CERTIK

CertiK Intel3D

H1 2026 Wrench Attacks

CertiK recorded 52 verified wrench attacks globally, up from 39 in H1 2025, a 33.3% year-over-year increase, with recorded financial exposure reaching an estimated $124.1 million, an 11.8-fold jump from $10.5 million in H1 2025.

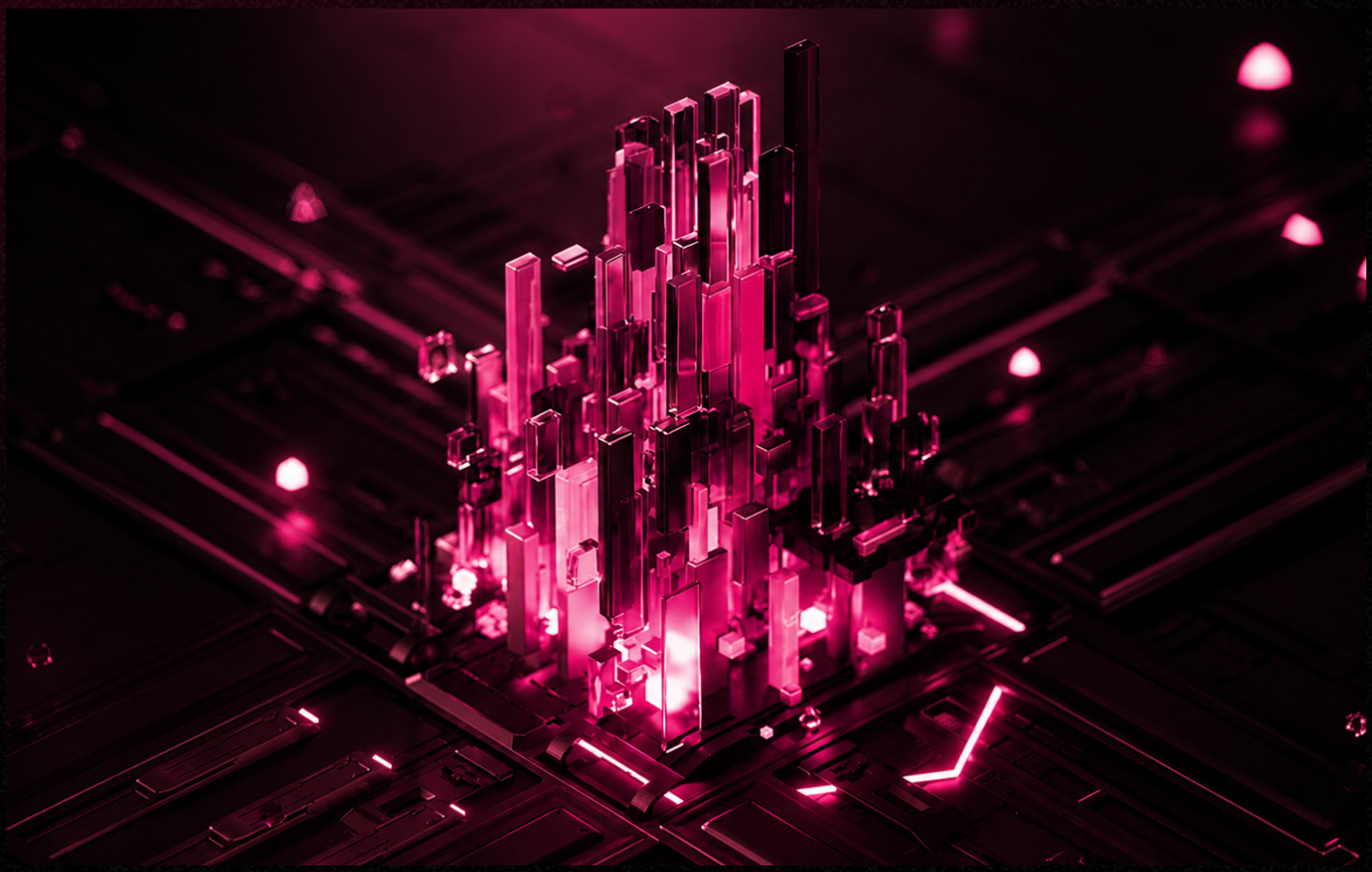

Table of Contents

Executive Summary

H1 2026 confirms that wrench attacks are no longer a fringe phenomenon or an edge-case risk for cryptocurrency holders. Over the first six months, CertiK recorded **52** verified incidents worldwide, representing a **33.3%** year-over-year (YoY) increase. The increase was driven by activity during the first quarter, which recorded **35** verified incidents compared to **22** in Q1 2025.

Recorded losses and ransom demands reached approximately **$124.1 million** in H1 2026, compared with approximately **$10.5 million** in H1 2025. These figures remain indicative, not exhaustive: many ransoms, failed demands, recovered funds, frozen funds, and private settlements are not publicly disclosed or are partially disclosed.

Geographically, the threat landscape became highly concentrated. Europe accounted for **39** of **52** verified H1 2026 incidents. France alone accounted for 33 incidents, making it the dominant national epicenter in the dataset. This continues the trajectory identified in the 2025 Skynet Wrench Attacks Report, which already found that Europe had become the most dangerous region for crypto holders. H1 2026 suggests that the trend has narrowed even further into a concentrated Western European crisis.

Tactically, the defining shift of H1 2026 is the rise of home invasion tied to crypto. Home invasions increased from one publicly reported incident in H1 2025 to 20 in H1 2026. Kidnapping remained persistently high, rising from **12** to **16** incidents. Torture remained unchanged at four cases, while murder remained present at one confirmed case in each H1 period.

Executive Summary

Scope of this report

This report analyzes the H1 2026 wrench attack landscape using the chart pack supplied for this report, the 2025 Skynet Wrench Attacks Report, and the public CertiK article "2026 Wrench Attacks Overview" published in May 2026.

A wrench attack is treated as a physical coercion incident in which adversaries use violence, intimidation or credible threats to compel a victim to transfer digital assets, surrender private keys, unlock a wallet, reveal credentials, or pressure a third party into compliance. The incident location is recorded based on the physical location of the coercive event, not the nationality of the victim or the attacker.

Incident counts are based on verified and public events only. A verified incident may be supported by law-enforcement disclosures, court documents, reputable media reporting, public victim testimony, on-chain traces linked to a physical attack, or corroboration across multiple credible sources.

Financial figures are best understood as "recorded exposure" rather than a complete accounting of stolen value. The dataset may include stolen assets, ransom demands, partial payments, frozen or recovered funds, failed demands, and loss estimates reported by victims or authorities. Under-reporting remains severe because victims may fear retaliation, reputational damage, tax exposure, or law-enforcement inaction.

Data limitations

- **Under-reporting**: many victims never file complaints or do not publicly disclose attacks.
- **Classification variance**: local authorities may record crypto-related coercion as robbery, kidnapping, extortion, or assault without a digital-asset marker.
- **Loss ambiguity**: ransoms demanded, ransoms paid, assets stolen, assets frozen, and assets recovered are frequently reported inconsistently.
- **Reporting lag**: incidents can be discovered or verified weeks after they occur, especially when investigations are active.
- **Source risk**: public reporting can omit sensitive details, including the full amount targeted, the identity of proxy victims, or the role of insiders.

