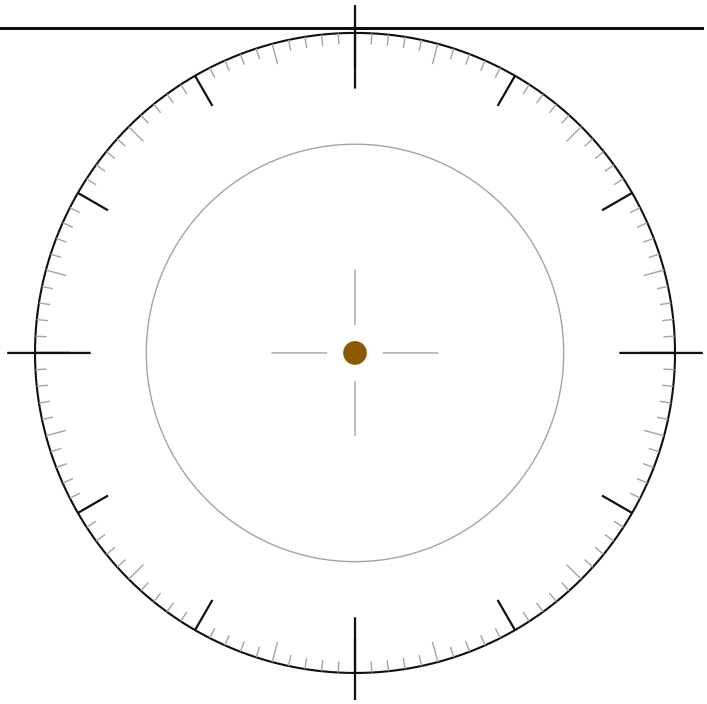
DEEO.AI

FICHE D'ACTUALITÉ · ACCÈS LIBRE



01 · IA

VEILLE IA · FICHE D'ACTUALITÉ · 30 OCTOBRE 2026

Binance : personne n'a volé la clé · Veille IA hors-série

Fiche d'actualité DEEO.AI · Veille IA, hors-série. Situation au 30.10.2026, enquête en cours.

PUBLICATION	30 octobre 2026
SITUATION	30.10.2026 · faits vérifiés à cette date
DOMAINE	01 · IA · Intelligence artificielle
VIDÉO	7 min 25, sur deeo.ai et YouTube : la vidéo et la fiche disent la même chose.

Vidéo · 7 min 25
deeo.ai/videos/veille-ia-hs-binance/

PARTAGE

Fiche en accès libre : vous pouvez la partager, en citant DEEO.AI.

CHAPÔ

Le 29 octobre 2026 au soir, environ 6,3 milliards de dollars sont sortis des caisses de Binance, que CNN décrit comme la plus grande plateforme d'échange de cryptomonnaies au monde. L'essentiel est parti en une vingtaine de minutes. C'est le plus gros vol jamais documenté. Pourtant, selon Binance, aucune clé secrète n'a fuité. Aucun coffre n'a été forcé : l'attaquant a fait signer le système lui-même, après être entré, semble-t-il, par l'ordinateur d'un ingénieur. Les enquêteurs privés désignent la Corée du Nord. Et l'IA ? Aucune source ne dit qu'elle a servi à ce vol. Mais la question de son rôle, du côté des voleurs comme des défenseurs, se pose plus que jamais.

Sources numérotées en fin de fiche, avec leur fiabilité ; les rapprochements faits par DEEO.AI sont signalés comme tels. L'enquête est en cours : les chiffres sont ceux connus au 30.10.2026 au soir et peuvent encore changer.

