> HÁTTÉRANYAG SZAKMABELIEKNEK

Binance: egy fejlesztő laptopján át a történelem legnagyobb kriptorablása, kb. 6 milliárd dollár

Nem a széfet törték fel, hanem egy laptopot

Esemény: 2026. október 29.
Lezárva: 2026. október 30. (kutatási változat: v1)
AI-csapattal készült, átnézte: Péter

Összefoglaló

2026. október 29-én a Binance kriptotőzsdéről a cég szerint kb. 6,3 milliárd dollárnyi eszközt érintő lopás történt (a Chainalysis szerint kb. 5,9 milliárd), ami a valaha volt legnagyobb kriptorablás. Az előzetes vizsgálat szerint egy DevOps-mérnök feltört laptopjáról jutottak el egy belső szolgáltatáskonténerig, és onnan adtak be jogosulatlan kifizetéseket; a cég szerint privát kulcs nem szivárgott, kb. 3 milliárd dollárt befagyasztottak, a kárt a SAFU-alapból és saját forrásból állja, a kifizetések átmenetileg szünetelnek. Elemzők (TRM Labs) az észak-koreai TraderTraitor csoportnak tulajdonítják, hatósági megerősítés még nincs. A legfontosabb teendő magánszemélyként: a rablás után várható hamis „Binance-ügyfélszolgálat”, kártérítési és pénzvisszaszerző megkeresésekre ne reagálj, és soha ne utalj „biztonságos tárcába”; szervezetként: a kulcsemberek gépét és a kifizetést indító folyamatokat is úgy védd, mint a kulcsokat.

KULCSMEGÁLLAPÍTÁSOK

- A Binance szerint kb. 6,3 milliárd dollárnyi eszköz érintett (Chainalysis: kb. 5,9 milliárd), ez a valaha volt legnagyobb kriptolopás, a 2025-ös Bybit-eset kb. négyszerese.
- Az előzetes vizsgálat szerint egy DevOps-mérnök feltört laptopja volt a kiindulópont, onnan egy belső szolgáltatáskonténerből indultak a jogosulatlan kifizetések; a privát kulcsok a cég szerint nem szivárogtak ki.
- Kb. 3 milliárd dollárt befagyasztottak (Tether 1,57 milliárd USDT, Circle 800 millió+ USDC), a Binance a veszteséget a SAFU-alapból és saját forrásból vállalta, a kifizetések átmenetileg szünetelnek.
- Elemzők az észak-koreai TraderTraitor csoportnak tulajdonítják, amely korábban fejlesztők gépén keresztül rabolta ki a DMM Bitcoint és a Bybitet; hatósági megerősítés még nincs.
- Magyar érintettség nem ismert; a fő hazai kockázat a hírre épülő második hullám: hamis ügyfélszolgálati, kártérítési és pénzvisszaszerző csalások.

Mi történt

2026. október 29-én (csütörtök) a világ legnagyobb kriptotőzsdéje, a **Binance** tárcáiból tömegesen áramlottak ki eszközök. Először felhasználók és blokklánc-figyelők jelezték a szokatlan kiáramlást, majd az alapító, Changpeng Zhao (CZ) írt arról az X-en, hogy valószínűleg feltörték a tőzsdét; ezután a Binance megerősítette, hogy biztonsági incidenst kezel. (TechCrunch; Fortune) – **megerősített**

A legfontosabb tények (2026. október 30. reggeli állapot):

