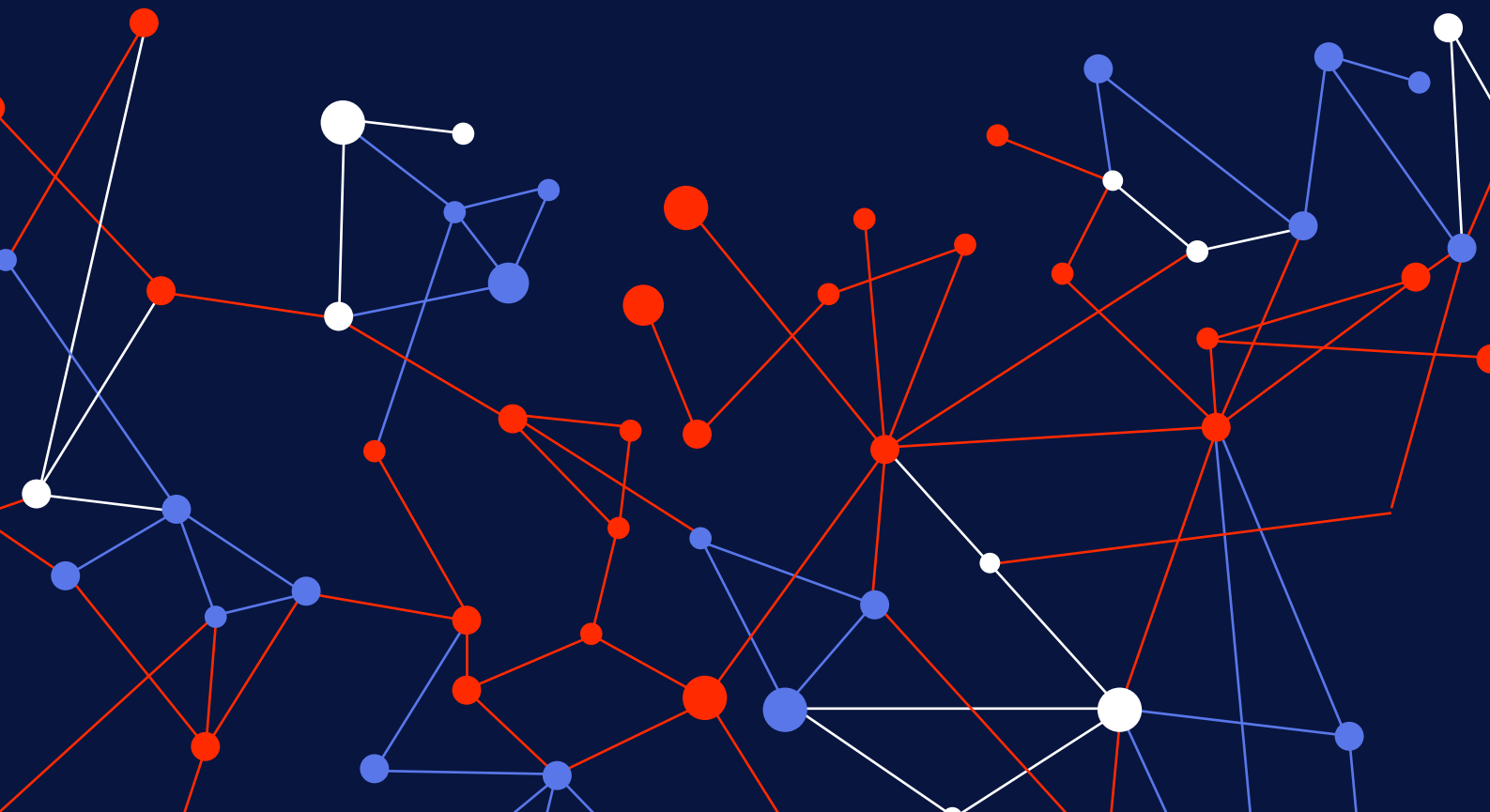
GLOBAL LEDGER

2025 Laundering Race Report

255 Crypto Hacks Analysis



Key Takeaways

1

$4.04B
Stolen in 2025

2

255
Hacks in 2025

3

2 sec
The fastest 1st funds move

4

x2
Speed of 1st funds move in H2'25 vs H1'25

5

~76%
Moved funds before the public report

6

~50%
Funds remain unspent, waiting to be laundered

7

~42%
Tornado Cash used in ~ ⅖ of cases

8

~7%
Returned

Executive summary

An H1–H2 breakdown of 2025 hacks shows that attackers are getting faster. In 2025, the first movement of stolen funds happened in as little as 2 seconds—**twice as fast as in H1 2025** and 2x faster than the quickest public incident disclosure. In practice, this means attackers were already **moving assets before the market even knew a hack had occurred.**

In **~76%** of hacks in 2025, funds moved before public reporting. The victims began reacting faster, too, compressing the average response window by ~2.1× in H2 and making bad actors slow down. In H1, hackers needed an average of ~8 days for laundering; in H2, 10.6 days. This shift reflects more **staged, fragmented laundering**, with smaller chunks, longer timelines, and more intermediaries. These techniques were present before, but their use expanded and intensified in H2.

The speed of laundering in 2025 came on top of much bigger losses: **$4.04B** stolen in 2025, up **by ~2.1×** from $1.94B in 2024, even though the number of hacks grew by only ~4%. Much of the damage—over 36%—was caused by the Bybit hack, accounting for $1.46 billion stolen.

This report from Global Ledger is the only industry study that analyzes the timing of crypto hacks. Breaking down these timelines, it reveals patterns others miss: how fast attackers move and where defenses fail.

Methodology

This report is built on **time-based tracing** and analysis of 255 hacks from 2025, laundering timing, gaps between incidents, public disclosure, funds movements, and obfuscation.

Data sources

The report's primary foundation is on-chain tracing of addresses associated with hacks using the Global Ledger proprietary KYT solution and an extensive entity database. These results were cross-referenced with open-source reporting, including official disclosures by affected projects, media coverage, and blockchain security research.

Scope

For this research, we define VASPs and mixers as endpoints, i.e., the points where illicit funds enter services that sharply reduce traceability. Once the last funds reach these endpoints, we consider further on-chain tracing non-decodable due to obfuscation, custodial pooling, or jurisdictional limits.

This definition ensures consistency in measuring laundering speed and behavior across cases. While deeper tracing is technically possible, it often carries a high risk of error and falls outside the scope of this analysis.

Each half-year is analyzed based on on-chain activity and disclosures available within that respective period.

Key Terms

Incident
Moment the hack occurred

Report
Time the incident was publicly disclosed

1st move
The first movement of stolen funds from the hacker's wallet

1st VASP/mixer deposit
The first deposit to a VASP or mixer

Last VASP/mixer deposit
Last funds reached VASP/mixer, after which tracing becomes non-decodable.

Limitations

As with all crypto crime research, several limitations apply. Not all hacks are publicly reported, and some remain undisclosed by affected projects. Attribution of attacks to specific actors, such as state-sponsored groups, is based on the best available evidence but cannot always be independently verified. Laundering flows may extend beyond the endpoints included here, but attribution beyond those points carries significant uncertainty.

Hackers set a record in the fastest cases of H2 2025, moving funds 2× faster than in H1

In 2025, crypto crime became faster, leaving less time for victims to react. In H2 2025, laundering was even quicker than in H1 and reached new extremes. In the fastest case, funds moved in just **2 seconds—twice** as fast as in H1 2025. This is also **2× faster** than the quickest public incident reporting.

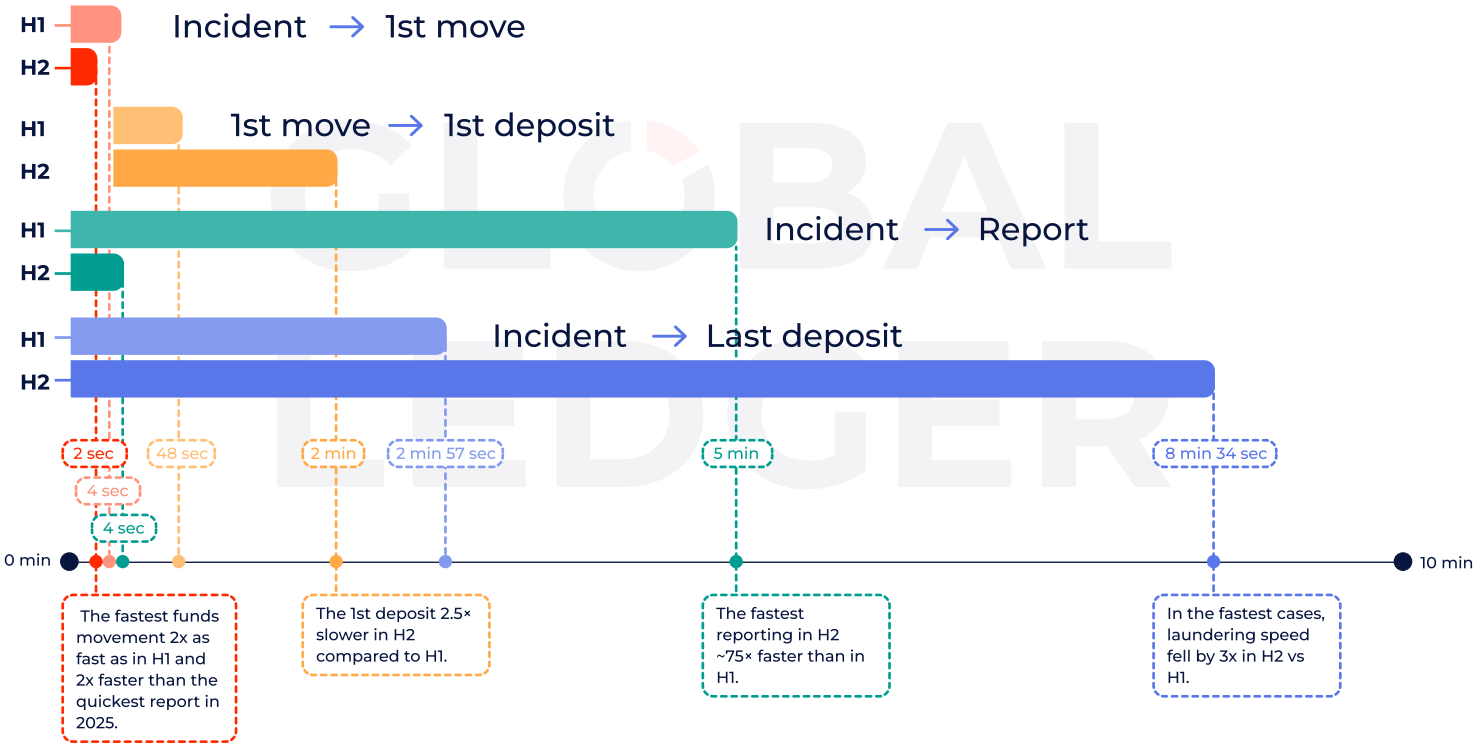
In practice, this means that in most cases, attackers were already moving funds before the market even knew a hack had occurred. On average, this happened in **~76.4%** of incidents across 2025. The share increased sharply in H2 to 84.6%, up from 68.1% in H1 2025.