EN UNE MINUTE

- **Le vol** : le 29.10.2026, à partir de 21 h 05 (heure de Paris), environ 6,3 milliards de dollars quittent Binance sur 10 blockchains, l'essentiel en une vingtaine de minutes. C'est environ quatre fois le précédent record, le vol de Bybit en 2025 [1] [3] [10].
- **Sans forcer le coffre** : selon Binance, aucune clé privée n'a fuité. La piste : l'ordinateur portable compromis d'un ingénieur, puis un système de signature détourné, qui a validé lui-même les retraits. Binance parle d'une attaque complexe, en plusieurs étapes [1] [3] [6].
- **Les dégâts limités** : environ 3 milliards ont été gelés, surtout par les émetteurs de « stablecoins ». Binance promet de couvrir toutes les pertes. Les fonds volés venaient des caisses de la plateforme, pas des comptes des clients [3] [4] [5].
- **La piste nord-coréenne** : les sociétés d'enquête TRM Labs et Chainalysis attribuent le vol au groupe nord-coréen TraderTraitor. Au 30.10, aucune attribution officielle : le FBI dit seulement avoir connaissance de l'incident et enquête [1] [2].
- **Et l'IA ?** Aucune source ne dit qu'elle a servi à ce vol. Mais des pirates nord-coréens l'utilisent déjà, et la même semaine, Anthropic a montré qu'un modèle pouvait trouver des failles graves dans des logiciels très répandus, avec peu d'intervention humaine [14] [15] [17].

1. Le vol en vingt minutes

1.1 Le 29 octobre 2026, à 20 h 05 en temps universel, soit **21 h 05 à Paris**, les premières sorties de fonds apparaissent sur les registres publics des cryptomonnaies, les blockchains. Elles touchent **10 blockchains**. Selon la société d'enquête TRM Labs, l'essentiel part en **environ 20 minutes**, puis d'autres vagues suivent jusque vers minuit, temps universel [1].

1.2 Le montant donne le vertige. Binance parle d'« environ 6,3 milliards de dollars » [3] [4]. TRM Labs compte 6,36 milliards aux prix du moment [1]. C'est **le plus gros vol jamais documenté**, environ **quatre fois** celui de Bybit, une autre plateforme, vidée d'environ 1,5 milliard de dollars le 21.02.2025 selon le FBI [1] [10].

1.3 Qu'a-t-on pris ? Selon TRM Labs, et de façon approximative : surtout des stablecoins, des cryptomonnaies adossées au dollar (USDT, USDC, RLUSD), mais aussi plus de 18 270 bitcoins (environ 1,47 milliard de dollars), environ 200 600 ethers et d'autres jetons [1].

1.4 Une précision importante : l'argent volé venait des caisses de la plateforme, pas des comptes des clients. Pour les clients, la gêne principale est ailleurs : ils ne peuvent plus retirer leur argent [5].

1.5 **La riposte, en moins d'une heure.** Les stablecoins ont une particularité : leur émetteur peut bloquer les jetons. Les premiers gros gels tombent moins d'une heure après le début du vol : Tether gèle 971 millions de dollars à 21 h 01, temps universel, puis Circle 823 millions à 21 h 04, d'après TRM Labs. Au total, selon TRM, Tether a gelé environ 1,8 milliard et Circle environ 825 millions [1]. Le 30.10, Binance chiffre l'ensemble des fonds gelés à **environ 3 milliards de dollars** [3].

1.6 **La réponse de Binance.** La plateforme promet : « Binance couvrira toutes les pertes », avec son fonds de secours, appelé SAFU, et ses fonds propres. Elle assure que « les fonds des utilisateurs sont en sécurité ». Le 30.10, elle dit avoir mis de côté plus de 6,34 milliards de dollars [3] [4].

1.7 Les **retraits sont suspendus** depuis le 29.10 au soir. Binance a annoncé leur reprise « dans les 45 heures », soit vers le 1er novembre [5]. Les dépôts ont rouvert. Les échanges continuent : seul un service, Binance Alpha, a cessé les siens [5].

1.8 **Les marchés.** Sur 24 heures, le bitcoin a perdu environ 5 %, l'ether environ 5 à 6 %, et le BNB, le jeton de Binance, environ 7 à 8 % [9].

2. Sans forcer le coffre

2.1 Une plateforme comme Binance range ses cryptomonnaies dans des portefeuilles numériques. Certains sont des **portefeuilles « chauds »** : des caisses connectées en permanence, qui servent aux retraits courants des clients. C'est de là que les fonds sont partis [1].

2.2 Comment ? Le 30.10, Binance donne une première explication. L'incident « pourrait impliquer » **l'ordinateur portable compromis d'un ingénieur DevOps**, c'est-à-dire chargé de faire tourner les serveurs. Cet ordinateur aurait permis d'accéder à un « conteneur de service », une petite boîte logicielle qui fait tourner une partie du système, et de **soumettre des retraits non autorisés**. Binance précise : **aucune preuve de fuite de clé privée**, la clé secrète qui permet de dépenser les fonds [3] [4].