- **Méret:** a Binance szerint az incidens becsült teljes hatása kb. **6,3 milliárd dollár**. A Chainalysis a lopás pillanatára vonatkozó becslését kb. **5,9 milliárd dollárra** (5,912 milliárd) módosította; ez a cég szerint közel négyszerese az eddigi második legnagyobb kriptorablásnak. Mindkét szám a valaha volt legnagyobb kriptolopást jelenti, megelőzve a Bybit 2025. februári, kb. 1,5 milliárd dolláros esetét. (Binance Square – Binance News; CoinDesk; The Hacker News) – **megerősített** (a két szám eltérő módszerű becslés, lásd Nyitott kérdések)
- **Mit vittek el:** az Arkham adatai szerint a támadói tárcákban egy ponton több mint 5,7 milliárd dollár volt, köztük kb. 1,5 milliárd dollár bitcoin, 0,9 milliárd ether, kb. 1,5 milliárd USDT és több mint 0,8 milliárd USDC. (CoinDesk; Fortune) – **jelentett** (két sajtóforrás, blokklánc-elemzőre hivatkozva)
- **Hogyan (előzetes vizsgálat):** a Binance szerint az incidens kiindulópontja valószínűleg egy **DevOps-mérnök (üzemeltető-fejlesztő) feltört laptopja** volt. Erről a gépről a támadó egy **szolgáltatáskonténerhez** (a tőzsde egyik belső, futó szoftverkomponenséhez) fért hozzá, és onnan **jogosulatlan kifizetési tranzakciókat** adott be. A cég szerint **nincs jele annak, hogy a tárcák privát kulcsai kiszivárogtak**. A Binance azt is közölte, hogy több tényező játszott közre, és a teljes útvonalat még vizsgálja; a laptop feltörésének módját, a konténer szerepét és a hibázó kontrollokat nem hozta nyilvánosságra. (Binance Square – Binance News; CyberInsider; The Hacker News) – **megerősített** (a cég elsődleges közlése; előzetes eredmény)
- **Befagyasztás:** a Binance szerint partnerekkel együtt kb. **3 milliárd dollárnyi** érintett eszközt fagyasztottak be a láncon; ez nem azonos a visszaszerzett pénzzel. A Tether több mint 1,57 milliárd USDT-t, a Circle több mint 800 millió USDC-t fagyasztott be; a Ripple kb. 200 millió dollárnyi eszközt. (Binance Square; CoinDesk; Portfolio; Cyber Security News) – **megerősített** (Tether, Circle) / **jelentett** (Ripple)
- **Az Arbitrum** biztonsági tanácsa a The Hacker News szerint kb. 30,5 millió dollárt fagyasztott be a „Binance Exploit”-hoz kötve. (The Hacker News) – **jelentett** (egy forrás)
- **A támadó mozgatja a pénzt:** a beszámolók szerint az eszközök egy részét decentralizált tőzsdén (Uniswap) váltották, és lopott USDT-t fedezetként használva legalább 20 000 WETH-et (kb. 44 millió dollár) vettek fel hitelbe az Aave-en, ami a stabilérmék befagyasztását megelőző menekítésre utalhat. (CoinDesk; Fortune) – **jelentett**
- **Ki állja a kárt:** a Binance szerint minden veszteséget a **SAFU-alapból** (Secure Asset Fund for Users, a felhasználók védelmére képzett tartalékalap, a beszámolók szerint kb. 1 milliárd dollárnyi bitcoin) és **saját forrásból** fedez; a cég és CZ szerint a felhasználók pénze biztonságban van. (Binance Square; CoinDesk; Cyber Security News) – **megerősített** (vállalás; részletes kártalanítási terv nincs)
- **Szolgáltatás:** a Binance óvatosságból felfüggesztette a be- és kifizetéseket, és visszavonta az érintett cím jogosultságát. Egy későbbi frissítés szerint a **befizetések újraindultak**, a **kifizetések szünetelnek**, amíg a kifizetési szolgáltatást és a kapcsolódó címeket átalakítják; a cég becslése szerint 48 órán belül indulhatnak újra. (CyberInsider; The Week; Portfolio) – **megerősített** (a 48 óra becslés)

- **Ki áll mögötte:** a Binance nem nevezett meg elkövetőt. A TRM Labs blokklánc-elemző cég „nagy bizonyossággal” az észak-koreai állami **TraderTraitor** csoportnak tulajdonítja, amelyet a Bybit-rablással is összeköt; a Blockaid és ZachXBT nyomozó is Észak-Koreára (Lazarus-csoport) utal. Bizonyítékot nyilvánosan nem tettek közzé. (CoinDesk; CyberInsider; HVG; Fortune) – **jelentett** (elemzői hozzárendelés, hatósági megerősítés nincs)
- **Piac:** a bitcoin 2–5%-ot, az ether 4–6%-ot, a Binance saját tokenje (BNB) kb. 5–8%-ot esett; a Fortune szerint a reakció viszonylag visszafogott volt. (CoinDesk; The Week; Portfolio) – **megerősített** (az eltérés a mérés időpontjából adódik)
- **Következő lépések:** a Binance részletes technikai utólagos elemzést (post-mortem) és a kármentés után frissített tartalékigazolást (Proof of Reserves) ígér. (Binance Square; CyberInsider) – **megerősített**