For these reasons, the statistics in this report should be read as the visible portion of a broader phenomenon.

Definitions and taxonomy

The report uses the same general taxonomy established in the 2025 Skynet Wrench Attacks Report, while adding “Forced Crypto Transfer” as a clearer label for cases in which the victim is compelled to execute a transaction without the broader context of kidnapping, ransom, or home invasion. Attack categories are assigned according to the dominant coercive mechanism visible in available sources.

Layer	Working definition
Home Invasion	Entry into an occupied residence to coerce wallet access or asset transfer.
Kidnapping	Abduction of a victim to force payment, access, or compliance.
Ransom	Payment demanded in exchange for release, safety, or asset recovery.
Forced Crypto Transfer	Immediate transfer of digital assets under direct threat.
Physical Assault	Physical force used to obtain access, devices, keys, passwords, or compliance.
Robbery / Armed Robbery	Theft through force, intimidation, or weapon threat.
Torture	Severe physical or psychological coercion used to force disclosure of sensitive information.
Murder	Killing of a victim as part of a crypto-related coercive event.

H1 2026: Global Incident Trend

The headline number for H1 2026 is **52** verified incidents, up from **39** in H1 2025, representing a **33.3%** YoY increase. The year began with an acceleration: January recorded **15** incidents compared with **9** the previous year, and March recorded **13** compared with **7**. April also increased sharply, rising from **2** to **8**. May and June then fell below the previous year's levels, but the cumulative total remained materially higher than H1 2025. The lower totals recorded in May and June may reflect a combination of increased law-enforcement pressure, changes in security practices, and/or reporting delays.

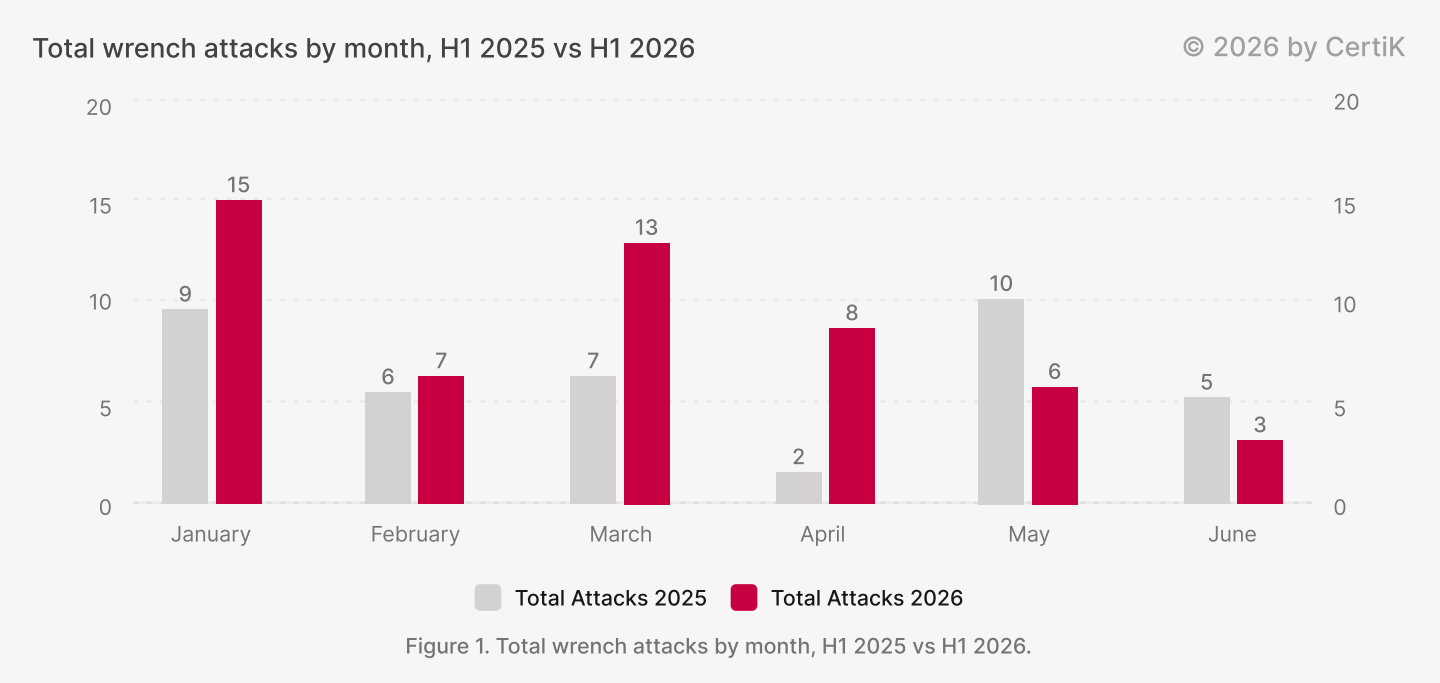

Figure 1. Total wrench attacks by month, H1 2025 vs H1 2026.

The quarter-level view clarifies the pattern. Q1 2026 was the spike period, with **35** incidents compared with **22** in Q1 2025. Q2 2026 recorded **17** verified incidents, matching the total observed during Q2 2025.