On average, in H2 2025, attackers were **11 hours 13 minutes and 16 seconds** ahead of **public reporting**. In H1 2025, this gap was 23 hours 14 minutes and 18 seconds, meaning the average **disclosure gap narrowed by ~2.1×** in H2.

Once funds started moving, they quickly reached obfuscation layers. In H1 2025, the fastest time from the first move to the VASP/mixer was **48 seconds,** while in H2 2025, it slowed to 2 minutes—**2.5× slower**.

In the fastest case of H1, the last funds reached VASP/mixer in 2 minutes 57 seconds. In H2, it took 8 minutes 34 seconds to launder funds, which is **nearly 3× slower**. However, in the H1 fastest case, the amount laundered was 5.6× smaller, and the laundering occurred in a single step. The H2 case involved larger sums and more staged movement, extending the laundering timeline.

Hackers set record in the fastest cases, moving funds 2× faster in H2



Closing the response gap requires a shift from ad-hoc reactions to continuous monitoring, standardized reporting, and proactive incident response

There are a few key steps to closing this response gap. First, Web3 projects must implement real-time on-chain and off-chain security monitoring to detect suspicious behavior and anomalies as they happen. Without internal detection and alerting, no external ecosystem response can move fast enough.

Second, the industry needs a widely adopted standard for incident reporting. Initiatives like SEAL911 already provide an effective emergency hotline for coordinating response and asset recovery, but too many projects still approach incident response reactively rather than proactively.

Closing the response gap ultimately requires a shift from ad-hoc reactions to continuous monitoring, standardized reporting, and proactive incident response, so defenders can operate at the same speed as attackers.

Yev Broshevan

CEO & Co-Founder at Hacken

Hackers have 2× less time for “quiet” laundering

The share of hacks with pre-disclosure fund movements increased by roughly ~42% compared to H1. Meanwhile, hack victims began reporting faster, leaving less time for hackers for quiet laundering, which could have reduced exposure to freezes and alerts triggered after public reporting.

Disclosure of an incident triggers a **coordinated response** across the ecosystem. AML tools providers label malicious addresses, after which compliance teams can block related flows. As a result, attackers have 2× less time and fewer opportunities to launder funds quietly. This effect is reinforced by a growing network of independent watchdogs and community investigators, who collaborate to identify, flag, and disrupt laundering linked to major incidents.

> **Integrating high-speed community alerts can be valuable if the data is verified**
>
> Integrating high-speed community alerts can be valuable, but only if the data is verified by a credible party. Otherwise, such systems risk abuse. Labels must be evidence-based or not applied — full stop. Probabilistic or insight-driven layers can exist, but they belong to investigators, not compliance workflows.

Richard Sanders

Investigator, volunteer for Ukraine

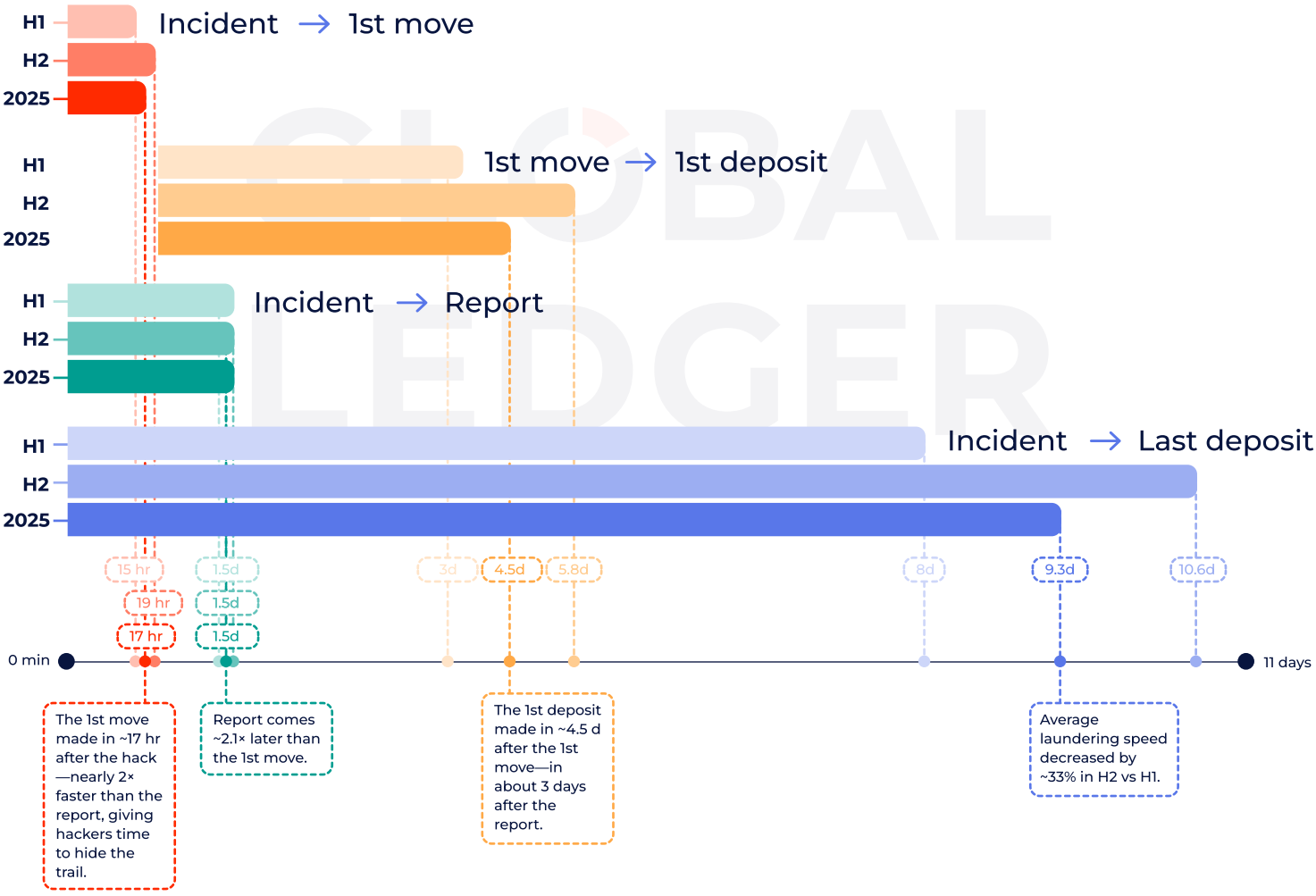
Average laundering speed fell by ~25% in H2

The average time from a hack to the first movement of funds was **~17 hours** (15 hours in H1 and nearly 19 hours in H2). Typically, stolen funds reach the first mixer/VASP in about **5.2 days** after the incident (with cases in H2 about **1.8× slower**).

In **~28.2%** of cases, the last deposit was made **within a single day.** In 41.5% of hacks, it was made within one week, and in 50.4%, in under 29 days. Only 5.8% took longer than one month. Across all these thresholds, H2 showed a slowdown of several percentage points compared to H1.

In about **19.6% of cases**, all the stolen funds reached the last deposit before the hack was publicly disclosed (22.7% and 16.9% in H1 and H2, respectively). On average, hackers needed **~9.3 days** to send all stolen funds to the last deposit. In H1 2025, it took them around 8 days, and in H2 2025, they laundered funds in 10.6 days.

On average, the report comes ~2.1× later than the 1st move



Exploits run as a sprint, while laundering drags hackers into a marathon

While hackers are faster at the start, the overall time of laundering has slowed to 10.6 days in H2. Attackers are now using more staged movements, smaller chunks, and fragmented paths through DeFi and bridges to avoid detection.

The data suggests that while hackers are winning the ‘sprint’ at the moment of the exploit, they are being forced into a ‘marathon’ for actual laundering due to better ecosystem visibility.