Ugyanaznap, külön eset: a Polymarket előrejelzési piac egy külső szoftverszolgáltató kompromittálása miatt rövid időre leállt; a kár kb. 2–3 millió dollár. A források szerint nincs összefüggés a Binance-esettel. (TechCrunch; CoinDesk)

Idővonal

Dátum	Esemény	Forrás
2024. március–május	TraderTraitor álláshirdetéses kódolási teszttel feltöri egy japán tárcaszoftver-cég munkatársának gépét; a DMM Bitcoin 308 millió dollárt veszít (megerősített, FBI)	BleepingComputer
2025. február 21.	Bybit: kb. 1,5 milliárd dollár; a Safe{Wallet} egyik fejlesztőjének gépét törték fel; az FBI a TraderTraitornak tulajdonítja (megerősített)	The Hacker News
2025. február 26.	Binance-ügyfeleknek „Lazarus-támadás” ürügyű hamis SMS-ek, „biztonságos tárcába” utaltatás (jelentett)	ForkLog
2026. október 29.	Tömeges kiáramlás a Binance tárcáiból; CZ jelzi a valószínű feltörést; a Binance megerősíti az incidenst, felfüggeszti a be- és kifizetéseket (megerősített)	TechCrunch; Fortune
2026. október 29.	A Tether (1,57 milliárd USDT) és a Circle (800 millió+ USDC) befagyaszt; a TRM Labs a TraderTraitornak tulajdonítja (megerősített / jelentett)	CoinDesk
2026. október 29–30. éjjel	A Binance közli: kb. 6,3 milliárd dollár hatás, kb. 3 milliárd befagyasztva, DevOps-laptop az előzetes kiindulópont, privát kulcs nem szivárgott, SAFU-ból és saját forrásból kártalanít (megerősített)	Binance Square
2026. október 30.	Befizetések újraindulnak, kifizetések szünetelnek, becslés: 48 órán belül; a Chainalysis kb. 5,9 milliárd dollárra teszi a lopást (megerősített)	CyberInsider; The Hacker News

Szereplők és háttér

- **Binance:** a világ legnagyobb kriptotőzsdéje; a 2025-ös adatok szerint kb. 335 millió regisztrált felhasználó és 160 milliárd dollár körüli ügyféleszköz. A lopott összeg a DefiLlama szerint a tőzsde kb. 144 milliárd dolláros eszközállományának nagyjából 4%-a. Jelenlegi vezetői között Yi He társvezérigazgató; az alapító CZ már nem irányítja a céget, de a legnagyobb részvényes. (CoinDesk; The Week; TechCrunch)
- **TraderTraitor (más néven Jade Sleet, UNC4899, Slow Pisces):** az FBI által az észak-koreai állami hackerek közé sorolt csoport, amely kifejezetten kriptocégeket támad. Az FBI neki tulajdonítja a DMM Bitcoin (2024, 308 millió dollár) és a Bybit (2025, 1,5 milliárd dollár) elleni támadást. (BleepingComputer; The Hacker News)
- **Blokklánc-elemzők (Chainalysis, TRM Labs, Arkham, Blockaid) és stabilérme-kibocsátók (Tether, Circle):** ők követik a pénz útját, illetve fagyaszthatják be a saját tokenjeiket. Ez az a pont,

ahol a kriptovilág „mégis” tud hasonlóan reagálni egy bankhoz: a központilag kibocsátott stabilérmék befagyaszthatók, a bitcoin és az ether nem. (CoinDesk)