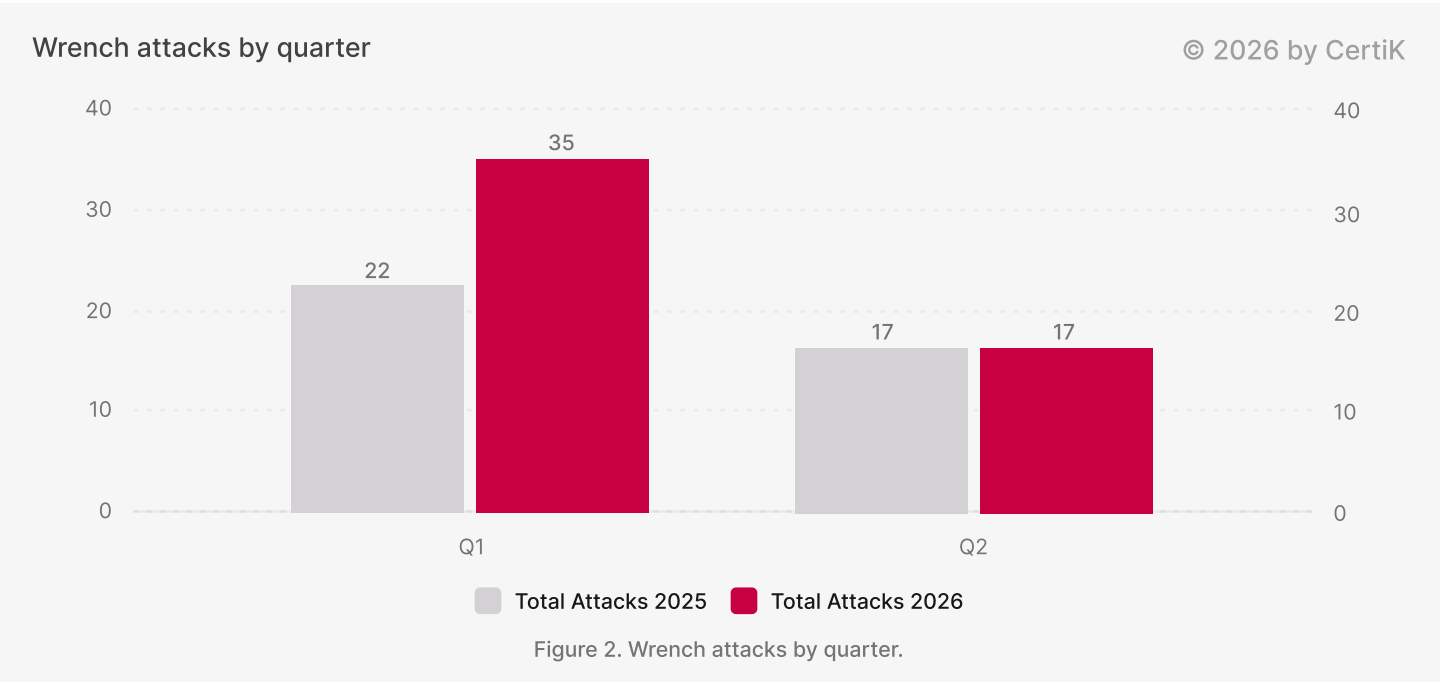

Figure 2. Wrench attacks by quarter.

A linear annualization of H1 2026 would imply around **100** incidents for the full year. **That should not be interpreted as a forecast**. The first half of the year contains two distinct phases: a major Q1 acceleration and a Q2 decline. If the Q1 pace returns, the full-year total could be materially higher. If Q2 stabilization continues, 2026 may still finish well above 2025 in financial impact even if incident volume does not double.

Incident Losses: Fewer Illusions, Higher Stakes

Recorded financial exposure associated with verified wrench attacks increased from **$10,532,242** in H1 2025 to **$124,180,400** in H1 2026. This represents an approximately **11.8**-fold increase, or **1,079%** YoY.

Average recorded exposure per incident also increased, rising from approximately **$270,000** in H1 2025 to approximately **$2.39 million** in H1 2026.

It is important to note that these figures do not exclusively represent confirmed stolen funds. Rather, they reflect the total value associated with recorded incidents, including ransom demands, funds transferred by victims, assets frozen by authorities or service providers, etc. As a result, these totals should be interpreted as an indicator of the overall financial scale of wrench attacks rather than a measure of realized criminal profits.

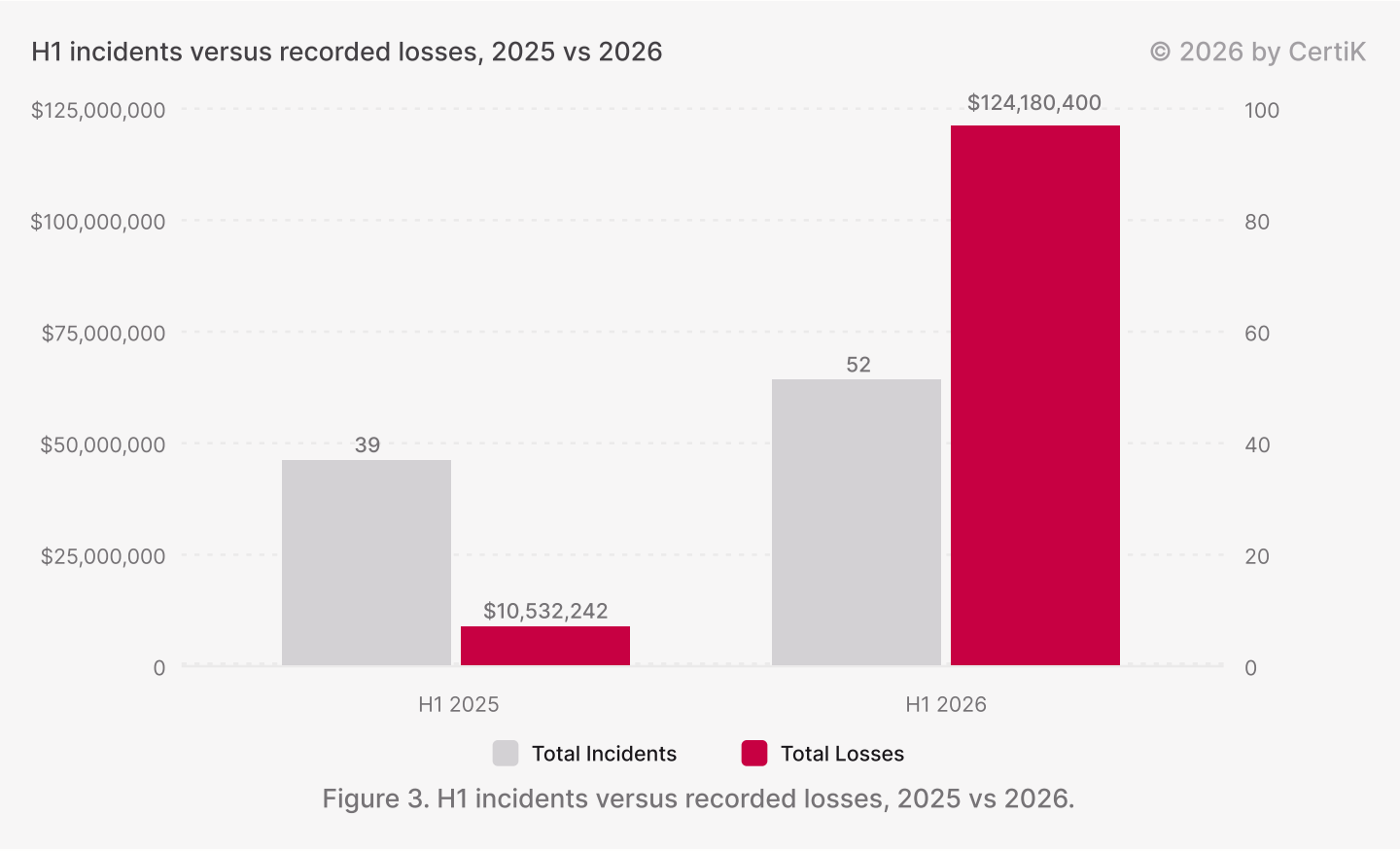

Figure 3. H1 incidents versus recorded losses, 2025 vs 2026.

The trend suggests that attackers increasingly believe that physical coercion can produce outsized returns. This belief changes criminal economics. Even failed attacks can be rational for crews if the expected payout is high enough and the organizers outsource operational risk to disposable ground-level teams.

The loss figure also understates the real cost. Victims face medical costs, relocation costs, security upgrades, loss of productivity, psychological trauma, reputational damage, and a long-term reduction in willingness to participate publicly in the ecosystem. For founders and executives, the direct financial loss may be smaller than the downstream cost of going private, limiting travel, reducing public appearances, or rebuilding custody processes under emergency conditions.

Geographic Distribution

The geographical distribution of verified wrench attacks changed between H1 2025 and H1 2026. Europe accounted for **39** of **52** recorded incidents in H1 2026, representing **75.0%** of all verified cases. During H1 2025, Europe accounted for **14** of **39** incidents, or **35.9%**.

