CERTIK
SKYNET

SKYNET
WRENCH ATTACKS REPORT

In 2025, wrench attacks evolved into a real threat to cryptocurrency holders, demonstrating that violence is no longer an edge case, but a structural risk of digital asset ownership. The threat has shifted from opportunistic crime to highly organized, transnational operations.

1. EXECUTIVE SUMMARY

In 2025, **wrench attacks** evolved into a real threat to cryptocurrency holders, demonstrating that violence is no longer an edge case, but a structural risk of digital asset ownership. The threat has shifted from opportunistic crime to highly organized, transnational operations. Attackers now combine OSINT-driven targeting, social engineering, and extreme physical violence to extract private keys.

This report documents **72 verified** physical coercion incidents worldwide, a **75% increase** compared to 2024. Kidnapping remains the primary attack vector, while physical assaults rose by **250% year-on-year**, highlighting a clear escalation in brutality.

Europe emerged as the most dangerous region, accounting for over **40% of global incidents**. France alone recorded the highest number of attacks worldwide, surpassing the United States.

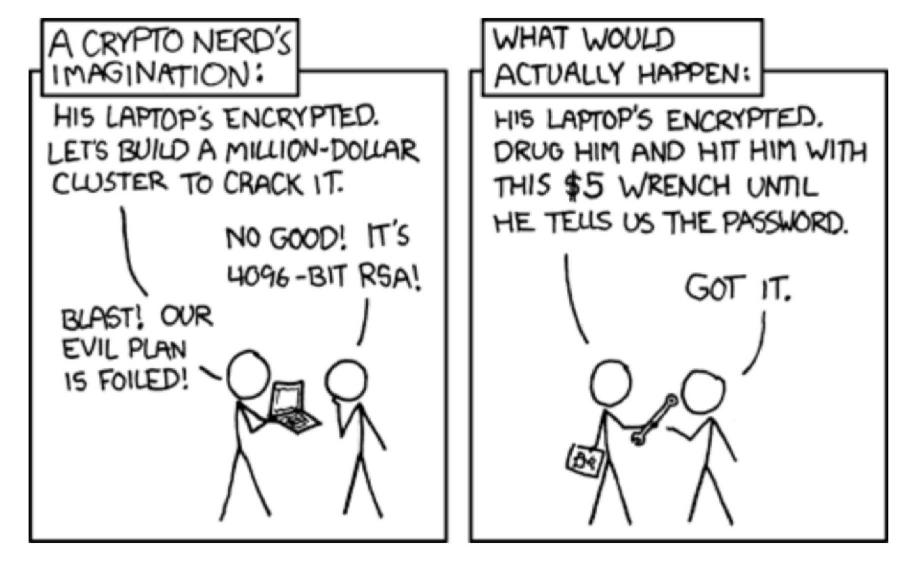
Confirmed financial losses due to wrench attacks exceeded **$40.9** million, up **44% from 2024** (though this figure significantly understates the true impact due to under-reporting, silent settlements, and untraceable ransoms). The psychological and reputational effects are severe, driving founders and high-net-worth individuals toward operational anonymity and geographic relocation.

2025 marks a clear inflection point: **physical violence is now a core threat vector in the crypto ecosystem**.