A minta nem új: a fejlesztő gépe a kapu. - **DMM Bitcoin, 2024:** a támadó toborzónak adta ki magát a LinkedInen, egy „felvételi kódolási teszttel” kártevőt futtatott egy tárcaszoftver-cég munkatársának gépén, ellopott munkamenet-sütikkel belépett a belső rendszerekbe, és egy legitim tranzakciós kérést manipulált. (BleepingComputer) – **megerősített** (FBI) - **Bybit, 2025:** a Safe{Wallet} egyik fejlesztőjének gépét törték fel, onnan a tárcaszolgáltató webes felületébe kártékony kód került, amely a Bybit következő tranzakcióját eltérítette. (The Hacker News) – **megerősített** - **A Security Alliance (SEAL) 2025-ös figyelmeztetése** szerint a csoport jellemzően hamis toborzói személyazonossággal keresi meg a gyártási (éles) vagy IT-hozzáféréssel rendelkező munkatársakat, kódtár-letöltéssel járó „technikai interjúval” juttat kártevőt a gépükre, majd napokig-hónapokig térképezi fel belülről, hol vannak a kulcsok és ki fér hozzájuk. (SEAL Radar – DPRK advisory) – **megerősített** (szakmai közösségi tanácsadás)

Fontos: a Binance-eset konkrét belépési módját (adathalászat, hamis állásajánlat, ellátási lánc vagy más) a Binance még nem közölte; a fenti esetek a csoport ismert módszereit mutatják, nem a mostani eset bizonyított menetét. – **feltételezés** (mintaazonosság)

Hogyan működik

> RED // TÁMADÓI SZEMMEL

Az eset legfontosabb tanulsága fogalmi: **nem a széf ajtaját törték fel, hanem a kulcstartó zsebét.** A tőzsdék a pénzt kulcsokkal védik, és a Binance szerint a kulcsok nem szivárogtak ki. A támadónak nem kellett ellopnia őket: elég volt bejutnia oda, ahol a rendszer *magától* aláírja és elküldi a kifizetéseket.

1. **Ember a láncban.** Egy DevOps-mérnök a munkája miatt hozzáfér az éles infrastruktúrához. Az ő gépe ezért a támadó szemében értékesebb, mint bármelyik ügyfélfiók. Az ilyen csoportok tipikusan hónapokig készülnek egy-egy kulcsember megközelítésére (hamis állásajánlat, tesztfeladat, „partner” üzenete). – **feltételezés** (ismert minta, nem a mostani eset igazolt menete)
2. **A gépről a gépházba.** A feltört laptopról a támadó egy belső szolgáltatáskonténerhez jutott, vagyis egy olyan programkomponenshez, amelynek „joga van” kifizetést indítani. (Binance Square)
3. **A rendszer saját kezével.** A konténerből beadott kifizetések a rendszer szemszögéből hivatalos kérések voltak: a kulcsok a helyükön maradtak, csak más mondta meg nekik, mit írjanak alá. Ezért a „nem szivárgott privát kulcs” egyszerre jó hír és figyelmeztetés: a kulcs védelme önmagában nem elég, ha a kulcsot használó folyamat eltéríthető.
4. **Gyorsaság és menekítés.** A pénzt rögtön szétosztották, váltották és fedezetként lekötötték, hogy a befagyasztható stabilérmék helyett nehezebben megfogható eszközökbe kerüljön. (CoinDesk)

Milyen gyengeségekre épít? - **Túl sok bizalom egy gépben:** ha egy munkatárs laptopja elég ahhoz, hogy valaki eljusson a kifizetésekig, a laptop a bankfiók kulcsa. - **Gépi jogosultság ellenőrzés nélkül:** egy automatizált szolgáltatás nagy összegű kifizetést indíthat; ha nincs független, emberi vagy külön csatornás jóváhagyás, a szokatlan kérés is átmegy. - **Hiányzó összeghatárok és lassítás:** egy több milliárdos kiáramlás csak akkor lehetséges, ha nincs olyan korlát, amely a szokatlan mennyiséget megállítja vagy késlelteti. Hogy a Binance-nél mi hibázott, még nem ismert. – **feltételezés**

A második hullám (a csalók oldala): a nagy rablások után a bűnözők a hírre építenek. 2025 februárjában, napokkal a Bybit-rablás után, Binance-ügyfelek a Binance valódi SMS-feladójának látszó üzenetet kaptak arról, hogy „Észak-Koreából léptek be a fiókjukba”; a visszahívott „ügyfélszolgálat” arra kérte őket, hogy pénzüket egy új, „biztonságos” tárcába utalják, amelyhez a csalóknak hozzáférése volt. (ForkLog; NCSC