2.3 TRM Labs a observé un moment clé. À 20 h 20, temps universel (21 h 20 à Paris), **une seule transaction porte 50 autorisations signées à l'avance**. Elles s'appuient sur un mécanisme d'Ethereum appelé EIP-7702 et transforment une caisse Ethereum de Binance en **aspirateur** contrôlé par l'attaquant. La caisse est vidée **environ trois minutes et demie** plus tard [1]. Ce mécanisme est ce qu'on a vu à l'œuvre ; ce n'est pas la cause première.

2.4 Pour TRM Labs, la cause la plus probable est ailleurs : le **système de signature** des portefeuilles chauds a été compromis. Autrement dit, c'est le système lui-même qui a « signé » les ordres de sortie. Comment l'attaquant a obtenu ces signatures ? On ne le sait pas encore [1].

2.5 L'histoire ne s'arrête pas à un ordinateur. Le 30.10, Binance dit avoir trouvé **d'autres points d'intrusion**, sans les décrire : « une attaque complexe » [6]. Richard Teng, co-PDG de Binance, résume : ce n'était pas une attaque « en un clic », mais une attaque **en plusieurs étapes**, sans fuite de clé privée [6].

2.6 Pour se représenter la scène : on n'a pas percé le coffre. On a obtenu des ordres de virement déjà signés, et la banque les a exécutés.

3. La piste nord-coréenne

3.1 Qui est derrière ? Deux sociétés spécialisées dans l'analyse des blockchains ont donné leur avis. **TRM Labs** attribue le vol, « avec une grande confiance », au groupe nord-coréen **TraderTraitor**. Elle s'appuie sur des indices trouvés sur la blockchain et en dehors [1]. **Chainalysis**

l'attribue au même groupe : des fonds sortis de Binance se sont mêlés, en direct, à ceux du vol de la plateforme Bitget, en septembre 2026, lui aussi attribué à la Corée du Nord [2].

3.2 Ce sont des enquêteurs privés. **Aucune attribution officielle** n'existe au 30.10 : ni d'un État, ni du FBI. Le FBI dit seulement « avoir connaissance de l'incident » et enquête, avec le Secret Service. Binance n'a nommé personne et coopère avec les forces de l'ordre [1]. Pour Bybit, en 2025, le FBI avait attribué le vol à la Corée du Nord cinq jours après les faits [10].

3.3 **Une attaque préparée.** Selon TRM Labs, le portefeuille de l'attaquant était alimenté dès le 28.10 au matin, au moins 36 heures avant le vol. L'argent venait de Tornado Cash, un service qui mélange les fonds pour brouiller leur origine [1].

3.4 **Une méthode connue.** Le FBI, l'agence américaine de cybersécurité CISA et le Trésor américain ont décrit la méthode de TraderTraitor dès le 18.04.2022. Le groupe envoie des messages à des employés de sociétés crypto, souvent des administrateurs système ou des ingénieurs DevOps. Il leur fait miroiter des **emplois bien payés**, pour leur faire télécharger de **fausses applications** piégées. Ensuite, il vole leurs accès [12].
On ignore à ce jour comment l'ordinateur de l'ingénieur de Binance a été compromis.

3.5 **Un air de déjà-vu.** Pour Bybit, l'attaque était passée par la machine d'un développeur de Safe{Wallet}, un prestataire de la plateforme, selon l'enquête menée par Safe et la société Mandiant, publiée le 06.03.2025 [11].

3.6 L'enjeu dépasse Binance. Selon Chainalysis, les vols attribués à la Corée du Nord ont atteint **au moins 2 milliards de dollars en 2025**, en hausse de 51 % sur un an [13].

4. L'IA, arme ou bouclier ?

4.1 Cette partie est une mise en contexte de DEEO.AI : aucune source ne relie l'intelligence artificielle à ce vol.

4.2 **Ce que disent les enquêteurs.** Ni Binance, ni TRM Labs, ni Chainalysis ne disent que l'IA a servi au vol. Chainalysis parle seulement d'un blanchiment « probablement automatisé », c'est-à-dire de fonds déplacés en masse par des programmes [2].

4.3 **Une opinion qui inquiète.** Bernardo Brites, PDG de Trace Finance, cité par Reuters et RTÉ le 30.10, estime : « It's becoming very hard to counter hacks as AI can find vulnerabilities faster than you can fix them » (il devient très difficile de contrer les piratages, car l'IA trouve les failles plus vite qu'on ne peut les corriger) [8]. C'est une opinion, pas un constat sur ce vol.

