe Prinzip bei Zahlungsfreigaben und Admin-Änderungen.

ISO 27001:2022 A.8.24, A.8.26

5

Den Auszahlungspfad begrenzen

Limits, Verzögerungen und Notbremsen, die technisch erzwungen sind und nicht nur dokumentiert. Eine Wallet, die in drei Minuten Milliarden abgibt, ist ein Konstruktionsfehler, kein Erkennungsfehler.

ISO 27001:2022 A.5.3, A.8.26 · DORA Art. 9

6

Nach dem Verhalten des Angreifers suchen

Frisch finanzierte Wallets, Testtransaktionen an fremden Zielen, Signaturen auf Vorrat, abgeschaltete MFA-Pflichten, ausgetauschte Dateien: alles Stunden bis Tage vorher sichtbar. Erkennung auf die Vorbereitung ausrichten, nicht auf den Abfluss.

ISO 27001:2022 A.8.15, A.8.16

7

Die Lieferkette mitdenken

Ginco, Safe, LayerZero, JumpCloud: Jeder zweite Einstieg lag beim Dienstleister. Identitätsanbieter, Wallet-Software und Signaturdienste gehören in dieselbe Bedrohungsanalyse wie die eigenen Systeme.

ISO 27001:2022 A.5.19, A.5.21, A.5.23 · DORA Art. 28

8

Üben

Gegen die dokumentierte Kette dieses Gegners, nicht gegen einen Phishing-Simulator. Der falsche Recruiter, der Docker-Container, die gestohlene Sitzung: nachstellen, messen, nachbessern.

ISO 27001:2022 A.5.24, A.5.26 · DORA Art. 26 (TLPT)

KAPITEL 10 · PRÜFFRAGEN

Zehn Fragen für das nächste Audit

Jede Frage ist im Fall Binance mit Nein beantwortet worden, auf die eine oder andere Weise. Sie eignen sich für das interne Audit, das Managementreview und das Gespräch zwischen Vorstand und CISO. Entscheidend ist nicht die Antwort, sondern der Beleg dafür.

Keine der Maßnahmen aus Kapitel 9 ersetzt eine Anforderung der Norm. Sie beantworten die Frage, die die Norm offen lässt: ob die vorhandenen Kontrollen gegen einen konkreten, dokumentierten Gegner wirken. A.5.7 verlangt Threat Intelligence; der Nachweis, dass sie in Architektur und Erkennung angekommen ist, lässt sich mit diesen zehn Fragen führen.

01 Welche Angreifergruppen sind für unsere Branche benannt, und wo steht das dokumentiert?

02 Wann wurde ein Bericht über einen Angreifer zuletzt in eine konkrete Änderung an Architektur oder Erkennung übersetzt? Beispiel nennen.

03 Welche Geräte dürfen Code aus externen Repositories ausführen, und gilt die Regel auch für Techniker mit Zugang zu Auszahlungs-, Signatur- oder Produktionssystemen?

04 Wie lange lebt eine Cloud-Sitzung, und erkennen wir, wenn ein gestohlenes Sitzungstoken von einem fremden Gerät benutzt wird?

05 Wird das, was signiert oder freigegeben wird, auf einem Gerät geprüft, das der Angreifer nicht kontrolliert?

06 Welche Transaktion, Auszahlung oder Änderung ist zu groß, um ohne zweite Instanz durchzugehen, und ist diese Grenze technisch erzwungen oder nur dokumentiert?

07 Welche Dienstleister haben Zugriff auf unsere Identitäten oder Freigabeprozesse, und was prüfen wir bei ihnen über den Vertrag hinaus?

08 Erkennt unser Monitoring die Vorbereitung eines Angriffs, also Testtransaktionen, neue Berechtigungen, abgeschaltete Schutzmechanismen, oder erst den Schaden?

09 Wann haben wir zuletzt die dokumentierte Kette eines realen Gegners gegen uns selbst nachgestellt, und was war das Ergebnis?

10 Wer außerhalb unserer Organisation würde einen laufenden Angriff zuerst bemerken, und auf welchem Weg erreicht uns diese Information?

ANHANG

Techniken, Quellen, Vorbehalte

A.1 Die sieben Akte nach MITRE ATT&CK

Die Technik-IDs stammen aus den Berichten der genannten Quellen und aus der Angriffskette in Grafik 3. Sie taugen als Prüfliste für die eigene Erkennungsabdeckung: Welche dieser Techniken würde unsere Erkennung sehen, welche unsere Architektur verhindern?

AKT	BEZEICHNUNG	TECHNIKEN NACH MITRE ATT&CK ENTERPRISE	ÖFFENTLICH BESCHRIEBEN SEIT
1	**Der erste Kontakt**	`T1585 Establish Accounts · T1566.003 Spearphishing via Service · T1593.001 Social Media`	FBI/CISA 04/2022 · GitHub 07/2023
2	**Der Köder**	`T1204.002 Malicious File · T1195.001 Software Dependencies · T1027 Obfuscation`	CISA 04/2022 · Unit 42 04/2025
3	**Die gestohlene Identität**	`T1552.001/.004 Unsecured Credentials · T1539 Steal Web Session Cookie · T1528 Steal Access Token`	FBI 12/2024 (DMM) · Unit 42 04/2025
4	**Die Zeit im System**	`T1078.004 Cloud Accounts · T1556.006 Disable MFA · T1087.004 Cloud Account Discovery · T1090 Proxy`	Mandiant 07/2023 · Sygnia 02/2025 · Google 07/2025
5	**Die Generalprobe**	`T1195.002 Supply Chain Compromise · T1565.001 Stored Data Manipulation · T1608 Stage Capabilities`	Safe/Mandiant 03/2025 · TRM 04/2026
6	**Der Zugriff**	`T1565 Data Manipulation · T1657 Financial Theft · T1557 Adversary-in-the-Middle`	FBI 12/2024 · Sygnia 02/2025
7	**Die Flucht mit der Beute**	`T1070.003 Clear Command History · T1070 Indicator Removal · T1485 Data Destruction`	Safe/Sygnia 03/2025 · TRM 10/2026