Regional distribution, H1 2025 vs H1 2026.

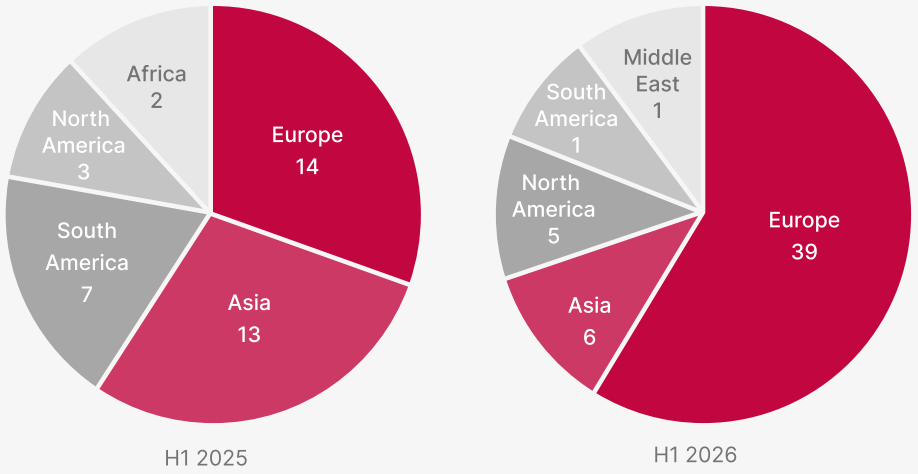

Figure 4. Regional distribution, H1 2025 vs H1 2026.

Regional Distribution

The regional distribution shows the compression of risk elsewhere. Asia declined from **13** incidents to **6**, South America from **7** to **1**, Africa from **2** to **0**, while North America rose from **3** to **5**. The Middle East registered **1** incident in H1 2026 after none in H1 2025.

Total incidents by region, H1 2025 vs H1 2026.

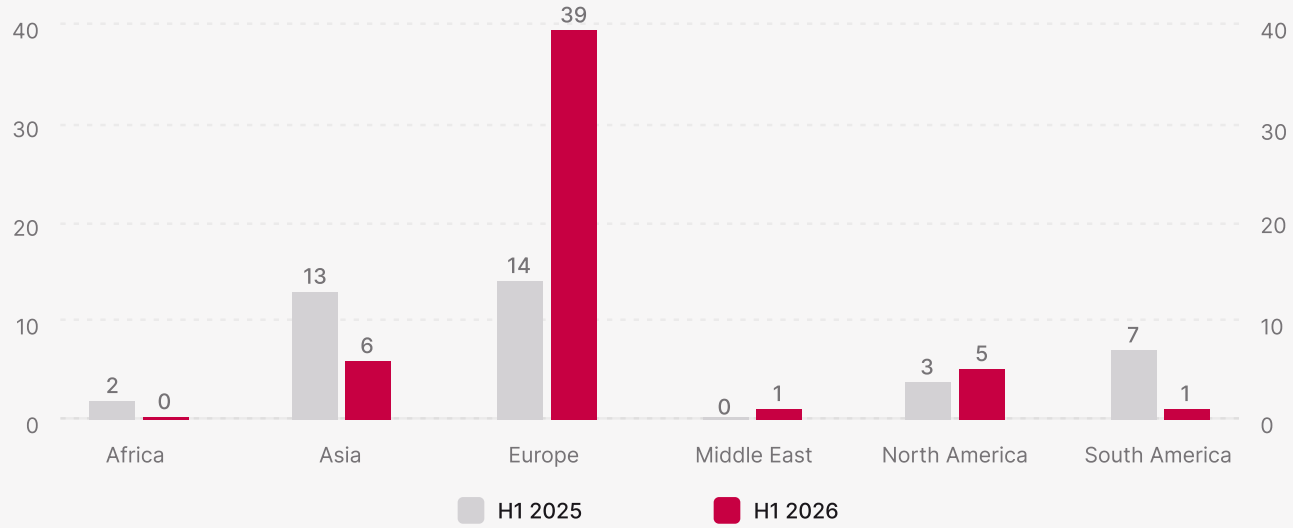

Figure 5. Total incidents by region, H1 2025 vs H1 2026.

Country Distribution

The country-level distribution largely reflects the regional pattern. France accounted for **33** of the **52** verified incidents recorded during H1 2026. The United States recorded **4** incidents, while Sweden and the United Kingdom recorded **2** incidents each. Belgium, Cambodia, Canada, Hong Kong, Malaysia, the Philippines, Spain, and Turkey each recorded **1** incident.

France accounted for **63.5%** of all verified incidents recorded globally during H1 2026 and **84.6%** of all European incidents during the period.

Note: that France's incident count could be much higher, with the Direction nationale de la police judiciaire (DNPJ) reporting 41 incidents between January and March 2026.

