KILLSWITCH · ISSUE #7 · 4 NOV 2026

They Didn't Steal Binance's Keys. They Made Binance Sign.

The keys stayed safe. The process that uses them did not.

Killswitch rating: Review your signing path this month

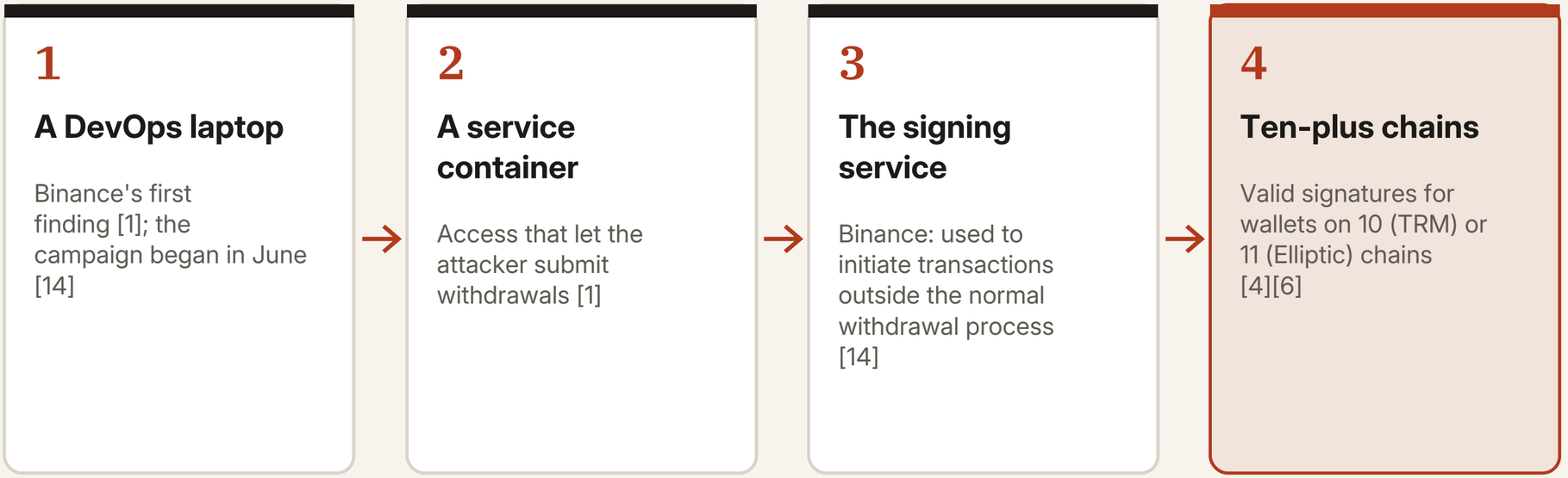
By Emmanuel Aigbehi Walstra

They didn't steal the keys. They made Binance sign.

About $6.3B left Binance hot wallets on 29 October, most of it in about 20 minutes [1][4].

- Binance: "no evidence of any wallet private key leak" [1].
- Analysts: the attacker reached the signing machinery, and it signed [4][6].

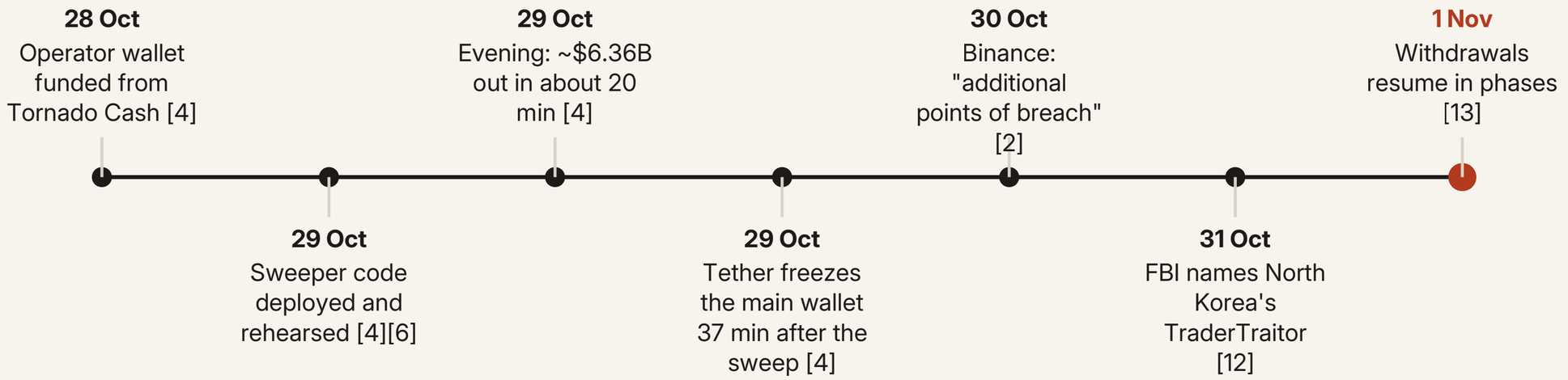
Started with at least one laptop. Ended at the signer.



Binance's 30 Oct account [1], Decrypt's report of its same-day update [2], and Binance's 3 Nov initial report [14], which confirms the signing-service step; TRM and Elliptic [4][6].

03 · 28 OCT TO 1 NOV

Staged a day ahead. Mostly drained in 20 minutes.