Slower laundering favors investigators if monitoring is continuous, automated

The slowdown of illicit funds indicates a shift toward more ‘patient’ laundering strategies. This slower pace gives investigators more time to map relational networks, freeze wallets early, and coordinate actions across jurisdictions before funds are dispersed. However, taking advantage of this opportunity requires continuous, automated monitoring—something most legacy compliance frameworks lack.

Mudassar Malik

CEO and founder of Deconflict.com

Multi-stage laundering, used in ~99% of hacks, extended timelines

Hackers respond with more **deliberate, staged laundering**. In H1 2025, we observed three hacks (2.5%) where all funds went to VASP/mixer within the first move. In H2 2025, there were no such cases. Staged and fragmented laundering was already used before, but in H2 it became more common, with funds spread across many smaller transfers. This fragmentation correlates with longer laundering timelines.

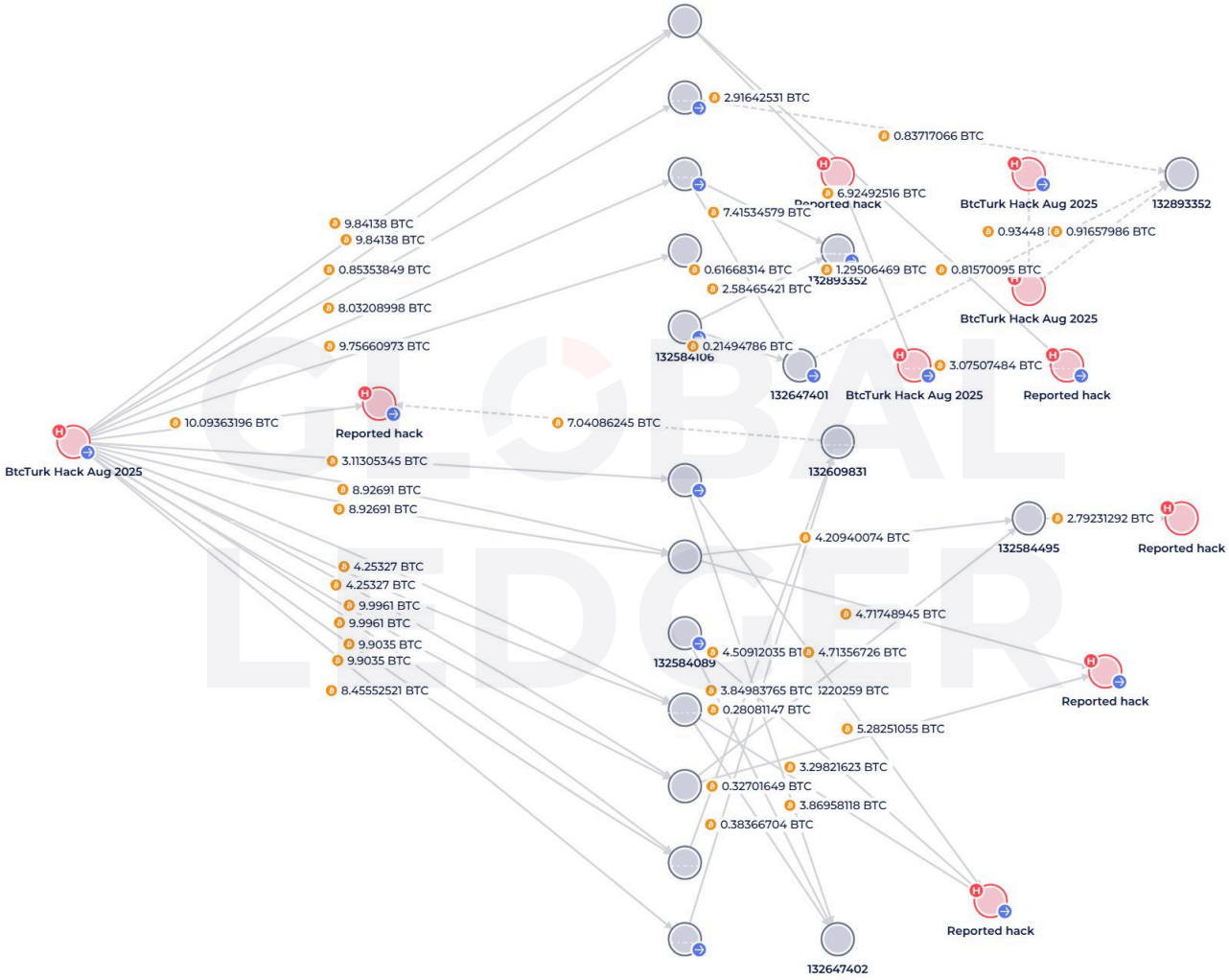
1. The process typically begins with initial funds **fragmentation**, where balances are broken into many smaller transfers distributed across multiple unhosted wallets.
2. The next stages typically involve obfuscation services such as **mixers,** as well as decentralized infrastructure—**cross-chain bridges, DEXs, and instant swap services** —which significantly increases the complexity of tracing stolen funds. Here, unhosted wallets also remain a core component of the flows—as intermediate staging and routing points between phases.
3. **‘Cash-out’** is often intentionally **delayed** until monitoring intensity declines. In many cases, a portion of stolen funds remains inactive for extended periods. This waiting behavior is a trade-off: longer timelines in exchange for lower exposure to freezes, sanctions screening, or law-enforcement actions.

BtcTurk hackers routed stolen bitcoins via unhosted wallets, CoinJoin, Wasabi, and Lightning Network

BtcTurk ~$48 million hack is an example of a deliberate, staged laundering, likely carried out by DPRK hackers. In August 2025, the exchange suffered a security breach that resulted in the theft of ETH, BTC, BASE, ARB, OP, POL, AVAX, zkSync, MANTLE, and Moonbeam from its hot wallets. BtcTurk reported that most user funds were safe in cold storage, but on-chain data confirmed that millions of dollars in BTC were transferred to attacker-controlled wallets soon after the breach.

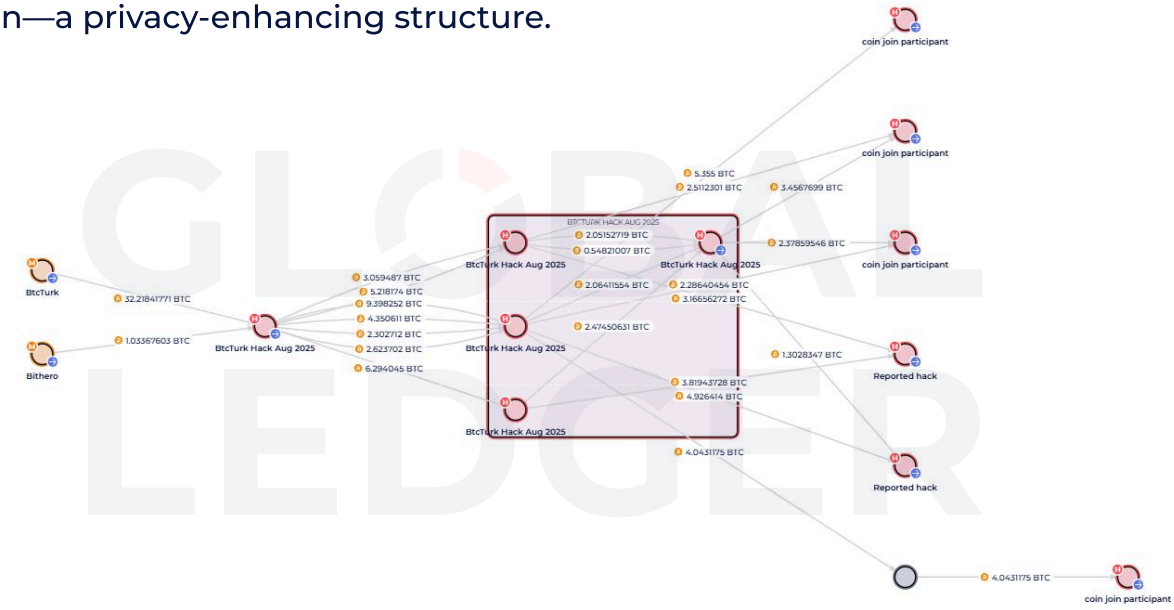
The multistage scheme used for laundering included:

- Routing funds through a chain of unhosted wallets



BtcTurk hackers sending part of stolen funds to a chain of self-hosted wallets. Screenshot from the Global Ledger KYT tool

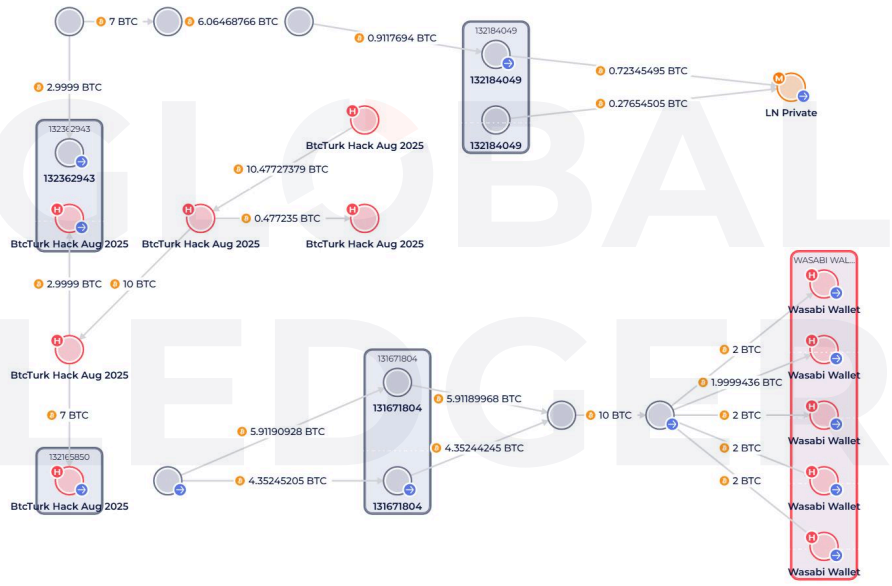
- Further concealing the origin of funds by sending them to CoinJoin—a privacy-enhancing structure.