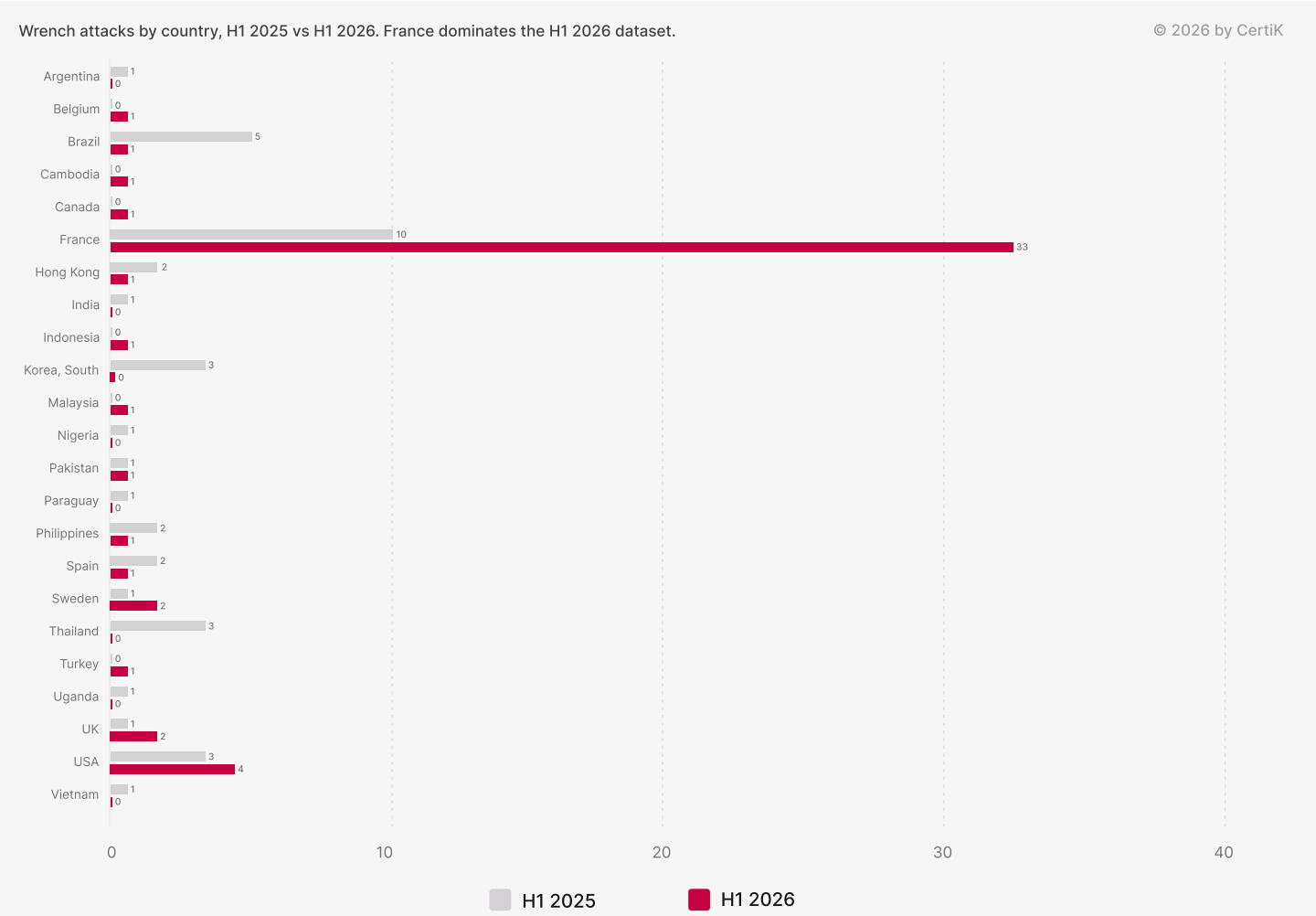

Figure 6. Wrench attacks by country, H1 2025 vs H1 2026. France dominates the H1 2026 dataset.

Why Europe?

The concentration of incidents in Europe does not appear to be attributable to a single factor. Several characteristics of the region may contribute to its representation within the verified public dataset, including the concentration of crypto-related businesses, investors, founders, and public-facing industry participants.

Europe also contains a large number of jurisdictions that maintain extensive administrative, regulatory, and tax records. In cases where such information is exposed through data breaches, leaks, or unauthorized disclosure, it can potentially be combined with publicly available information to identify individuals associated with significant crypto holdings.

Public reporting practices may also contribute to the observed concentration. Many European incidents receive extensive media coverage and are often accompanied by court documents, law-enforcement statements, or victim testimony, making verification more straightforward than in jurisdictions where reporting is more limited.

The concentration of incidents in Europe may also reflect broader criminal environment factors. Several European jurisdictions have experienced sustained concerns regarding violent crime, organized criminal activity, and repeat offending. While the H1 2026 dataset cannot establish causation, the frequency of reported wrench attacks suggests that some offenders perceive the potential rewards as sufficient to justify the legal and operational risks associated with these crimes.

However, Europe's overrepresentation in the dataset is largely attributable to the number of incidents recorded in France.

Why France?

French Interior Minister Laurent Nuñez recently stated that authorities had recorded **77** crypto-related physical incidents during H1 2026, compared with **45** during H1 2025. This report applies a narrower methodology and only includes incidents that were publicly reported and independently verifiable. Under this methodology, CertiK recorded **33** verified wrench attacks in France during H1 2026, compared with **10** during H1 2025. No other country recorded a comparable number of verified public incidents during the reporting period.

Several factors may contribute to France's prominence within the dataset. France hosts a large and visible cryptocurrency ecosystem, including exchanges, founders, investors, service providers and frequent industry events. At the same time, the country has experienced a series of major data exposure incidents affecting both private and public-sector organizations. Recent examples include the compromise of France Travail and the security incident disclosed by the Agence Nationale des Titres Sécurisés (ANTS). Such incidents increase the availability of personal information that may be combined with open-source intelligence and publicly available blockchain data to identify potential targets.

Figure 7. International Cyber Digest post on the ANTS data breach in France.

French authorities have also highlighted the involvement of younger offenders in ongoing investigations. According to public reporting, approximately 200 individuals have been arrested since the beginning of the year in cases linked to crypto-related kidnappings and extortion, with

several dozen of those arrested identified as minors. While these figures do not allow conclusions regarding offender motivations, they demonstrate that participation in wrench attacks is not limited to established organized crime actors and may involve a broader range of criminal profiles.

Law-enforcement authorities have undertaken several high-profile operations in response to the wave of attacks. In June 2025, Moroccan authorities arrested Badiss Mohammed Bajjou, who was described in public reporting as a suspected organizer linked to multiple crypto-related kidnapping cases. However, the H1 2026 dataset does not show a reduction in verified incidents following that arrest.

The available data does not establish whether the individuals arrested represented the entirety of the network involved in these crimes. However, the continued occurrence of incidents after major arrests suggests that the threat cannot be attributed to a single actor and may involve multiple groups, facilitators, or independent offenders operating within the same ecosystem.

Taken together, the H1 2026 data suggests that France remains the primary geographic concentration of publicly reported wrench attacks.

Attack Type Evolution

Home invasion moved from a marginal category to the dominant H1 2026 vector: **20** incidents compared with only **1** in H1 2025. This category alone accounts for roughly **41%** of all H1 2026 incidents.