2. INTRODUCTION & CONTEXT

2.1 Definition of Wrench Attacks

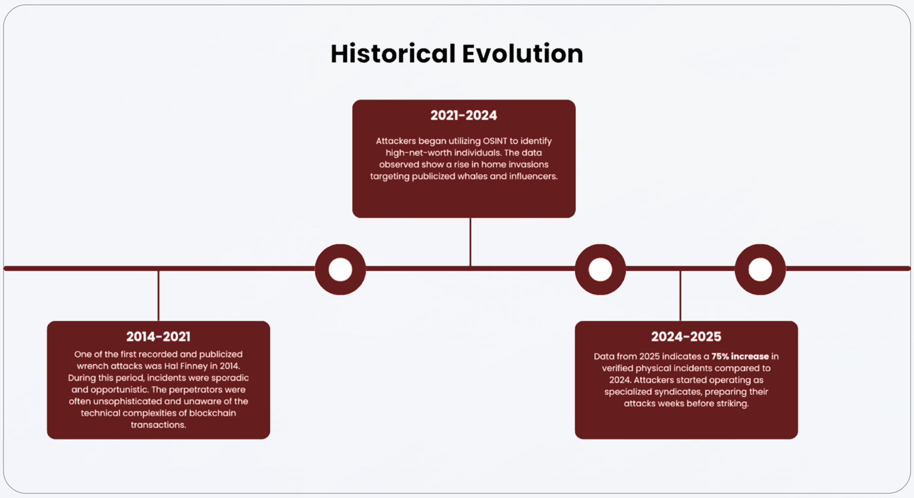
In the lexicon of digital asset security, a "Wrench Attack" is a physical coercion event where an adversary uses violence, intimidation, or confinement to compel a victim to surrender private keys or passwords. The term originates from the popular xkcd webcomic (strip #538), which satirically illustrated that sophisticated 4096-bit RSA encryption could be bypassed more effectively by a $5 wrench than by a supercomputer.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Unlike cyberattacks that exploit software vulnerabilities, wrench attacks exploit the human endpoint. They bypass cryptographic security layers by targeting the physical safety of the key holder.

2.2 Historical evolution

The trajectory of physical crypto-crime has shifted from opportunistic theft to industrialized, transnational organized crime.



Historical Evolution

2014–2021

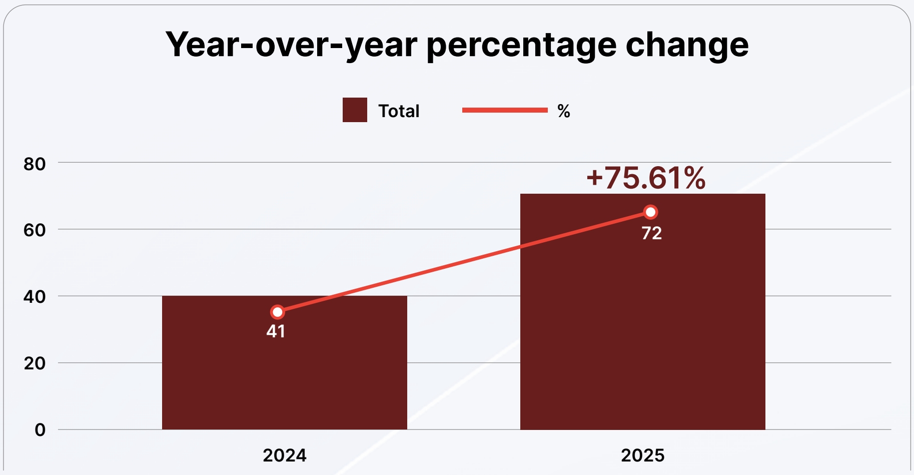
One of the first recorded and publicized wrench attacks was Hal Finney in 2014. During this period, incidents were sporadic and opportunistic. The perpetrators were often unsophisticated and unaware of the technical complexities of blockchain transactions.

2021–2024

Attackers began utilizing OSINT to identify high-net-worth individuals. The data observed show a rise in home invasions targeting publicized whales and influencers.

2024–2025

Data from 2025 indicates a **75% increase** in verified physical incidents compared to 2024. Attackers started operating as specialized syndicates, preparing their attacks weeks before striking.



2.3 Differentiation from other attacks

While cyberattacks (phishing, malware, drainers) target crypto wallets, wrench attacks target the person who holds the private keys to those wallets.

- **The Technical Paradox:**
  As cryptographic standards and hardware security become more and more sophisticated, the cost of a technical exploit rises exponentially.

- **Human Failure:**
  It is easier to frighten and threaten a human to transfer their cryptocurrency than it is to hack a protocol or a wallet.