BtcTurk hackers sending part of stolen funds to CoinJoin.
Screenshot from the Global Ledger KYT tool

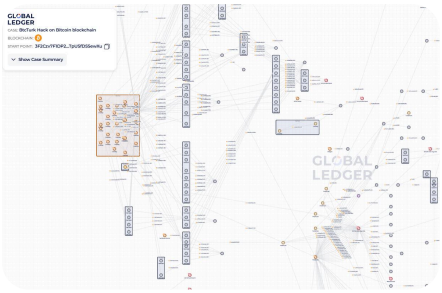
- Using THORChain, Wasabi Wallet, Chainflip, and the Lightning Network to further obscure the transaction trail.

Lightning Network is a Bitcoin Layer-2 network designed to improve transaction speed and reduce fees while enhancing user privacy. By routing payments off-chain and limiting visibility to participating nodes, it hides on-chain trails. Attackers leverage these features to further obscure transaction trails.



BtcTurk hackers sending part of stolen funds to the Lightning Network and Wasabi Wallet.
Screenshot from the Global Ledger KYT tool

These layered methods are meant to make tracing harder. They show that illicit actors understand how investigations work and deliberately act to complicate tracking and attribution.



Review how funds moved

Check the case online

Staged laundering erodes traceability step by step

The BtcTurk case illustrates how attackers rely on staged execution rather than speed. The combination of self-hosted wallet chains, mixing, cross-chain routing shows a deliberate, well-orchestrated scheme where each step is designed to gradually weaken traceability, complicate clustering and attribution. Instead of a linear path to a VASP or cash-out point, attackers construct layered routing paths that degrade analytical certainty.

Effective response to sophisticated attacks requires rapid-response protocols, cross-jurisdictional coordination, and advanced tracing capabilities

The extended timeline creates intervention opportunities, but success depends heavily on attacker sophistication. Less experienced threat actors, increasingly entering crypto crime aided by AI tools, often lack efficient laundering knowledge, giving recovery teams time to compile evidence packages and coordinate with service providers.

However, sophisticated attackers deliberately slow the process strategically. They split funds into tranches, route through privacy tools like Tornado Cash, or hold assets during unfavorable market conditions to reduce traceability and test laundering strategies.

Success requires operational readiness other than just having sufficient time: established rapid-response protocols, strategic networks spanning jurisdictions and service providers, and technical capabilities to track complex fund flows. The marathon phase alone doesn't guarantee better outcomes without proper infrastructure to exploit it.

Marcin Zarakowski

CEO of Recoveris

Collecting information on the counterparties is key to countering these risks. The most robust mechanism to verify a self-custodial wallet owner is AOPP, which relies on a cryptographic signature, which can only be provided by the holder of the appropriate private key. When it comes to transactions between VASPs, the mandatory collection of user identities—facilitated by global industry-standards like TRUST and TRP—enables both recipient and originator institutions to decide whether to engage with a counterparty (be it the correspondent entity or transacting person) before the transfer of funds is completed. These can inform the VASP's own sanction controls and support flagging inconsistencies that point to suspicious activity.

Hannah Zacharias

Head of Regulatory Affairs at 21 Analytics

Hackers sent 3× more to bridges than mixers in 2025

In 2025, over **$2.01 billion** of stolen funds were routed through **bridges**—nearly 49.75% of total losses and over 3× more than via mixers and privacy protocols. In H1, over $1.5 billion was cross-chained, while in H2, this volume **declined by nearly 3×** to $510.64 million.

Moving funds cross-chain now comes with a lot more visibility and risk

Today, analytics providers are much better at pulling data across chains and understanding how bridges actually move value. From our side, we try to make this as clear as possible. We run a public explorer where anyone can see where funds are coming from and where they go. Transparency is important.

We also check transactions with several AML providers before they go through. We don't believe bridges should decide on their own which addresses are good or bad. That's a job for specialists like Global Ledger. Because of this, bridges just aren't an easy option for attackers anymore. Moving funds cross-chain now comes with a lot more visibility and risk than it used to.

Andriy Velykyy

CEO and co-founder of Allbridge

~50% of funds stolen in 2025 were cross-chained

Bridges are leveraged by bad actors for large-scale laundering, with almost **½ of the funds** stolen in 2025 **cross-chained**. This dynamic was evident in the Bybit incident, where $1.38 billion (94.91% of the funds stolen in this hack) moved through bridges.

Operating as permissionless smart contracts, **many cross-chain protocols are not designed to detect or freeze** illicit flows. Bad actors use them to move stolen assets between chains quickly, evade sanctions and KYC, and mask the origins by combining multiple technologies, such as bridges, aggregators, swap pools, mixers, and private networks.

Bridges are motivated to filter suspicious activity early

In reality, it's often simpler for attackers to use low-quality exchanges, OTC desks, or informal networks, where controls are weak or mostly just for show. With bridges, the cost of being associated with bad flows is much higher.

We also see a shift toward simpler ways of moving value, especially for stablecoins. Models like Circle's CCTP or LayerZero's OFT make it cheaper and more predictable to move liquidity across chains, with very little slippage. That's great for users. At the same time, these flows rely on centralized stablecoins. And that matters, because if something goes seriously wrong, issuers can step in and freeze assets. That makes these routes much less attractive for hackers, who don't want that kind of uncertainty.

Andriy Velykyy

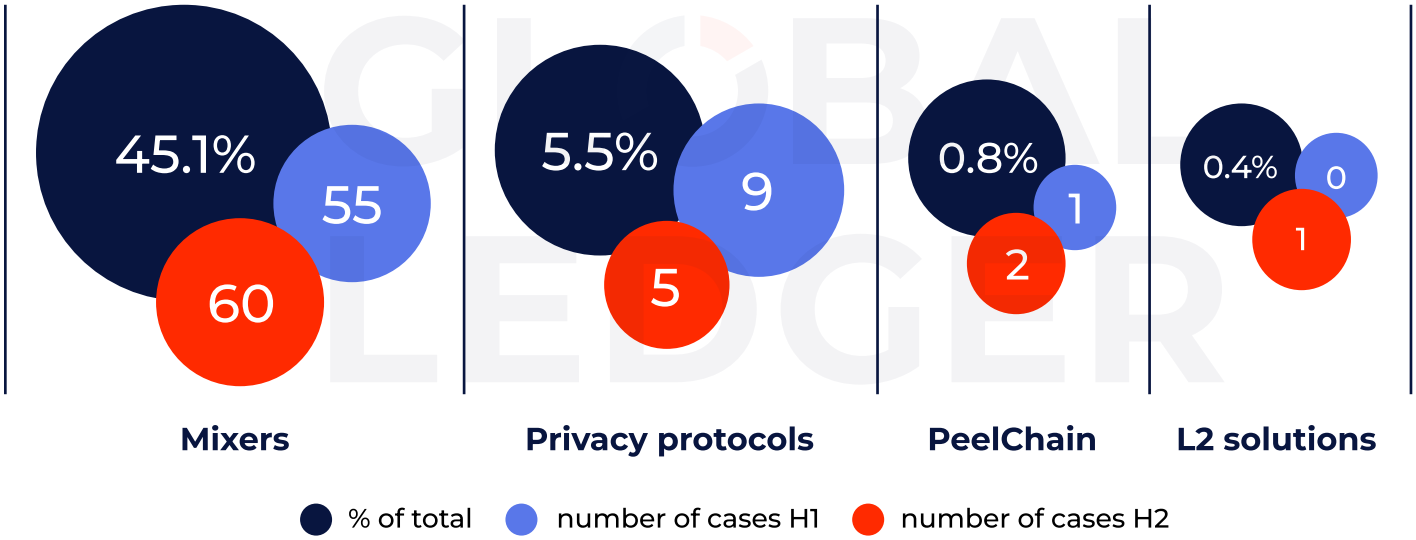
CEO and co-founder of Allbridge

Tornado Cash usage rose by over 31 p.p. following the lifting of sanctions

Mixers and privacy protocols often follow bridges as the next step in hiding final recipients. In 2025, **650.1 millio**n were routed via them, with a decline of roughly 8% half-over-half.

Mixers were used in **45.1%** of all hacks, privacy protocols account for 5.49%, peel chains for 0.78%, and L2 solutions for 0.39%.

Mixers used in 45.1% of all hacks in 2025



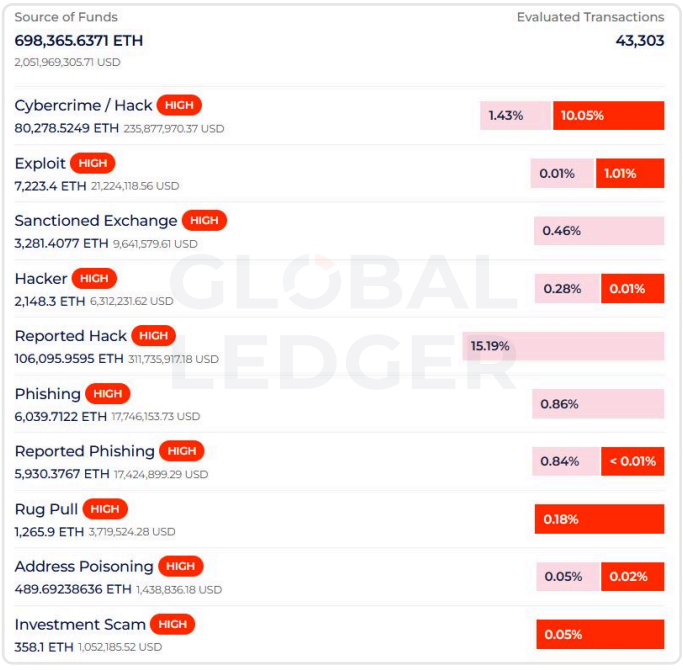
Tornado Cash leads the chart in terms of popularity among crypto mixers, used in **41.57%** of all hacks (115 of 255) in 2025.