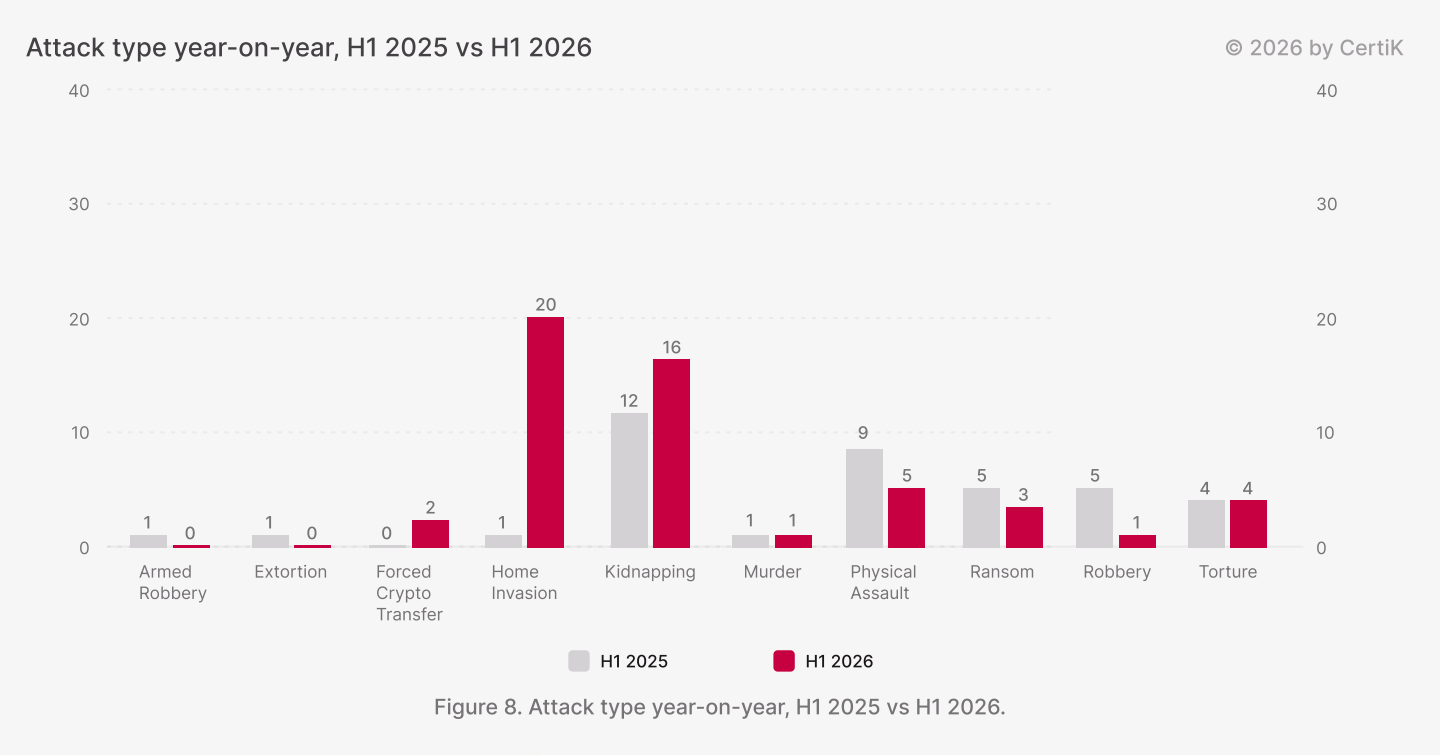

Figure 8. Attack type year-on-year, H1 2025 vs H1 2026.

Kidnapping remained structurally important, increasing from **12** to **16** incidents. Unlike opportunistic robberies, kidnappings require planning, confinement logistics, communication channels, payment instructions, and often cross-border laundering support. The persistence of kidnapping suggests that organized groups still view crypto holders and their relatives as viable high-return targets.

Home invasion as the defining 2026 vector

A home invasion attacks the entire security perimeter of the victim: physical residence, family routines, door access, alarm response, device locations, seed storage, and the victim's ability to remain calm under pressure. It also collapses the distinction between individual security and family security.

This trend should force a rethink of self-custody advice. It is not enough to tell holders to use hardware wallets and keep seed phrases offline. A cold wallet inside a residence can become accessible if the victim is forced to unlock it. A seed phrase hidden at home can become a liability if attackers have time to search. A single-signer setup can become catastrophic if the signer can be coerced into moving assets instantly. In 2026, strong custody means designing systems that remain resilient even when a human is under duress.

Proxy targeting and family pressure

Proxy targeting is one of the most disturbing features of the current threat landscape. Attackers do not need direct access to the primary holder if they can threaten a spouse, parent, child, employee, driver, assistant, or close friend. Proxy victims often have weaker operational security, more predictable routines, and less training than the primary target. They may also be easier to identify from social media, corporate bios, conference photos, school references, or public records.

The effect is psychological leverage. A victim may initially prioritize the security of their assets over their own physical safety, but most will abandon security protocols if they believe a loved one is in immediate danger. This is why family preparedness must become part of serious crypto security.

Notable H1 2026 Cases

Le Chesnay-Rocquencourt (Home Invasion) — France

In March 2026, a couple were attacked during a home invasion in Le Chesnay-Rocquencourt, near Paris. The assailants used violence to force the victims to transfer approximately €900,000 in bitcoin before leaving the residence. No recovery of the transferred funds was reported at the time of publication.

The case illustrates how attackers can bypass digital security controls by targeting victims directly within their homes and coercing an immediate on-chain transfer.

Genting Highlands (Kidnapping) — Malaysia

On April 17, 2026, a South Korean national was abducted while travelling from Genting Highlands to Kuala Lumpur and held for four days at a property in Melaka. The kidnappers demanded a ransom of 10 million USDT from the victim's family, who reportedly paid 3 million USDT to secure his release. Malaysian authorities subsequently froze and recovered 2.46 million USDT of the ransom. Three South Korean suspects were arrested and investigated under Malaysia's Kidnapping Act.

Sillytuna (Physical Assault) — United Kingdom

The Sillytuna case illustrates the high-value coercion model. The victim was physically forced to surrender approximately **$24 million** in aEthUSDC. The alleged laundering path crossed multiple chains before conversion into Monero.

This case shows that physical coercion can now produce losses comparable to major cyber incidents, while bypassing the technical safeguards that normally protect on-chain assets.

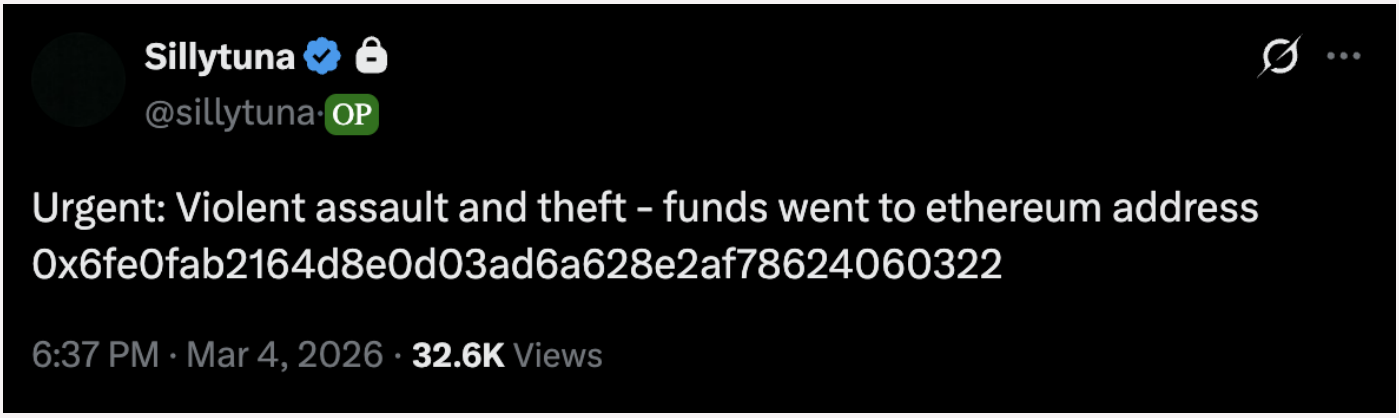

Figure 9. Sillytuna tweet, March 4 2026.

Attacker Profiles & Modus Operandi

H1 2026 confirms the professionalization of physical crypto-crime, but not necessarily the professionalization of every actor involved. The operating model increasingly appears layered. At the top are organizers and sponsors who identify targets, purchase or aggregate data, coordinate logistics, and control laundering. Below them are local coordinators who recruit teams, arrange vehicles or safe locations, and handle immediate surveillance. At the bottom are ground-level operators, often young men recruited through messaging apps or local criminal networks for a fixed fee. In some cases, these individuals are coerced into committing such acts under penalty of physical harm to themselves or their relatives.

Data-driven targeting

The most important TTP shift is the move toward data-driven targeting. In older models, criminals relied heavily on visible wealth signals, social media flexing or conference appearances. In 2026, attackers can combine leaked databases, tax or compliance records, exchange customer data, social media profiles, ENS names, public wallet activity, real estate information, and phone-number intelligence to build a target package without prolonged physical surveillance.