2.4 Scope of the report

This report analyzes the global landscape of physical crypto-threats from January 1, 2025, to December 31, 2025. It draws upon verified incident reports from law enforcement and publicly disclosed victim accounts.

1. **Jurisdictional Variance:**
   In many regions, law enforcement agencies still lack the frameworks or training to properly record "crypto-theft" as a distinct crime, often categorizing it generically as robbery or dismissing it entirely due to the intangible nature of assets.

2. **Cultural & Individual Factors:**
   Victims often choose not to file complaints due to fear of retaliation, shame, or a lack of trust in local authorities' ability to recover funds.

3. **Black Market Silence:**
   A subset of attacks targets individuals holding illicit funds (e.g., tax evasion or grey-market earnings), who are unable to seek legal recourse without incriminating themselves.

Therefore, the statistics in this report should be viewed as the tip of the iceberg, rather than a full scope of the wrench attack landscape.

3. TAXONOMY & CLASSIFICATION

3.1 Types of Wrench Attacks

Based on our verified incident data, we categorize physical coercion events into ten distinct categories. These categories reflect the varying levels of violence and complexity employed by attackers.

- **Armed Robbery:**
  The theft of digital assets where the perpetrator uses a lethal weapon (gun, knife, etc.) to immediately threaten the victim. The encounter is typically of short-duration and high-intensity.
- **Blackmail:**
  Coercion based on the threat of revealing compromising information (doxxing, private data) unless payment is made. It becomes a "wrench attack" variant when combined with physical stalking or threats to family safety.
- **Extortion:**
  The practice of obtaining assets through force or threats. Unlike robbery, extortion can be a prolonged campaign of pressure, often involving threats against the victim's business or loved ones.
- **Home Invasion:**
  The unauthorized and forceful entry into an occupied private residence.
- **Kidnapping:**
  The abduction and unlawful detention of a person against their will.
- **Murder:**
  The unlawful killing of a victim during the commission of a crypto-theft. This represents the most extreme outcome.
- **Physical Assault:**
  The infliction of bodily harm without necessarily using a weapon. This includes beatings used to intimidate the victim into unlocking devices.
- **Ransom:**
  A specific demand for payment for the release of a kidnapped victim. In crypto-cases, the ransom is almost exclusively demanded in privacy coins (Monero) or via mixers to obfuscate the trail.

- **Robbery:**
  The taking of property (phones, hardware wallets) from a person by using force or fear, but without a lethal weapon. Common in opportunistic street-level attacks.

- **Torture:**
  The deliberate infliction of severe physical or mental pain to force the disclosure of information. This marks a shift from simple theft to extreme brutality, as seen in the January 2025 Ledger co-founder cases.

3.2 Classification by target

Attackers select their victims based on a calculated risk-reward analysis, prioritizing targets with high potential payouts and exploitable security vulnerabilities.

Retail
High-net-worth individuals who publicly disclose their holdings on social media typically lack professional security details, making them soft targets with high payouts.

Industry Executives & Founders
C-level executives and protocol founders represent high-value targets. While they often employ personal security details, they remain vulnerable during transit or at public events.

Family Members & Close Friends
Also called Proxy Targets. Criminals weaponize emotional bonds by targeting spouses, children, or elderly parents to force compliance from the primary holder.

- **Psychological Leverage:**
  Attackers understand that victims are more likely to bypass security protocols immediately when a loved one is threatened.

- **Lower Security Profile:**
  Family members often lack the rigorous OpSec training of the primary target.

OTC Traders
Individuals engaging in face-to-face cash-for-crypto transactions. These meetings are frequently ambushes masquerading as legitimate business deals. The fake meetup tactic lures traders to a controlled location where they are robbed immediately upon revealing proof of funds.

3.3 Classification by access vector

The **access vector** is the mechanism by which attackers breach the victim's security perimeter and extract private keys or passwords.