Its usage increased sharply in H2. Its share rose from 42.9% of cases in H1 to 74.3% in H2—a **31.4 percentage-point increase.** After sanctions were lifted in March 2025, the mixer became more accessible again, which resulted in its wider use, including in laundering activity.

In 2025, Tornado Cash received over $2.05 billion on Ethereum

In 2025, Tornado Cash received over $2.05 billion on Ethereum, with ~654.98 million coming from high-risk activity, such as scams, hacks, phishing, high-risk exchanges, etc.

In 2025, Tornado Cash received $2.05B+ on Ethereum, with ~654.98M from high-risk activity



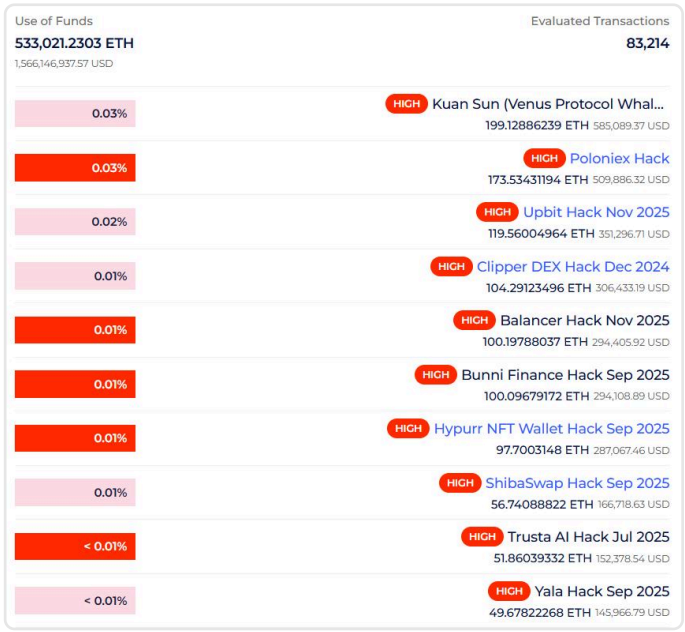
Screenshot from the Tornado Cash entity exposure report. Jan 1-Dec 31, 2025. Global Ledger

During 2025, the total volume of outgoing transactions from the mixer reached **$1.57 billion;** about 155.55 million went to high-risk addresses. Nearly the same volume of funds (~154.2 million) was sent to low-risk addresses.

Tornado Cash has become a critical component of hacker infrastructure

Funds leaving Tornado Cash move to wallets controlled by the same malicious actors involved in earlier hacks, e.g., incidents from 2023-2024. These include the Poloniex hack from November 2023, when ~$132 million worth of crypto was stolen (valued at the time of the incident), and the Clipper DEX hack from December 2024, with ~$450,000 in losses.

Funds from Tornado Cash went to wallets linked to hacks from 2023-2024



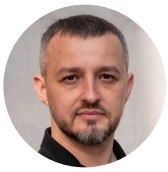
Screenshot from the Tornado Cash entity exposure report. Jan 1-Dec 31, 2025. Global Ledger

The share of funds sent from Tornado Cash to CEXs increased after sanctions were lifted

Before sanctions were lifted (January–March 20, 2025), CEXs received ~$278,470 from Tornado Cash (**0.16%** of its total outgoing transactions). After the lifting of sanctions (March 21-December 31, 2025), ~$66.7 million from Tornado Cash to CEXs (**4.74%**). Notably, eight of these exchanges are ranked **among the top 10** by trading volume on CoinMarketCap.

While the absolute volumes in the pre-sanctions period are relatively small (reflecting a much shorter observation window), the rise of the share of funds sent to CEXs is notable. It suggests that the lifting of sanctions may have made it easier for hackers to route funds to exchanges for cash-out.

> The dramatic surge in Tornado Cash usage—from 42.9% to 74.3% of cases following the lifting of sanctions—presents a significant national security challenge. This resurgence highlights how quickly state-sponsored actors, such as the Lazarus Group, exploit any perceived regulatory softening to smooth their laundering operations.
>
> As Ukraine aligns its legislation with MiCA (Markets in Crypto-Assets) standards, we are championing a model of 'Accountable Transparency'. We respect the right to financial privacy, but the fact remains that when a single mixer handles nearly 75% of illicit flows, it becomes a systemic risk to the integrity of the financial system. Our 2026 strategy involves implementing advanced de-anonymization tools for privacy-enhancing protocols and mandating that VASPs apply strict enhanced due diligence for any assets originating from non-compliant mixers. In the post-sanction era, our mission is to ensure that Ukraine's legalized crypto-market is a fortified environment where illicit assets are identified in milliseconds, regardless of the obfuscation layers applied.



Oleksandr Plakhotnyuk

Chief of Division for Combating Crimes Related to Virtual Assets at the Cyberpolice Department of the National Police of Ukraine

In H2, Tornado Cash was used in ~75% of cases

Attackers still rely on a **single, well-known mixer** instead of using several, getting sufficient obfuscation at a lower cost. Additionally, popular mixers attract more volume, making individual transactions harder to distinguish from the crowd.

This dynamic is clearly visible in the case of Tornado Cash, which remained the most widely used mixer in 2025. Its share of laundering cases rose from 42.9% in H1 to nearly **75% of cases** in H2, following the lifting of sanctions.

When restrictions eased, funds originating from Tornado Cash were no longer automatically flagged or blocked, and exchanges largely stopped receiving sanctions-based alerts tied to the protocol, as it was removed from sanctions lists. With fewer compliance barriers, laundering flows became smoother and cash-out easier.

Tracing must shift to probabilistic and behavioral-based clustering models

The data shows that the revocation of sanctions on Tornado Cash has led to a resurgence of legacy mixers within illicit financial ecosystems. It means that tracing methodologies must shift from static blacklist-based systems toward probabilistic and behavioral-based clustering models. Investigators should incorporate temporal transaction analysis, mixer inflow–outflow correlation, and cross-protocol entity linking to map disguised capital flows. Empirical evidence supports that machine-learning–based signature detection significantly reduces false negatives, especially when integrated with real-time intelligence feeds from law enforcement and commercial APIs.

Mudassar Malik

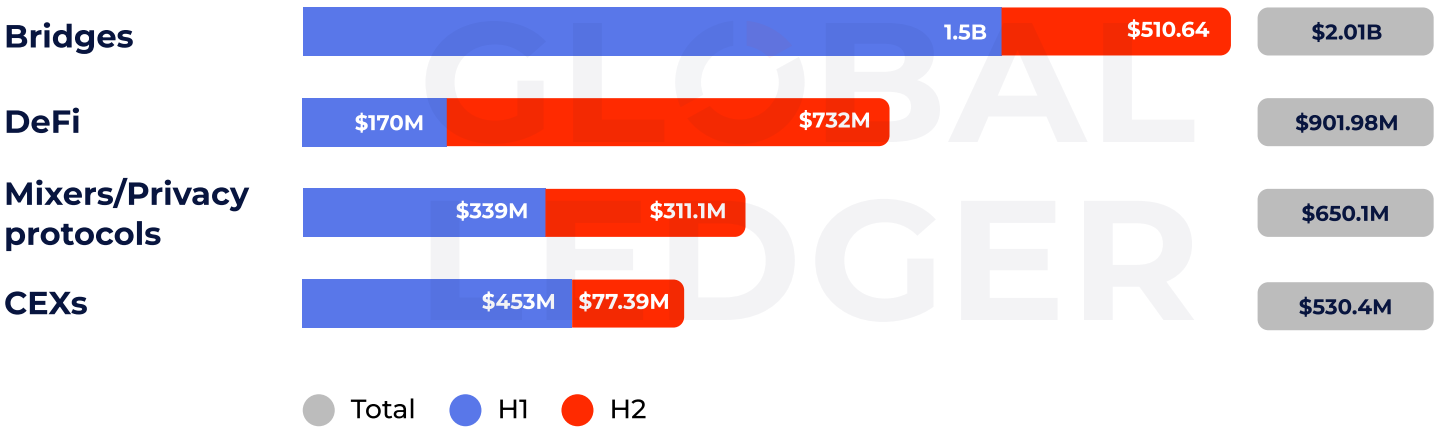
CEO and founder of Deconflict.com

Funds from hacks sent to CEXs fell 5.9× in H2

Over **$901.98 million** (~22.3% of total) was sent to the **DeFi ecosystem** post-hack, with H2 volumes (~$732 million) exceeding H1 ($170 million) by more than **4.3×**, making DeFi platforms the #2 laundering route by year-end.