A target package can include a full name, address, phone number, family structure, estimated wealth, known wallet activity, employer, travel habits, and social graph. Once this profile exists, the physical attack becomes the final stage of a mostly information-driven process. This is why data minimization is no longer a privacy luxury. It is a physical safety control.

Insider Access and Data Brokerage

Several investigations and public reports published during H1 2026 indicate that insider access has become part of the broader data supply chain around crypto-related targeting. In one case, French authorities alleged that a tax administration employee sold confidential information relating to cryptocurrency investors to criminal networks. In a non-French example, Kraken disclosed an extortion attempt after malicious insiders within its client-support environment recorded internal systems showing client data. Public reporting has also identified dark-web recruitment posts seeking employees at cryptocurrency platforms and other data-rich organizations in order to obtain internal access or customer information.

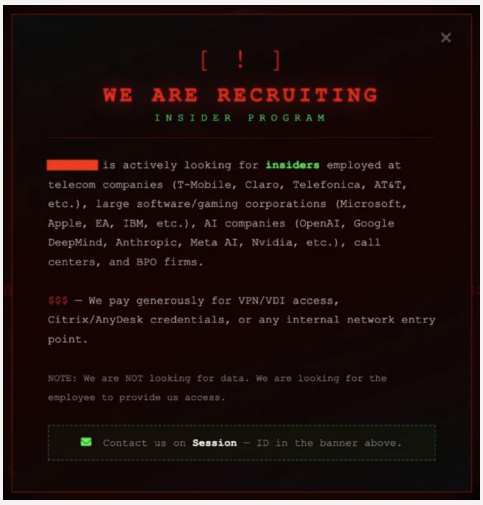

Figure 10. Recruitment notice of a cybercriminal organization.

This activity represents a different category of threat from traditional open-source intelligence. Rather than relying only on social media, conferences, public blockchain activity, or exposed online profiles, criminal groups may obtain information from insiders who already have access to verified customer records, tax information, support tools, residential details, contact information, identity documents, or other personal identifiers.

The H1 2026 dataset does not determine how frequently insider-derived information is used during wrench attacks. However, these cases show that the attack surface extends beyond the victim's own operational security. Public institutions, exchanges, contractors, support providers, and other third parties that store sensitive customer or identity information may also contribute to the targeting environment.

Access vectors

- **Doorbell vector**: attackers impersonate delivery workers, utility staff, neighbors, law enforcement, or maintenance personnel to get the door opened.
- **Fake meeting vector**: victims are lured to business meetings, OTC trades, investment pitches, or private appointments where the environment is controlled by the attackers.
- **Transit vector**: victims are intercepted between predictable locations such as home, office, airport, hotel, event venue, school, or gym.
- **Proxy vector**: family members or associates are targeted to create emotional leverage over the primary holder.
- **Insider or acquaintance vector**: a trusted contact provides location, routine, access, or credibility to reduce the target's suspicion.

Coercion and transaction execution

Once attackers gain control of the victim, the goal is to compress decision time and remove the victim's ability to consult others. Phones may be taken, devices isolated, family members separated, and threats escalated until the victim unlocks wallets or reveals credentials. Attackers may use the victim's own device to pass biometric checks or platform risk controls. Some crews appear to understand enough about wallets, exchanges, and cross-chain liquidity to move assets quickly, while others depend on remote organizers for transaction instructions.

The technical implication is that single-signer custody is fragile under duress. A victim who can unilaterally transfer all assets can be coerced into doing so. Stronger controls include multi-signature or MPC with geographically distributed signers, withdrawal delays, transaction-size thresholds, allowlists, staged vault architecture, and emergency freeze processes that do not rely on the threatened individual alone.

Ecosystem Impact

The spread of wrench attacks affects more than the immediate victims. It changes how builders, investors, traders, employees, and families participate in the crypto ecosystem. Public identity was once viewed as a trust-building mechanism. In the current environment, public identity can become a liability if it links a real person, address, social graph, and perceived holdings.

Psychological and behavioral impact

The psychological impact is severe because wrench attacks violate the most private security boundary: the body, the home, and the family. Victims and potential targets may withdraw from public discussion, reduce conference attendance, stop posting online, relocate, change routines, or transfer assets to custodial arrangements they would previously have rejected. This chilling effect reduces transparency and can push legitimate actors into anonymity.

Operational impact on companies

Crypto companies cannot treat these incidents as personal problems for executives. A founder's home invasion can become a company crisis if the founder controls treasury wallets, administrative keys, multisig shares, deployment permissions, or exchange relationships. Even when no corporate funds are lost, the operational disruption can be substantial. Boards and security teams should ask whether any employee under duress could move assets, approve transactions, alter permissions, or expose sensitive user data.

Public-data and compliance impact

The current threat model also raises questions about the concentration of sensitive financial data. Stronger tax reporting, exchange compliance, and identity verification can create valuable records linking individuals to crypto holdings. Those records may be necessary for regulatory purposes, but they become dangerous if access logging, insider monitoring, retention limits, and breach notification are weak. DAC8 became applicable on 1 January 2026, introducing new reporting obligations for crypto-asset service providers and enabling the automatic exchange of crypto-asset transaction information between EU tax authorities.

DAC8 provides for automatic exchange of information on crypto-assets between EU countries. It is the eighth amendment of the Directive on Administrative Cooperation in Direct Taxation.

The Directive aims to strengthen the overall legal framework on the automatic exchange of information (AEOI) to fight tax fraud and combat tax evasion and tax avoidance by enlarging its scope to cover crypto-assets.

DAC8 rules enter into force on 1 January 2026, expanding tax transparency to crypto-asset transactions. Reporting Crypto-Asset Service Providers should begin preparing now:

- **Single registration** in the Member State if you operate in the EU but are *not* authorised under MiCA.
- **Start collecting data** on reportable crypto-asset transactions of all EU-resident users, including residents of the Member State where you are established, from 1 January 2026.
- **Reporting** is due within **9 months** after the end of the first fiscal year covered by the directive – that is between 1 January and 30 September 2027.
- **Check domestic requirements** including reporting deadlines and formats.

Figure 10. Extract from DAC8 implemented in Europe in January 2026.

H2 2026 Threat Outlook

H2 2026 is likely to be shaped by three competing forces: enforcement pressure, criminal adaptation, and market visibility. Law-enforcement action can disrupt local crews, but the economic incentives remain strong. As long as attackers believe that a single successful operation can yield seven- or eight-figure exposure, the model will continue to attract organizers.

1. Base-case continuation: if the H1 pace simply repeats, 2026 could close near **100** verified incidents, with recorded exposure above **$228 million**. This is an arithmetic annualization, **not a forecast**.
2. Rebound scenario: if Q1 conditions return, Europe could see renewed acceleration, especially around conferences, market rallies, or further data-leak revelations.
3. Displacement scenario: pressure in France may push crews toward neighboring countries, expatriate hubs, or jurisdictions where crypto communities are visible but enforcement capabilities are weaker.
4. Proxy escalation: attackers may increasingly target family members, employees, drivers, assistants, or public relatives because they are easier to approach and produce stronger emotional leverage.
5. Data-market escalation: leaked or insider-sourced lists linking identity, address, and crypto wealth may become a specialized criminal commodity.