Physical Security Breaches represent the initial penetration phase. Attackers employ a range of techniques to overcome physical barriers such as locks, alarms, and gated communities. For example the **Doorbell Vector**, where perpetrators impersonate delivery personnel, utility workers, or law enforcement to gain entry into occupied residences. In more sophisticated operations, criminals conduct weeks of surveillance using **OSINT** to identify when targets are most vulnerable.

Coercion Techniques escalate the attack from mere trespassing to forcible extraction of credentials. Unfortunately, many recent incidents have involved prolonged **torture** sessions. In cases involving hardware wallets with PIN protection, victims are beaten until they unlock their device, rendering cold storage ineffective against determined adversaries.

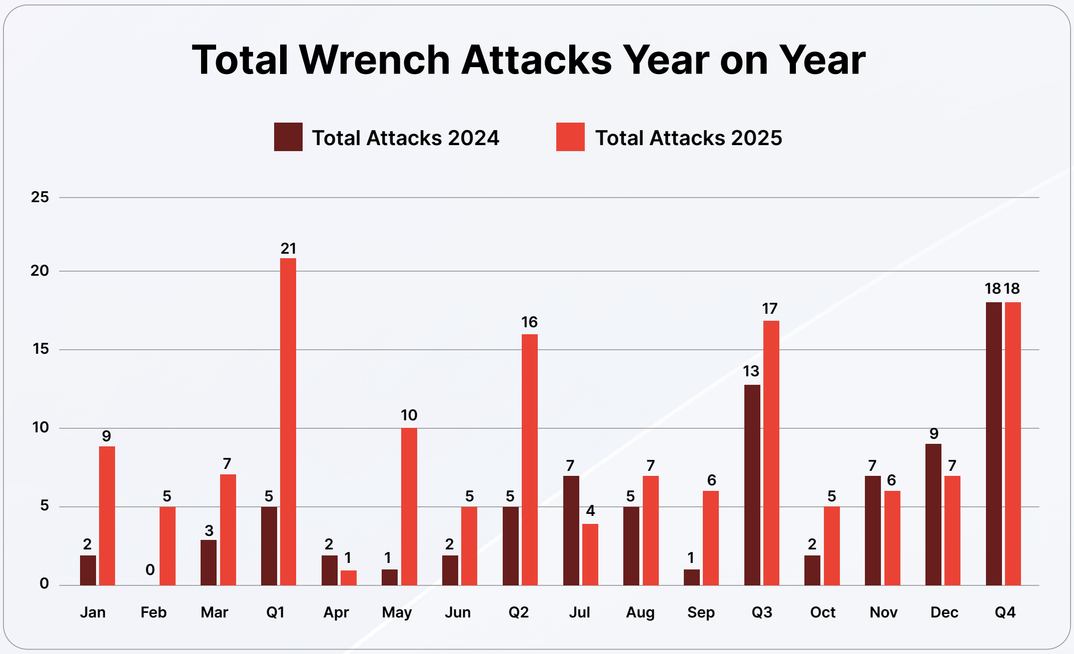
Social Engineering Vectors precede physical attacks, blurring the line between cyber and physical crime. The **Honey Pot** technique involves creating fake romantic relationships or business partnerships to lure victims into controlled environments where they can be ambushed. This allows them to map a victim's routine and pinpoint the precise window for a physical strike.

4. 2025 THREAT LANDSCAPE

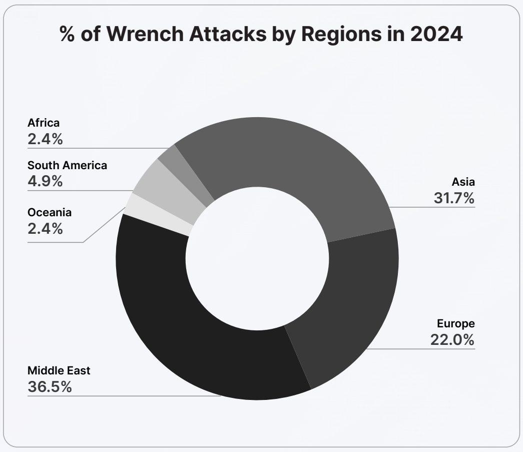
2025 is officially the most violent year in the history of cryptocurrency, with 72 recorded incidents compared to 41 in 2024, representing a 75% increase.