4.4 **L'IA déjà chez les pirates nord-coréens.** Plusieurs entreprises d'IA l'ont documenté :

- Anthropic (27.08.2025) : des informaticiens nord-coréens utilisent son IA, Claude, pour se fabriquer de fausses identités, réussir des tests techniques, puis faire le travail une fois embauchés [15] ;
- OpenAI (juin 2025) : des comptes bannis fabriquaient de faux profils pour décrocher des emplois à distance [16] ;
- Google (05.11.2025) : un groupe nord-coréen a utilisé son IA, Gemini, pour du repérage sur les portefeuilles crypto ; un autre, pour développer des attaques [17].

4.5 **La même semaine, sans lien avec le vol.** Le 27.10.2026, deux jours avant le vol, l'équipe « Frontier Red Team » d'Anthropic a publié une démonstration. Un modèle de recherche interne, non publié, a trouvé des **failles nouvelles** et monté des attaques sur **Chrome, Safari, Android et Linux** ; pour Windows, il a obtenu un plantage à distance. Il l'a fait « avec peu d'intervention humaine », après une première consigne. Les failles ont été **signalées aux éditeurs avant la publication** : Google, Apple, Microsoft et les développeurs de Linux. Anthropic présente ce travail comme une avance donnée aux défenseurs [14].

4.6 **Le bouclier.** Les mêmes modèles servent aussi à chercher les failles pour les corriger. Anthropic propose par exemple, depuis le 08.10.2026, un service gratuit de recherche de failles pour les logiciels libres [18]. Quant au suivi en direct des fonds volés, qui a permis les gels rapides, il repose sur l'analyse des blockchains par TRM Labs et Chainalysis. Il n'est pas présenté comme de l'IA [1] [2].

4.7 Alors, arme ou bouclier ? Les deux usages existent déjà. Dans ce vol, rien ne montre que l'IA ait joué un rôle. Mais le point d'entrée supposé, l'ordinateur d'une personne, est justement celui que l'IA peut aider à tromper, ou à protéger. La question reste ouverte.

5. Ce qu'on sait aujourd'hui

- **Le montant** : environ 6,3 milliards de dollars sortis, dont environ 3 milliards gelés [1] [3].
- **Le solde de l'attaquant** : il détient encore environ **2,4 milliards de dollars** hors de portée des émetteurs de stablecoins, sous forme de plus de 420 000 ethers et de 18 270 bitcoins, selon TRM Labs [1].
- **Les clients** : leurs comptes n'étaient pas la cible, mais leurs retraits restent bloqués. Au 30.10 au soir, les retraits n'avaient pas repris ; Binance a annoncé leur reprise vers le 1er novembre [5].
- **L'enquête** : TRM Labs et Chainalysis désignent le groupe nord-coréen TraderTraitor. Le FBI enquête, avec le Secret Service, sans attribution officielle [1] [2].
- **La cause** : un ordinateur d'ingénieur compromis, un système de signature détourné, et d'autres points d'intrusion encore non décrits [3] [6].

5.1 Ce qu'on attend : la reprise réelle des retraits, le rapport technique promis par Binance, une éventuelle attribution officielle, et l'évolution des montants gelés.

5.2 Pour résumer : on a dérobé six milliards sans forcer de coffre, en faisant signer le système lui-même, après être entré par l'ordinateur d'un ingénieur. Le maillon faible, c'est la personne derrière l'écran. L'IA va-t-elle la rendre plus facile à tromper, ou plus facile à protéger ?

Sources

Consultées le 30.10.2026. Fiabilité indiquée en italique.