Centralized exchanges showed the opposite trend: H2 inflows **fell nearly 5.9×** compared to H1 ($77.39 million vs $453 million), bringing the total sent to CEXs in 2025 to **~$530.39 million.**

In 2025, ~50% of stolen funds bridged



Attackers become more cautious, waiting for cash-out

The collapse of exchange inflows in H2 and the fact that ~48.76% of losses remain unspent (see the section at the end of the report) suggest **that attackers are acting more cautiously.**

Instead of moving funds right away, attackers appear to **wait out initial scrutiny** before taking the next steps. Laundering takes longer and relies more on delayed, step-by-step execution rather than fast liquidation.

DPRK hackers behind at least ~47% of total losses in 2025 hacks

In 2025, DPRK hackers stole **$1.89 billion (~46.8%** of total losses), with a sharp half-year imbalance. Five incidents in H1 accounted for over $1.55 billion, while five incidents in H2 totaled just $134.86 million, meaning H1 losses were **~9.04× higher** than H2. The volume and imbalance are driven largely by the Bybit exploit, where nearly $1.46 billion was stolen in a single incident.

The composition of **targets** also **changed over the year**. In H1, DPRK-linked attacks affected a wide range of targets, including major CEXs (such as Bybit and Phemex), DeFi platforms, and personal wallets. In H2, activity became more concentrated, with incidents limited mainly to five CEXs and one blockchain incubator, without a large-scale exploit comparable to Bybit.

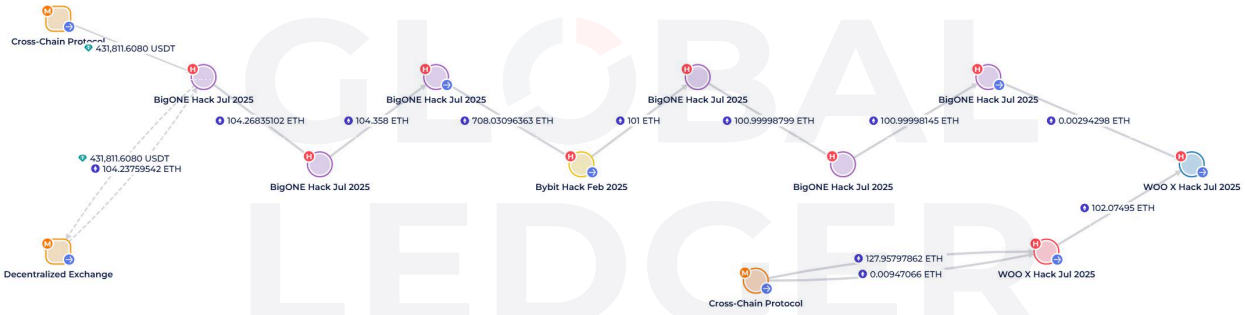
DPRK reuses the same self-hosted wallet infrastructure across different hacks

Global Ledger conducted a more **in-depth analysis** of six hacks allegedly connected to the DPRK hackers (WOO X and Seedify were confirmed by the exploited entity as linked to Lazarus; other cases suggest North Korean involvement):

- BigONE hack, Jul 2025: $29.7 million
- WOO X hack, Jul 2025: $13.7 million
- BtcTurk hack, Aug 2025: $48.1 million
- Seedify hack, Sep 2025: $1.7 million
- SwissBorg hack, Sep 2025: $41.5 million
- Upbit Hack, Nov 2025: $36.8 million

The analysis revealed on-chain patterns that link incidents together:

- Reusage of the **same self-hosted wallets** across ByBit, Woo, and BigOne incidents.



Screenshot from the Global Ledger KYT tool

- Heavy reliance on **multiple single-use wallet infrastructure**, with stolen funds being split into random amounts. This is a strong sign that laundering was carried out not by a single individual, but rather by a group of actors or through pre-planned, sophisticated automation.
- **HuiOne group** associated wallets identified as one of the laundering destinations of the Seedify incident.

Screenshot from the Global Ledger KYT tool

- After an incident occurs, illicit actors do not always rush to launder funds. In 58% of H2 cases, the first post-incident movement takes place within 15 minutes. By contrast, DPRK-attributed hacks show a longer average delay of **54 minutes—3.6× longer.** Among them, the Seedify hack had the shortest delay at 13 minutes and 51 seconds, while in the WOO X case, the stolen funds were first moved only after 2 hours and 22 minutes.

Lazarus Group-linked activity can be identified, or at minimum suspected, based on the following patterns:

1. Large-scale thefts, typically involving tens or hundreds of millions of dollars in cryptocurrency.
2. Each incident follows a highly sophisticated and premeditated intrusion, rather than opportunistic exploitation.
3. There is no evidence of an immediate laundering strategy; instead, operators often delay funds movement while developing a structured laundering plan.
4. Extensive obfuscation techniques are used, including heavy reliance on cross-chain transfers, DEX routing, and single-use wallets, with no apparent concern for transaction fee losses.
5. A hybrid laundering model is observed, combining methods such as CoinJoin, Tornado Cash, and Wasabi Wallet.

6. Targets are predominantly entities with substantial on-chain balances, indicating deliberate victim selection.
7. Centralized exchanges are frequent victims, accounting for seven out of 11 observed cases.

DPRK attacks on CEXs increased 2.5× in H2

The share of DPRK-linked incidents targeting CEXs increased from approximately **40% in H1 to over 83% in H2.** Without a Bybit-scale opportunity in H2, DPRK actors concentrated on smaller CEX intrusions, indicating sustained intent while total losses remained event-driven.

Private key compromises remained the leading DPRK attack vector in both H1 and H2, despite some diversification in tactics in the second half of the year.

DPRK-linked operations prioritize scalable access-based theft and concentrate on high-liquidity targets. The patterns are especially concerning as the losses go far beyond the crypto industry itself. According to the United Nations, the stolen funds are used to support state weapons programs, which means cyber theft in crypto directly contributes to broader geopolitical and security risks, not just financial damage.

Diverse timing and tactics require long-term tracking and continuous monitoring of stolen assets

North Korean cyber operations consist of multiple independent threat clusters, each with its own laundering process, timing, techniques, and preferred services. One DPRK cluster relies heavily on Tornado Cash for laundering, while another literally never uses Tornado Cash or any other mixer and instead routes funds primarily through centralized exchanges. Even when looking specifically at Tornado Cash, withdrawal behavior varies widely — some actors withdraw funds within 1–2 days after deposit, while others deliberately wait weeks or even months before proceeding.

This diversity in timing and tactics is exactly why long-term tracking and continuous monitoring of stolen assets is becoming essential for effective threat intelligence.

Yev Broshevan

CEO & Co-Founder at Hacken

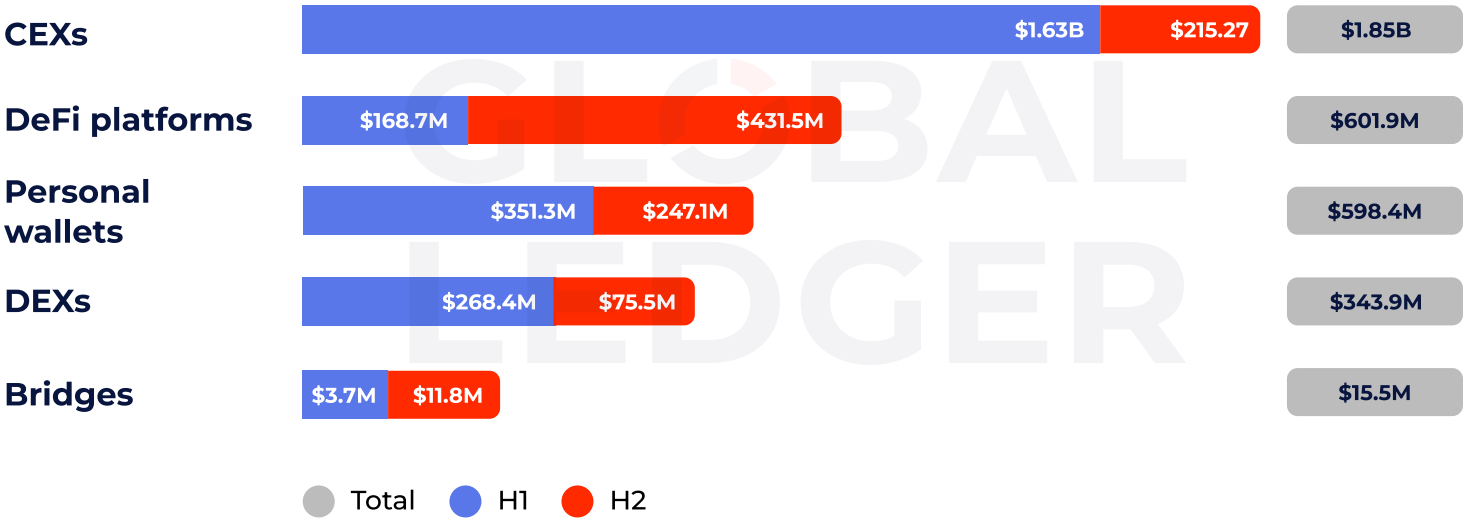
In H2, CEXs losses from hacks dropped by 7.6×; DeFi platforms lost 2.6× more compared to H1

In 2025, CEXs were the most attractive target for attackers, having lost **$1.85 billion** in hacks (**45.79%** of total losses). Of this amount, $1.63 billion was stolen in H1, and $215.27 million was lost in H2—a **7.6× decline** in losses in H2.

However, these figures are heavily skewed by the $1.46 billion Bybit hack. Without this incident, CEXs would have fallen behind **DeFi platforms**, which have lost $601.88 million (14.9% of total losses) in 2025, with a **~2.6× increase** half-over-half.

Personal wallets round out the top three, with **$598.4 million** (14.82% of total). Losses in this category **declined by approximately 29.7%** in H2, falling from $351.3 million in H1 to $247.1 million in H2.