TRM [4], Elliptic [6], Decrypt [2], FBI [12], TechCrunch [13]. All dates 2026.

Valid signatures, every chain

- Ethereum: one transaction with 50 signed EIP-7702 authorisations, one per nonce [4][6].
- The sweeper then emptied the wallet: $2.53B in one transaction [6].
- Other chains: ordinary signed transfers [4].
- Binance, 3 Nov: the attacker used its wallet signing service to initiate transactions outside the normal withdrawal process [14].

FBI: North Korea's TraderTraitor

- FBI, 31 Oct: North Korea was responsible; it calls the activity TraderTraitor [12].
- TRM: TraderTraitor, "high confidence" [4]. Chainalysis: funds commingled with the Bitget theft [5].
- Binance says its investigation has not blamed any individual employee [2].

06 · THE NUMBERS

Same theft, four counts

1 Binance [14]

About $6.34B; about $2.85B frozen or intercepted

2 TRM Labs [4]

$6.36B on 10 chains; about $2.7B frozen

3 Chainalysis [5]

About $6.4B; about $2.8B frozen

4 Elliptic [6]

$6.43B on 11 chains; $2.85B (44%) frozen or seized

Totals differ by firm, by price and by time of count. Frozen figures change by the hour.

07 · ACT

Five controls for the signing path

1. **Isolate who can ask for signatures**
   Privileged workstations only; no daily-use laptops
2. **Policy before signature**
   The signer checks destination, amount and type, not just the caller
3. **Treat batch requests as an IoC**
   Many signatures across a range of nonces [4]; cap value per wallet per hour
4. **Reject unexpected delegations**
   EIP-7702 authorisations only when expected; alert on any [4]
5. **Separate by chain and tier**
   One compromise should not sign for every chain [4]

Killswitch's own list. TRM's recommendations are marked [4]; the velocity cap is ours.

Where this lives in your frameworks

Privileged endpoint	A.8.1, A.8.2 · NIS2 21(2)(i), (j) · DORA Art. 9
Signing policy and duties	A.5.3 · cl. 6.1.3 · NIS2 21(2)(a) · DORA Art. 9 · RTS 2024/1774 Art. 21(b)
Detect odd signing	A.8.15, A.8.16 · DORA Art. 10
Respond and report	A.5.24-A.5.26 · NIS2 21(2)(b), Art. 23 · DORA Art. 17-19

Killswitch's own mapping; check ISO titles. For DORA-regulated entities, DORA is the sector-specific act (NIS2 Art. 4) [9][10].

ISO/IEC 27001:2022 [8] · NIS2 [9] · DORA [10] · RTS 2024/1774 [11]. Killswitch mapping.

09 · STILL OPEN

What we don't know yet

- Full findings: Binance's 3 Nov report is initial; review ongoing [14].
- Technical details: Binance keeps some confidential [14].
- Chain count: 10 (TRM) or 11 (Elliptic).
- Final stolen and frozen totals.

Do this month

- List every system that signs or approves for you.
- Requests only from privileged workstations or service identities.
- Check what the signer verifies beyond authentication.
- Alert on batch signing; cap value per wallet.
- Rehearse a revocation; keep the evidence.

Sources

[1] Binance: Security Incident Update (30 Oct 2026)
[2] Decrypt: Binance Finds "Additional Points of Breach" in $6.3B Hack
[3] BBC News live: Binance hack
[4] TRM Labs: North Korea Steals USD 6.36 Billion From Binance in the Largest Hack in History
[5] Chainalysis: Binance Hack: Tracing the $6.4 Billion Theft to North Korea
[6] Elliptic: The largest theft in history: North Korea behind the $6.4 billion Binance hack (final update 1 Nov 2026)
[7] Reuters via Yahoo News: FBI and US Secret Service working with Binance after $6.3 billion hack, source says
[8] ISO/IEC 27001:2022 Information security management systems
[9] NIS2 Directive (EU) 2022/2555, Articles 4, 21 and 23
[10] DORA, Regulation (EU) 2022/2554, Articles 2, 9, 10 and 17 to 19
[11] Commission Delegated Regulation (EU) 2024/1774 (ICT risk-management RTS), Article 21
[12] FBI Cyber Alert: North Korea Responsible for $6 Billion+ Binance Attack (31 Oct 2026)
[13] TechCrunch: Binance resumes withdrawals following $6.3 billion breach (1 Nov 2026)
[14] Binance: 29 October Binance Security Incident: Initial Findings and Response Update (3 Nov 2026)

Facts are from Binance, the FBI, TRM Labs, Chainalysis, Elliptic and named news reports, as published by 4 Nov 2026. On-chain figures are the analysts' and differ by firm and by time. Binance's 3 Nov report is an initial one and its investigation is ongoing. The velocity cap, the control list and the framework mapping are Killswitch's own.

FROM THE PUBLISHERS OF KILLSWITCH

Map your signing and privileged-access controls, with the evidence

GRCOMPLIANCE

Keep your privileged-access, signing and incident controls, owners and evidence in one place, mapped to ISO 27001, NIS2 and DORA.

Try the live demo →

demo.grcompliance.com

Self-host free: github.com/Sectutor/GRCompliance-Core

SECTUTOR

Security and GRC books, training and audit kits.

sectutor.com

Emmanuel Aigbehi Walstra is a CISO who also serves as a virtual CISO (vCISO) for several organisations, with 30+ years in cybersecurity, 10,000+ people trained, and author of the CCSP Excellence books.