[1] TRM Labs, analyse du vol de Binance et de son attribution, https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history , 30.10.2026. *Société d'analyse de blockchain ; source la plus détaillée, données provisoires (« story still developing ») ; l'attribution est son avis.*

[2] Chainalysis, derniers constats sur le vol de Binance, https://www.chainalysis.com/blog/binance-exploit-latest-findings-and-response/ , 30.10.2026. *Société d'analyse de blockchain ; attribution et chiffres provisoires.*

[3] CoinDesk, article du 29.10.2026 sur le piratage de Binance, https://www.coindesk.com/business/2026/10/29/potential-multi-billion-binance-hack-hitting-crypto-markets . *Presse spécialisée ; reprend les déclarations de Binance.*

[4] ABC7 (Associated Press), estimation par Binance du montant de l'intrusion, https://abc7.com/story/binance-estimates-security-breach-impact-63-billion/19999397/ , 30.10.2026. *Agence de presse ; reprend les déclarations de Binance.*

[5] TechCrunch, suspension des retraits par Binance, https://techcrunch.com/2026/10/29/binance-pauses-withdrawals-as-hackers-suspected-of-stealing-billions-in-crypto/ , 29.10.2026. *Presse spécialisée.*

[6] Decrypt, nouveaux points d'intrusion trouvés par Binance, https://decrypt.co/382203/binance-finds-additional-points-of-breach-in-6-3b-hack , 30.10.2026. *Presse spécialisée ; reprend les déclarations de Binance et de Richard Teng.*

[7] CNN, article sur le vol de Binance, https://www.cnn.com/2026/10/30/tech/binance-crypto-heist-hnk-intl , 30.10.2026. *Presse généraliste.*

[8] RTÉ (avec Reuters), réactions au vol de Binance, https://www.rte.ie/news/business/2026/1030/1597305-binance-bitcoin-world/ , 30.10.2026. *Presse généraliste ; la citation de Bernardo Brites est une opinion.*

[9] The Block, baisse du bitcoin après le piratage, https://www.theblock.co/news/markets/2026-10-29-bitcoin-slides-below-77000-binance-hack-432183 , 29.10.2026. *Presse spécialisée ; variations sur 24 heures, approximatives.*

[10] FBI, avis public sur le vol de Bybit (I-022625-PSA), https://www.ic3.gov/PSA/2025/PSA250226 , 26.02.2025. *Source officielle.*

[11] Safe Ecosystem Foundation, communiqué sur l'enquête menée avec Mandiant après le vol de Bybit, https://safe.global/blog/safe-ecosystem-foundation-statement , 06.03.2025. *Source primaire (entreprise concernée).*

[12] FBI, CISA et Trésor américain, avis AA22-108A sur TraderTraitor, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a , 18.04.2022. *Source officielle.*

[13] Chainalysis, bilan des vols de cryptomonnaies en 2025, https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/ , 18.12.2025. *Société d'analyse de blockchain ; estimations de la source.*

[14] Anthropic (Frontier Red Team), « Discovering and exploiting vulnerabilities in critical, real-world software with Claude », https://www.anthropic.com/research/discovering-vulnerabilities-with-claude , 27.10.2026. *Source primaire ; sans lien avec Binance.*

[15] Anthropic, rapport sur la détection des usages malveillants de Claude, https://www.anthropic.com/news/detecting-countering-misuse-aug-2025 , 27.08.2025. *Source primaire (constats de l'entreprise).*

[16] OpenAI, rapport sur les usages malveillants de l'IA, https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf , juin 2025. *Source primaire (constats de l'entreprise).*

[17] Google Threat Intelligence Group, usage des outils d'IA par des groupes malveillants, https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools , 05.11.2025. *Source primaire (constats de l'entreprise).*

[18] Anthropic, lancement d'un service de recherche de failles pour les logiciels libres, https://www.anthropic.com/research/launching-opt-in-vuln-finding-service-for-open-source , 08.10.2026. *Source primaire (annonce de l'entreprise).*

Point vérifié par DEEO.AI le 30.10.2026 vers 18 h 50 : le FBI dit seulement avoir connaissance de l'incident et enquête, avec le Secret Service, sans attribution officielle ; les retraits n'avaient pas repris.

DEEO.AI cite ces sources et ne garantit pas leurs chiffres ; les estimations, attributions et déclarations restent sous la responsabilité de leurs auteurs. Cette fiche n'est pas un conseil d'investissement.

SITUATION	Faits vérifiés au 30.10.2026, sur les sources primaires.
VIDÉO	La vidéo de cette actualité (7 min 25) est sur sa page de deeo.ai : https://deeo.ai/videos/veille-ia-hs-binance/
PARTAGE	Fiche en accès libre : vous pouvez la partager, en citant DEEO.AI.
CONTACT	admin@deeo.ai · deeo.ai

DEEO.AI OBSERVATOIRE DE L'ÉMERGENCE DE L'IA