CEXs losses in hacks dropped by 7.6× in H2



Decline in CEX losses reflects the absence of a large-scale breach, not reduced attack activity

The H2 decline in CEX losses is primarily driven by the absence of a Bybit-scale event rather than a broad shift in attacker focus. Excluding the Bybit hack, CEX losses actually increased by approximately **21.5%** in H2 compared to H1.

DeFi platform losses continued to climb in H2, reaching levels approximately **2× higher** than those recorded by CEXs. Interestingly, decentralized exchanges' (DEXs) losses declined sharply in H2, falling to $75.45 million—approximately **3.6× lower** than in H1.

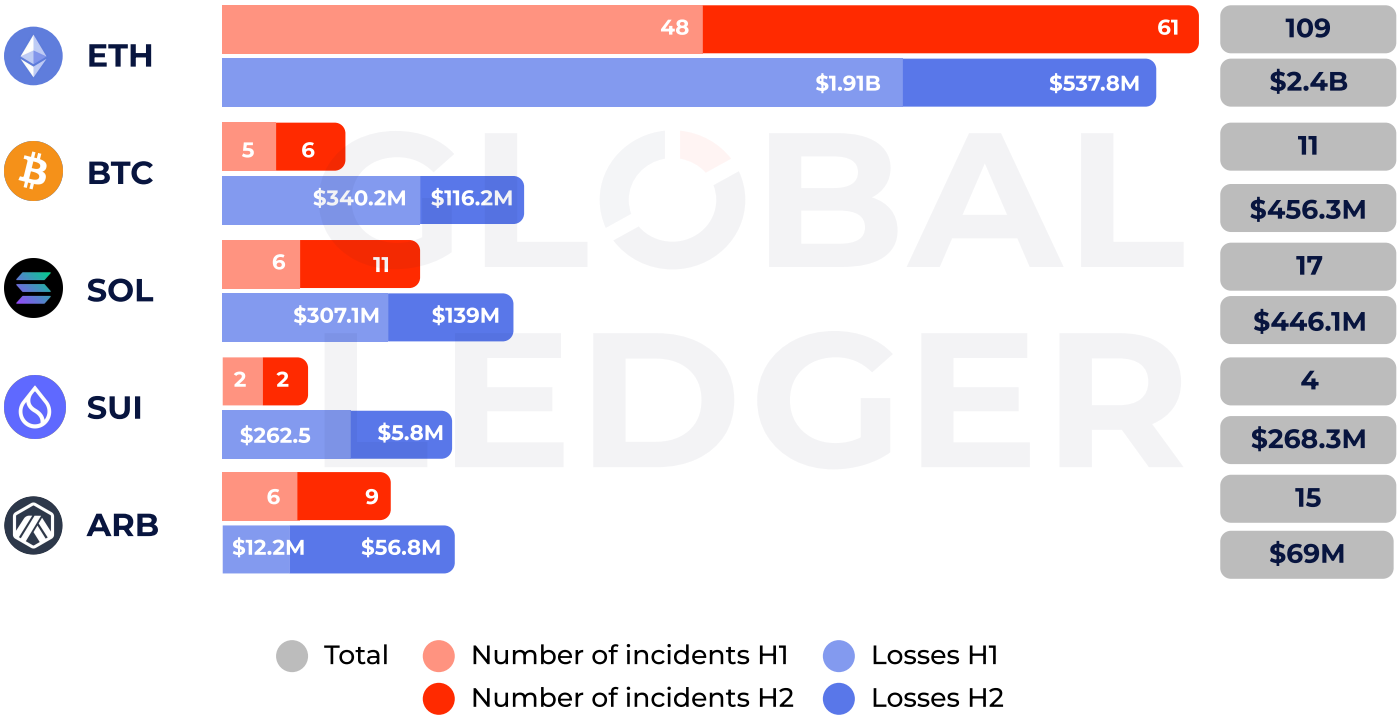
Risk has not decreased but has redistributed into environments where exploitation is easier to repeat and harder to stop.

Ethereum leads the chart in terms of stolen value, with $2.4B stolen in 2025

Ethereum remains the most targeted blockchain both in terms of stolen value and the number of hacks. In 2025, hackers stole over **$2.44 billion** from **Ethereum**, which is **60.64%** of total losses across 109 cases. Losses were heavily front-loaded, with H1 volumes about 3.6× higher than in H2 ($1.91 billion vs. $537.8 million). The gap is largely driven by the Bybit hack, which concentrated a significant share of Ethereum losses.

Bitcoin ranks second, with **$456.33 million** in losses (11.31%), with H1 losses nearly 3× higher than H2 ($340.2 million vs. $116.2 million). It is followed closely by Solana at $446.09 million (11.05%), where H1 losses were about 2.2× higher than H2 ($307.1 million vs. $139 million).

Ethereum leads in stolen value: $3.8B in 2025



With the highest TVL and the largest ecosystem of smart contracts, Ethereum becomes the top target for hackers

Ethereum has by far the **largest concentration of on-chain liquidity** in decentralized finance, making it a natural focal point for high-value hacker activity. Ethereum's Total Value Locked (TVL) is substantially higher than that of any other chain, routinely exceeding $71 billion and accounting for around 58% of all DeFi TVL globally.

Another key factor behind Ethereum's prominence as a target is its reliance on **smart contracts**. Smart contract exploitation remains one of the most frequent root causes of hacks (see the next chapter). This risk is not limited to Ethereum mainnet: Ethereum L2 networks, as well as other chains like Solana and TRON, face similar exposure due to contract logic.

Contract exploits accounted for ~64% of incidents, while malicious approvals caused $1.5B in losses

Throughout 2025, **contract exploits** accounted for **63.53% of incidents**. The share fell from 69.75% in H1 to 58.09% in H2, a decline of 11.66 percentage points. However, the damage caused by these hack types increased by 35.69% in H2, with total losses reaching **$861.54 million in 2025**.

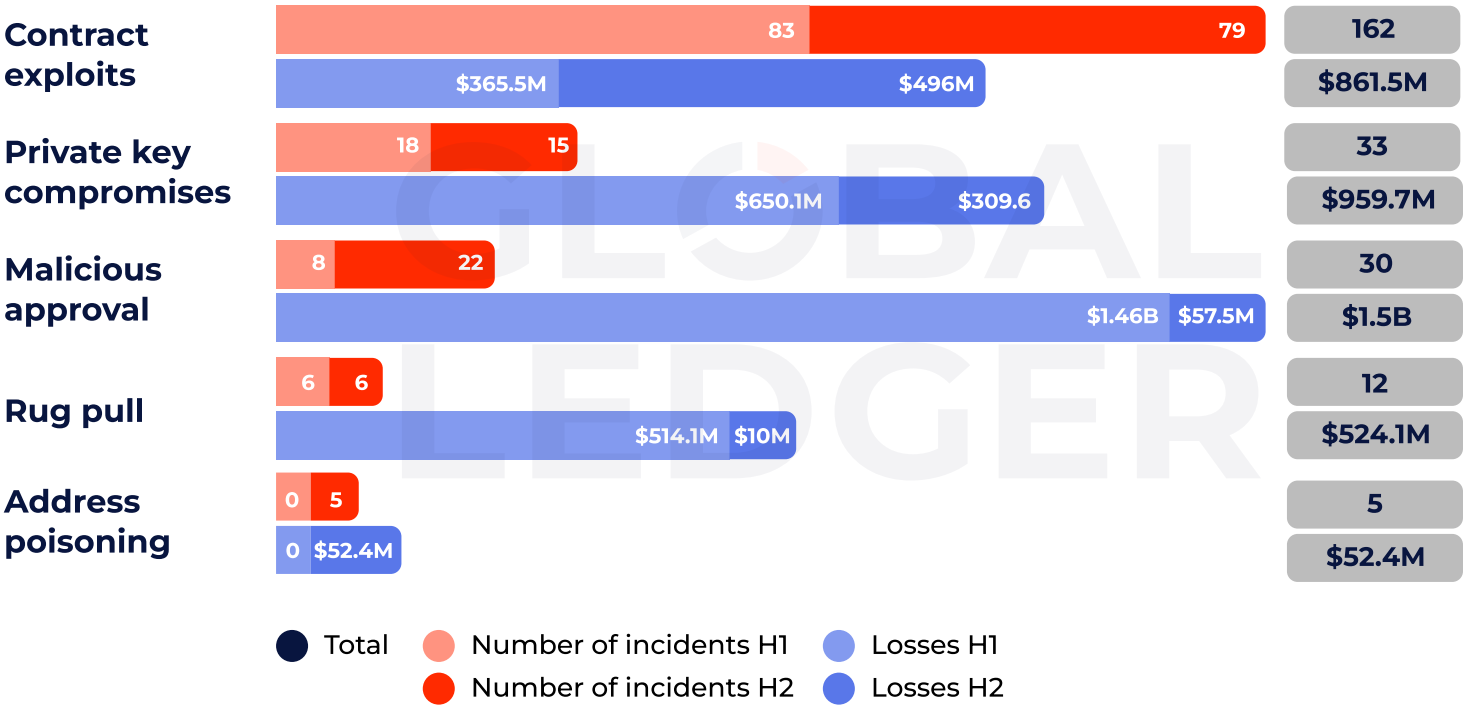
Private key compromises accounted for **13.33%** of hacks but caused more losses in 2025 — **$959.68 million**. Though the number of incidents decreased slightly (from 18 in H1 to 16 in H2), the damage caused by this type of attack declined by 52.37% in H2 compared to H1.