Svájc) A másik visszatérő forma a „pénzvisszaszerző” csalás: hatóságnak, ügyvédi irodának vagy nyomozócégnek adja ki magát valaki, és előleget kér a „visszaszerzésért”. Az FBI szerint a hatóság nem kér pénzt a nyomozásért, és magáncég nem tud lefoglalást elrendelni. (FBI IC3) A Binance már az incidens első óráiban arra figyelmeztetett, hogy óvakodjanak a nem hivatalos linkektől és a fiókadatokat kérő megkeresésektől. (TechCrunch)

Hatás és magyar vonatkozás

- **Kár:** kb. 5,9–6,3 milliárd dollár, ebből kb. 3 milliárd befagyasztva; a végleges veszteség napok alatt derül ki. A Binance vállalta, hogy a felhasználók nem veszítenek; ha ez teljesül, a kárt a tőzsde viseli. (Binance Square; Fortune)
- **Érintett csoportok:** közvetlenül a Binance; közvetve az ügyfelek, akik a kifizetések szüneteltetése miatt átmenetileg nem férnek hozzá a pénzükhöz, és mindenki, akit a hírre épülő csalók megkeresnek.
- **Tágabb hatás:** ha az elemzői hozzárendelés helytálló, a lopott összeg egy szankciók alatt álló állam bevételét növeli; az FBI korábban a Bybit- és a DMM-rablást is ugyanennek a csoportnak tulajdonította. (The Hacker News – Bybit; BleepingComputer) – **feltételezés** (a mostani esetre)

Magyar vonatkozás: - **Magyar érintettség nem ismert.** A magyar sajtó (Portfolio, HVG, Fintech.hu, Cryptofalka) október 30-án beszámolt az esetről, de magyar felhasználókra, hazai hatóságra vagy hazai hatásra vonatkozó információt nem közölt. (Portfolio; HVG) - Az MNB, az NBSZ NKI vagy a rendőrség részéről az esethez kapcsolódó figyelmeztetést 2026. október 30-ig nem találtunk. - A kockázat itthon is a második hullám: a magyar kriptótulajdonosokat is elérhetik magyar nyelvű, „Binance-ügyfélszolgálat”, „kártérítés” vagy „pénzvisszaszerzés” ürügyű hívások, SMS-ek és hirdetések. Konkrét magyar esetről még nincs tudomás. – **feltételezés** (a korábbi nemzetközi minták alapján)

Mit tegyél

> `BLUE // MIT TEGYÉL MOST`

Magánszemély (ha van kriptód, akár Binance-en, akár máshol): - **Ne utalj semmit „biztonságos tárcába”**, bárki kéri. Valódi tőzsde soha nem kéri, hogy a pénzedet egy általa megadott vagy most létrehozott tárcába mozgasd. (NCSC Svájc) - **Ne hívj vissza SMS-ben vagy e-mailben kapott számot**, és ne kattints az üzenetben kapott linkre; a tőzsde alkalmazásában vagy a kézzel beírt hivatalos címen nézd meg az értesítéseket. A hamis SMS ugyanabban a beszélgetésben is megjelenhet, mint a valódi. (NCSC Svájc) - **A kártérítéshez nem kell semmit tenned.** A Binance a SAFU-ból és saját forrásból vállalta a veszteség fedezését; ha valaki „kártérítési regisztrációért”, „feloldási díjért” vagy „ellenőrzésért” kér adatot vagy pénzt, az csalás. (Binance Square) - **„Pénzvisszaszerző” cégnek ne fizess.** A hatóság nem kér pénzt, magáncég nem tud lefoglalást elrendelni. (FBI IC3) - **Senkinek ne adj távoli hozzáférést** a gépedhez vagy a telefonodhoz, és ne mondd meg a visszaállító kifejezést (seed phrase), a jelszót vagy a 2FA-kódot. - **Ne pánikolj:** a kifizetések átmeneti szünetelése nem jelenti, hogy a pénzed elveszett; a hivatalos csatornákon kövesd a frissítéseket, és ne a közösségi médiában keringő számokra hallgass. (Cyber Security News) - **Hosszabb távon:** amit nem kereskedésre használsz, azt ne tartsd tőzsdén; ha saját tárcát használsz, a visszaállító kifejezést tartsd offline.