A.2 Vorbehalte zur Faktenlage

Der Einstieg über den DevOps-Laptop stammt bisher allein von Binance; ein technischer Abschlussbericht ist angekündigt. Die Einschätzung zur Signaturinfrastruktur ist eine Bewertung von TRM Labs. Die Attribution zu TraderTraitor trifft TRM mit hoher Konfidenz, das FBI bestätigt nordkoreanische Akteure; die Verbindung zu Bitget, die das Analysehaus BitOK zieht, ist eine analytische Zuordnung, keine bewiesene Identität. Drift wird von Drift und SEAL 911 dem Cluster UNC4736 zugeordnet, nicht TraderTraitor; die Nordkorea-Zuordnung von Bitget ist unbestätigt. Die Zertifizierungsangaben beruhen auf Binance-Pressemitteilungen von 2019 und 2023; ob sie 2026 gültig sind und die Wallet-Infrastruktur umfassen, ist nicht veröffentlicht. Alle Schadenssummen sind Bewertungen zum Zeitpunkt des Abflusses.

A.3 Quellen

Zum Binance-Hack

- TRM Labs: North Korea Steals USD 6.36 Billion From Binance trmlabs.com
- Elliptic: The largest theft in history elliptic.co
- Bitquery: Binance hack investigation bitquery.io
- BeInCrypto / BitOK: Wie kam es zum Binance-Hack? de.beincrypto.com
- Richard Teng auf X, 30. Oktober 2026 x.com/_RichardTeng
- Decrypt: Binance Sets Aside $6.34B decrypt.co

- CNBC: Binance resumes withdrawals, 90 % covered cnbc.com
- CNBC: Hack raises questions about wallet safety cnbc.com
- Axios: Binance halts trading axios.com

Zum Akteur und seiner Verortung

- FBI, CISA, Treasury: AA22-108A TraderTraitor (April 2022) cisa.gov
- xorl: North Korea (DPRK) Cyber Operations Groups, v2.2 xorl.wordpress.com
- Mandiant: Not So Lazarus (2022) cloud.google.com
- Mandiant: Assessed Cyber Structure of North Korea in 2023 cloud.google.com
- Mandiant: JumpCloud supply chain, UNC4899 (Juli 2023) cloud.google.com
- GitHub Security Alert (Juli 2023) github.blog
- FBI: Cryptocurrency funds stolen by DPRK (August 2023) fbi.gov
- FBI PSA: North Korea responsible for Bybit hack (Februar 2025) ic3.gov
- Unit 42: Slow Pisces coding challenges (April 2025) unit42.paloaltonetworks.com
- Wiz: TraderTraitor Deep Dive wiz.io
- heise: Erste Ermittlungsdetails zum Bybit-Fall heise.de
- TRM Labs: Drift Protocol trmlabs.com
- Security Affairs: Kelp DAO, LayerZero attribution securityaffairs.com
- Security Affairs: DMM Bitcoin, FBI attribution securityaffairs.com

Zu Binance, Zertifizierung und Regulierung

- Decrypt: Binance granted ISO 27001 (2019) decrypt.co
- Binance: ISO 27001 und 27701 Zertifizierungen (Juni 2023) aap.com.au
- Binance: SOC 2 Type II (Dezember 2023) aap.com.au
- Fortune: Trump pardons Changpeng Zhao fortune.com
- BTC-ECHO: Binance zieht Bilanz nach Europa-Aus btc-echo.de
- TechCrunch: Binance pledges changes after 2019 hack techcrunch.com
- Daniel Heessel: Erpressen lässt sich Berlin nicht. Ausnehmen schon. (Security Insider, September 2026) security-insider.de

THREAT-INFORMED®

Compliance stoppt keine Angreifer. Wir schon.

ÜBER THREAT-INFORMED

Threat-Informed Cyber Security Solutions GmbH baut Sicherheit vom Angreifer her: Wer greift uns an, wie erkennen wir ihn, was tun wir, damit er scheitert. Daraus entstehen ISMS nach ISO 27001, BSI IT-Grundschutz und KRITIS, Audits und GAP-Analysen gegen ISO 27001, NIST CSF, CIS Controls und MITRE ATT&CK Coverage, sowie Threat-Informed Defense als Programm. Compliance ist dabei das Ergebnis, nicht der Ausgangspunkt.

ÜBER DEN AUTOR

Daniel Thomas Heessel ist Gründer und Managing Partner von Threat-Informed, ISO 27001 Lead Auditor, CISSP, CISM und MITRE ATT&CK Defender. Er prüft seit Jahren Managementsysteme für Informationssicherheit, unter anderem für den TÜV NORD, und hat selbst vier ISMS aufgebaut. 2026 wurde er von der CISO Alliance als CISO of the Year ausgezeichnet. Er schreibt für Security Insider und IT-SICHERHEIT und arbeitet an dem ersten deutschsprachigen Buch über Threat-Informed Defense.

KONTAKT

Daniel Thomas Heessel · +49 173 9977827 · threat-informed.de