Malicious approvals, with **11.76%** of cases, accounted for **$1.51 billion** in losses. However, the sum is skewed by the volume of the Bybit exploit (nearly $1.46 billion), which significantly inflated the impact of the malicious approval category.

Hackers stole **$524.10 million** in **rug pulls (4.71%** of incidents). However, losses fell more than 5× in H2 compared to H1 despite the same number of incidents.

Address poisoning was not observed in H1. In H2, five such incidents (**1.96%** of total) led to **$52.41 million** in losses, making it the fourth-largest attack type by stolen volume.

Contract Exploits = 64% of Cases. Malicious Approvals = $1.5B Losses



> Criminals learn from the controls institutions impose on suspicious behaviour, and keeping stolen funds for longer may help them avoid detection and investigative attention, enabling the laundering process to continue. However, with broader Travel Rule implementation globally, this and similar strategies are no longer valuable for attackers. Every self-hosted address needs to be verified before a regulated, Travel Rule-compliant entity interacts with it, guaranteeing the owner is identified at every transaction step.

Hannah Zacharias

Head of Regulatory Affairs at 21 Analytics

Smart contract security is no longer enough. Operational security is where the billion-dollar risks now sit

Access control and authorization failures have become some of the most damaging threats in Web3, often surpassing smart contract exploits in financial impact, underscoring why security must evolve from point-in-time audits to continuous, end-to-end protection across infrastructure, operations, and human processes.

Hacken's 2025 Yearly Security Report shows over $2 billion stolen by North Korean threat actors in 2025 alone, primarily through phishing and credential compromise, with centralized exchanges remaining the main targets. This highlights that operational security, not just code, is now the weakest link.

In DeFi, operational security breaches already rival smart contract hacks in total losses, yet the industry still treats security largely as a contract audit problem. In 2026, security firms must evolve from point-in-time audits to continuous, protocol-wide security — strengthening access controls, enforcing multisig and timelocks, deploying monitoring and EDR, and hardening teams against social engineering.

Yev Broshevan

CEO & Co-Founder at Hacken

Malicious approvals drive ~1.8× more losses than smart contract exploits

In 2025, contract exploits dominated by count, but **malicious approvals** drove **1.76× more losses**, illustrating a disconnect between attack frequency and financial impact.

Contract exploits are frequent but often capped by protocol-level limits or rapid mitigation. In contrast, malicious approvals and private key compromises directly target user wallets and signing authority, allowing attackers to access large balances in a single step. Address poisoning similarly exploits user behavior rather than technical vulnerabilities.

Together, these patterns show that systemic and behavioral weaknesses pose greater financial risk than smart contract exploits.

Malicious approval scams require rapid response from recovery teams

Unlike contract exploits with immutable on-chain proof, malicious approval scams rely on Web2 infrastructure, like fake websites, fraudulent channels, manipulated interfaces. This evidence typically disappears within days, creating urgent preservation challenges.

Recovery teams must rapidly deploy web-forensics tools that capture and preserve this ephemeral evidence in court-admissible formats. When properly documented, this evidence shifts responsibility from victim to perpetrator. Success depends on timing: capturing deception infrastructure before it vanishes, and proper forensic methodology meeting evidentiary standards.

Marcin Zarakowski

CEO of Recoveris

Nearly half of the stolen funds remain unspent

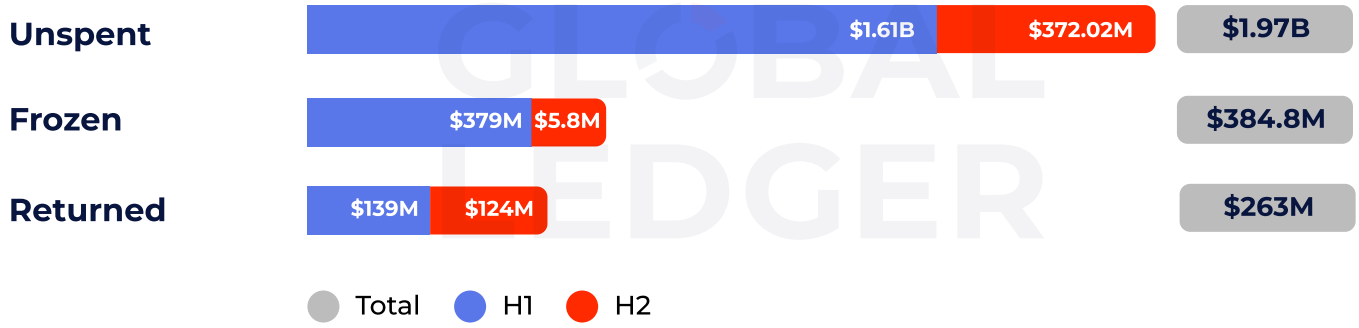
At the time of the research, over **$1.97 billion (48.76%** of total losses) remained **unspent**, meaning the funds didn't move or stopped moving. Some of them are likely still in the process of being laundered, as attackers may be waiting for the heat to die down.

Frozen funds totaled $384.79M, representing **~9.52%** of the total losses. The volume of funds frozen in H1 was **~65× higher** than in H2, with Cetus ($162 million), Nobitex[1] ($83.89 million), and Bybit ($72.46 million) leading the list.

$263.23 million, or just **6.52% of total losses**, was **returned**, showing a 10.79% decrease in H2 compared to H1. Here, the Bybit incident, with $38.44 million recovered, is not leading the chart. Higher recovery volumes were recorded for the UPCX hack ($72.97 million) and the Balancer hack ($55.1 million).

1 In the Nobitex hack, funds were deliberately sent to burn addresses as a symbolic act. In that incident, $83.89 million was hacked and burned, effectively a public execution of the assets.

~50% of stolen funds remain unspent



Asset recovery fails to keep pace with theft

The fact that nearly **½ of stolen funds remain unmoved** suggests attackers are deliberately delaying laundering.

While 9.52% of total losses were **frozen**, this outcome remains **highly concentrated in a few large cases**. Enforcement actions show some effect, but voluntary returns remain uncommon, with most recoveries driven by rapid intervention rather than goodwill.

Asset recovery continues to **lag far behind** theft volumes—a persistent gap between detection, response, and enforcement. Some projects have explicitly negotiated with attackers to recover funds, though such cases are rather exceptional and typically **require offering bounties**, which can result in up to ~90% returns, like in the GMX hack.

In contrast, threats of enforcement action alone are less effective, though there are exceptions. One example is the Loopscale incident, where the funds were returned in full after the project team assured the attacker that no legal action would be pursued if the funds were returned by a specified deadline.

Investigators need more interoperability, with tracing APIs, compliance data, and law enforcement work

Asset recovery remains limited due to two core issues: slow cross-border legal processes and fragmentation of laundering pathways. On the legal side, delays in data sharing, asset-freeze authorization, and evidence standardization make real-time cooperation difficult. Technically, attackers now exploit micro-laundering techniques, leveraging cross-chain bridges, privacy-preserving DeFi protocols, and rapid asset conversions to overwhelm manual tracing and reporting systems. This means the investigative community should focus on interoperability, integrating law enforcement casework, compliance data, and industry-grade tracing APIs.

Mudassar Malik

CEO and founder of Deconflict.com

At the time of the research, over **$1.97 billion (48.76%** of total losses) remained **unspent**, meaning the funds didn't move or stopped moving. Some of them are likely still in the process of being laundered, as attackers may be waiting for the heat to die down.

Frozen funds totaled $384.79M, representing **~9.52%** of the total losses. The volume of funds frozen in H1 was **~65× higher** than in H2, with Cetus ($162 million), Nobitex ($83.89 million), and Bybit ($72.46 million) leading the list.

$263.23 million, or just **6.52% of total losses**, was **returned**, showing a 10.79% decrease in H2 compared to H1. Here, the Bybit incident, with $38.44 million recovered, is not leading the chart. Higher recovery volumes were recorded for the UPCX hack ($72.97 million) and the Balancer hack ($55.1 million).

Conclusion

1 Faster first funds movement leaves little time to react

In the fastest cases, the first movement of stolen funds occurred in 2 seconds. Across 2025, ~76% of hacks saw funds move before public disclosure, rising to 84.6% in H2. It leaves minimal time for early intervention.

2 With faster public reporting, attackers have less time for 'quiet' laundering

Public disclosure became faster in H2 2025, narrowing the response gap by ~2.1× compared to H1. As a result, attackers have 2x less time and fewer opportunities to launder funds quietly.

3 Staged laundering dominates in ~99% of cases

Single-step laundering is rare. In H1 2025, only in 2.5% of incidents, attackers sent all the funds to VASP/mixer in the first move, while no such cases were observed in H2. Most incidents relied on fragmented, multi-stage funds movement, obscuring funds flows.

4 3× more stolen funds cross-chained than mixed

Approximately $2.01B, or ~49.8% of all stolen funds in 2025, was cross-chained. It is over 3× more than sent to mixers and privacy protocols. Tornado Cash alone was used in ~41.6% of all hacks, with its share rising sharply in H2 to ~74% of cases, following the lifting of sanctions.

5 Reduced exchange inflows indicate slower laundering

The volume of funds sent to centralized exchanges fell 5.9× compared to H1. Attackers are more cautious and appear to be waiting out initial scrutiny before taking the next steps. The high level of unspent funds (~50%) also suggests hackers wait for the heat to die down.

6 Low recovery rates persist

At the time of analysis, only $263M (6.52%) of stolen funds was returned, with a 10.79% decrease in H2 compared to H1, showing that successful recovery remains the exception.

Subscribe to the Global Ledger newsletter for upcoming reports

Subscribe