Kisvállalkozás (ha fejlesztőkkel, üzemeltetőkkel dolgozol): - **A rendszergazdai vagy éles hozzáféréssel rendelkező gép külön kategória:** ne legyen rajta magáncélú böngészés, ismeretlen tesztfeladat vagy letöltött kódtár futtatása. (SEAL Radar) - **Tudatosítsd a munkatársakban** a hamis állásajánlatos trükköt:

aki „felvételi tesztként” kódot kér futtatni, az gyanús. (BleepingComputer) - **Pénzmozgásnál két kulcs:** nagy összegű utalás vagy kifizetés ne induljon egyetlen ember vagy egyetlen gép döntésére; legyen összeghatár és második jóváhagyó, külön csatornán.

Szervezet: - **Kezeld a kulcsemberek végpontjait koronaékszerként:** EDR, szoftver- és böngészőbővítmény-leltár, rendszeres átvizsgálás; nézd át, kerestek-e gyanús „toborzók” éles hozzáférésű munkatársakat. (SEAL Radar) - **A kulcs védelme nem elég, a kulcsot használó folyamatot is védeni kell:** a kifizetést indító szolgáltatásoknál legyen független jóváhagyás, összeg- és sebességkorlát, és automatikus megállítás szokatlan mintánál. - **Fejlesztői gépről ne legyen közvetlen út az éleshez:** dedikált, elszigetelt adminisztrációs munkaállomás, rövid életű, feladathoz kötött jogosultság, munkamenet-sütik és tokenek védelme. (BleepingComputer) - **Aláírásnál független ellenőrzés:** a jóváhagyó a tranzakció adatait egy külön eszközön (pl. hardvertárcán) is ellenőrizze, ne csak a böngészőfelületen; teszteld szokatlan próbatranzakciókkal, hogy a jóváhagyók észreveszik-e. (SEAL Radar) - **Készülj a második hullámra:** egy nagy incidens után előre megírt ügyfélkommunikáció („így keresünk, és így soha”), a hivatalos csatornák egyértelmű megnevezése, és a kiadott figyelmeztetések ismétlése. (TechCrunch)

Szakmai blokk

- **CVE:** nincs; a Binance nem nevezett meg sebezhetőséget. Az eset jelenlegi ismeretek szerint végpont-kompromittálásra és belső hozzáféréssel való visszaélésre épül. (CyberInsider)
- **Érintett komponens:** a Binance kifizetési szolgáltatása és egy belső szolgáltatáskonténer; a cég a kifizetési szolgáltatást és a kapcsolódó címeket átalakítja. (CyberInsider)
- **MITRE ATT&CK (szerkesztői leképezés, a csoport ismert módszerei és a közölt lánc alapján – feltételezés):**
- T1566 Phishing / T1204 User Execution (álláshirdetéses csali, kódolási teszt – a csoport ismert módszere, a mostani esetben nem igazolt);
- T1539 Steal Web Session Cookie, T1550 Use Alternate Authentication Material (a DMM-esetben igazolt);
- T1078 Valid Accounts (a mérnök hozzáférésének felhasználása);
- T1021 Remote Services / T1610 Deploy Container jellegű mozgás a konténerkörnyezet felé;
- T1657 Financial Theft (jogosulatlan kifizetések).
- **Észlelési ötletek (fogalmi):**
- kifizetési kérések, amelyek nem a megszokott belső forrásból vagy ütemezésből érkeznek; összeg- és darabszám-anomália rövid időablakban;
- adminisztrátori végpontokon új, ismeretlen kódtár futtatása, szokatlan böngészőbővítmény;
- ugyanazon munkamenet-azonosító szokatlan helyről vagy eszközről;
- konténerkörnyezetbe belépés fejlesztői gépről, munkaidőn kívül vagy változtatási jegy nélkül.
- **Hivatalos ajánlások, háttér:** FBI-közlemények a TraderTraitorról (DMM Bitcoin, Bybit); a SEAL 2025. februári DPRK-figyelmeztetése; az FBI IC3 figyelmeztetései a pénzvisszaszerző csalásokról. (BleepingComputer; SEAL Radar; FBI IC3)
- **Indikátorok:** típus szerint támadói blokklánc-címek, amelyeket blokklánc-elemzők (Arkham, Chainalysis, TRM Labs) és a Binance követ; hivatalos, összesített IOC-listát 2026. október 30-ig nem tettek közzé.