The most important forecasting variable is not the price of bitcoin alone. It is the visibility of holders. Bull markets increase perceived wealth, but data exposure determines whether attackers can identify and locate that wealth.

Recommendations

The objective here is to reduce targetability, make coercion less profitable, and ensure that one threatened human cannot unilaterally release catastrophic value.

For individuals and families

- Reduce doxxing: remove portfolio screenshots, wallet addresses, home details, travel plans, conference routines, and luxury signals tied to crypto identity.
- Separate wallets by purpose: keep daily spending wallets small and isolate long-term holdings in vault structures that cannot be moved instantly.
- Geographically separate signing devices and recovery material: do not keep hardware wallets and seed phrases together, and avoid storing high-value recovery material at home.
- Adopt multi-party controls for significant holdings: use multi-signature or MPC setups where no single person can move all assets under duress.
- Implement withdrawal friction: time locks, spending limits, allowlists, and staged vaults reduce the value of immediate coercion.
- Prepare family protocols: establish emergency code words, safe contacts, check-in routines, and instructions for suspicious visitors or fake deliveries.
- Harden home access: cameras, intercom verification, delivery protocols, alarm procedures, and neighbor coordination matter for high-risk holders.

- Use a travel phone: keep high-value wallets, password managers, exchange accounts, and seed material off the phone used in public or at events.

For founders and visible holders

- Conduct a personal threat model that includes family members, home address exposure, routine predictability, travel, and public speaking schedule.
- Remove unilateral authority over treasuries, admin keys, deployment permissions, and emergency controls.
- Treat conferences and business meetings as hostile environments until verified: confirm venues, counterparties, transport, and attendance through independent channels.
- Review old interviews, social posts, podcast appearances, and photos for home, school, family, or routine leakage.
- Create a duress response plan with legal counsel, company security, custody providers, and trusted signers.

For institutions

- Map all human single points of failure: identify who can move funds, approve transactions, reset access, or expose user data.
- Use multi-party custody with policy controls: multisig or MPC should include role separation, approval thresholds, allowlists, time delays, and emergency freezes.
- Extend security training to families and assistants of high-risk personnel where appropriate and lawful.
- Minimize employee and customer data retention.
- Monitor insider access to sensitive customer or executive data with immutable logs and alerting for abnormal queries.
- Review conference security, executive travel, hotel selection, ground transportation, and meeting verification procedures.

For wallet providers

- Design for duress: support delayed withdrawals, emergency freezes, spending caps, and policies that users can configure before a crisis.
- Improve account recovery safety: recovery mechanisms should not allow attackers to turn a victim’s phone, email, or biometric unlock into full asset access.
- Build privacy-preserving UX defaults that reduce address reuse, public wealth signaling, and accidental doxxing.

For regulators and law enforcement

- Classify crypto-related physical coercion explicitly so incidents are not lost under generic robbery or assault categories.

- Audit insider access to sensitive records and investigate abnormal searches for crypto-related profiles.
- Support victim reporting pathways that reduce fear of retaliation and protect privacy where possible.

In all cases, victims should contact the competent law-enforcement authorities in their jurisdiction as quickly as possible. SEAL also provide security frameworks and resources that can help individuals and organizations reduce exposure to physical and digital threats.

How CertiK Can Help

CertiK's **OpSec Service** can help high-risk executives strengthen their operational security and understand how exposed personal information could be used to build a targeting profile. The assessment identifies the data most likely to create physical-security risks, including information linked to an executive's identity, family, residence, or movements. CertiK can then recommend practical measures to reduce this exposure and improve personal security procedures.

At the organizational level, CertiK can assess how sensitive executive or customer information may be exposed through internal systems and processes. Its services include penetration testing, key-management reviews, and assessments of resilience to phishing or unauthorized access. The objective is to identify weaknesses and implement concrete remediation before threat actors can exploit them.

CertiK's **OpSec Service** also supports the operational-resilience and business-continuity objectives established under VARA, DORA, and MiCA. CertiK can further assist organizations in addressing the broader security requirements associated with these regulatory frameworks.

CertiK Security Workspace complements these services by combining Web2 threat intelligence with on-chain investigation and AML analytics in a single platform. This gives institutions a unified view of threat-actor activity across the surface web and blockchain. It tracks and attributes threats relevant to their operations, including ransomware operators, DPRK-linked and state-sponsored groups, and cybercrime activity such as fraudulent investment platforms. By correlating off-chain intelligence with on-chain transaction flows and AML risk signals, the platform helps investigators move from an initial signal to case-ready evidence within a single workflow.

CertiK's Strategic Partnerships

In 2026, CertiK pledged to create stronger cooperation between blockchain security firms, exchanges, investigators, and international law-enforcement bodies such as INTERPOL and Europol to combat scams, exploits, money laundering, and other crypto-enabled crime. Rather than treating security incidents as isolated events, we want to increase intelligence sharing, improve incident response, support investigations, and help recover stolen assets where possible. The initiative also aims to raise security standards across the industry and protect users from increasingly sophisticated attacks.

By December 2027, we commit to:

the platform helps investigators move from an initial signal to case-ready evidence within a single workflow.

- Providing real-time threat intelligence and risk monitoring through our security tooling to aid global regulatory oversight.

- Establishing a Senior Expert Task Force to provide pro-bono technical consultation and forensic testimony for high-impact cross-border exploits and policy consultations.
- Delivering annual policy and security briefings on blockchain security for INTERPOL and UNODC-affiliated agencies.

Conclusion

The H1 2026 dataset indicates that wrench attacks continue to evolve as an organized form of crypto-enabled crime. Public reporting increasingly describes structured target selection, pre-attack reconnaissance and the use of multiple participants during a single operation.

The reporting period also highlights the expanding attack surface available to threat actors. Open-source intelligence, personal data breaches and insider access to sensitive databases can all contribute to victim identification. As a result, exposure is no longer determined solely by wallet security or custody architecture but also by the amount of personal information available about an individual.

While this report is limited to publicly verifiable incidents, the observed methodologies remain consistent across multiple jurisdictions and investigations. Continued monitoring will be required to determine whether the patterns observed during H1 2026 represent a temporary concentration of activity or a longer-term evolution in how organized criminal groups target digital asset holders.

CERTIK

Company Overview

CertiK is the largest Web3 security service provider, founded in 2017 and headquartered in New York. Since then, it has grown into a trusted risk management partner for global regulators, institutions, and Web3 innovative enterprises.

The company offers full-lifecycle risk management solutions, integrating them into institutional clients' system development lifecycles (SDLC). CertiK manages and controls risk exposure at every stage of digital asset deployment, transforming reactive patching into proactive governance.

CertiK also works closely with regulators and financial institutions across multiple jurisdictions, contributing to policy development and regulatory consultation efforts.

5,500+
Clients Served

117,000+
Vulnerabilities Detected

$600B+
Market Cap Assessed

70%+ of the Top 500 CoinMarketCap Projects Audited

Trusted Across Leading Ecosystems

BNB Chain · Bitcoin · TON · Cosmos · Cardano · Aptos · Algorand · Sui · Kaia · ZKPs

Elevate Your Web3 Journey

certik.com | bd@certik.com