Ellentmondások és nyitott kérdések

Nyitott kérdések

- **6,3 vagy 5,9 milliárd?** A Binance a „becsült teljes hatást” közli, a Chainalysis a lopás pillanatára vonatkozó piaci értéket; a korai beszámolók 1,7 és 8 milliárd dollár között szórtak. Ezért ez az anyag így fogalmaz: „kb. 6 milliárd dollár, a Binance szerint 6,3, a Chainalysis szerint 5,9 milliárd”. (Fortune; The Hacker News)
- **Mennyi a befagyasztott összeg?** A Binance „kb. 3 milliárdot” közöl, a Cyber Security News szerint a Binance által igazoltan befagyasztott összeg 2,54 milliárd dollár volt egy korábbi frissítésben; a különbség a gyorsan változó állapotból adódhat. (Cyber Security News)
- **Befizetések:** egyes források szerint be- és kifizetés is szünetel (HVG, Binance Square első közlése), mások szerint a befizetések már újraindultak (CyberInsider, The Week, Portfolio). A későbbi állapot a befizetések újraindulása.
- **Hogyan törték fel a laptopot?** Nem ismert; a Binance post-mortemet ígér.
- **Ki volt?** A TRM Labs hozzárendelése elemzői értékelés; hatósági (pl. FBI) megerősítés október 30-ig nincs, és a Binance nem nevezett meg elkövetőt.
- **Visszaszerezhető-e a nem befagyasztott rész?** Nem ismert; a bitcoin és az ether nem fagyasztható be központilag.
- **Mikor indulnak újra a kifizetések?** A Binance becslése 48 óra, de ezt maga is becslésnek nevezi.

Forrásértékelés

Forrás	Típus	Megbízhatóság	Mit támaszt alá
Binance Square – Binance News	cég (elsődleges összefoglaló)	magas (a saját állításairól)	6,3 milliárd, 3 milliárd befagyasztva, DevOps-laptop, privát kulcs, SAFU, post-mortem
CoinDesk	sajtó	magas	Chainalysis-becslés, Tether/Circle, Arkham-egyenlegek, Aave, TRM-hozzárendelés, piac
The Hacker News	sajtó	közepes–magas	Chainalysis 5,912 milliárd, Arbitrum, támadási lánc
CyberInsider	sajtó	közepes–magas	befizetés vissza, kifizetés szünetel, 48 óra, TraderTraitor (TRM)
Fortune	sajtó	magas	korai becslések, eszközmegoszlás, nyitott kérdések
TechCrunch	sajtó	magas	első órák, CZ, Binance csalásfigyelmeztetés, Polymarket
The Week	sajtó	közepes	állapot okt. 30., piac, háttér
Cyber Security News	sajtó	közepes	2,54 milliárd igazolt befagyasztás, SAFU mérete, Ripple
Portfolio	sajtó (HU)	közepes–magas	magyar sajtóvisszhang, befagyasztók, 48 óra
HVG	sajtó (HU)	közepes–magas	magyar sajtóvisszhang, TRM-hozzárendelés
The Hacker News – Bybit	sajtó	magas	Bybit-előzmény, FBI-hozzárendelés
BleepingComputer – DMM Bitcoin	sajtó (FBI-közlés alapján)	magas	TraderTraitor módszere: hamis toborzó, kódolási teszt, munkamenet-eltérítés
SEAL Radar – DPRK advisory	kutató (szakmai közösség)	magas	DPRK-taktikák, védekezési ajánlások
FBI IC3 – PSA230811	hatóság	magas	pénzvisszaszerző csalások, piros zászlók

Forrás	Típus	Megbízhatóság	Mit támaszt alá
NCSC Svájc – Binance SMS-csalás	hatóság	magas	„biztonságos tárca” csalás mechanizmusa, tanácsok
ForkLog	sajtó	közepes	Bybit utáni „Lazarus”-ürügyű csalás (2025. feb.)