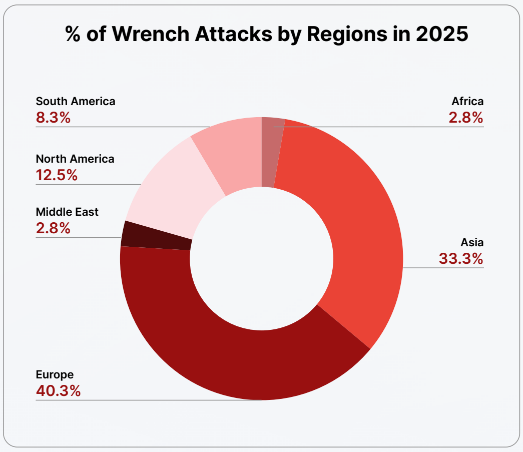
4.1 Global statistics in 2025

Q1 2025 saw an explosive start with **21 incidents** in a single quarter. While Q2 saw a slight dip with **16 incidents**, activity slightly increased in Q3 and Q4 with **17 and 18 incidents** recorded, respectively. May was the most violent month with **10 incidents**, just ahead of January with **9 incidents**.



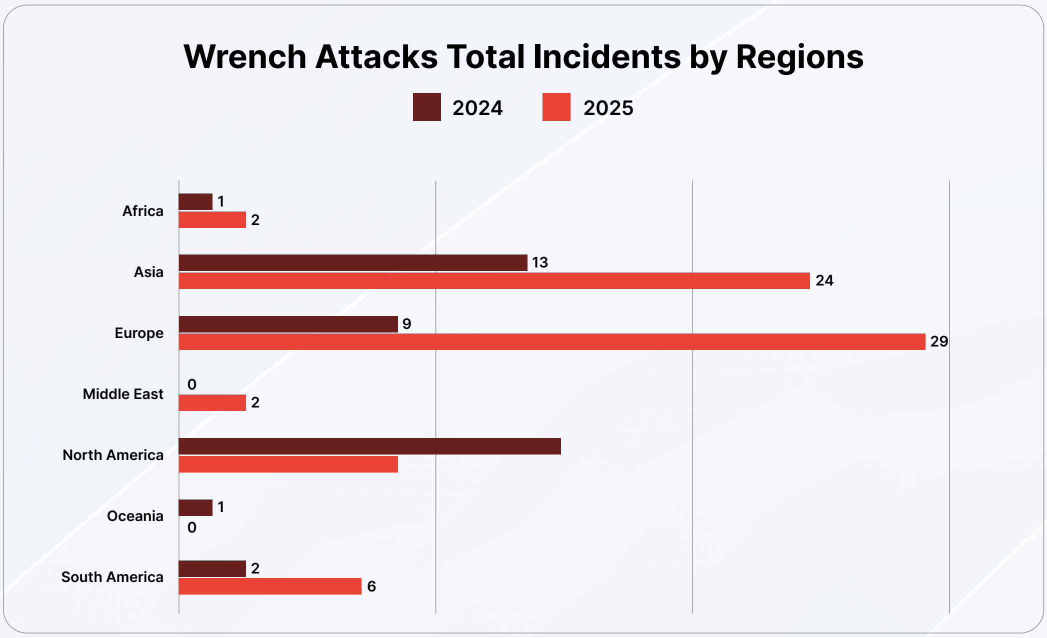
4.2 Geography of attacks


% of Wrench Attacks by Regions in 2024


% of Wrench Attacks by Regions in 2025

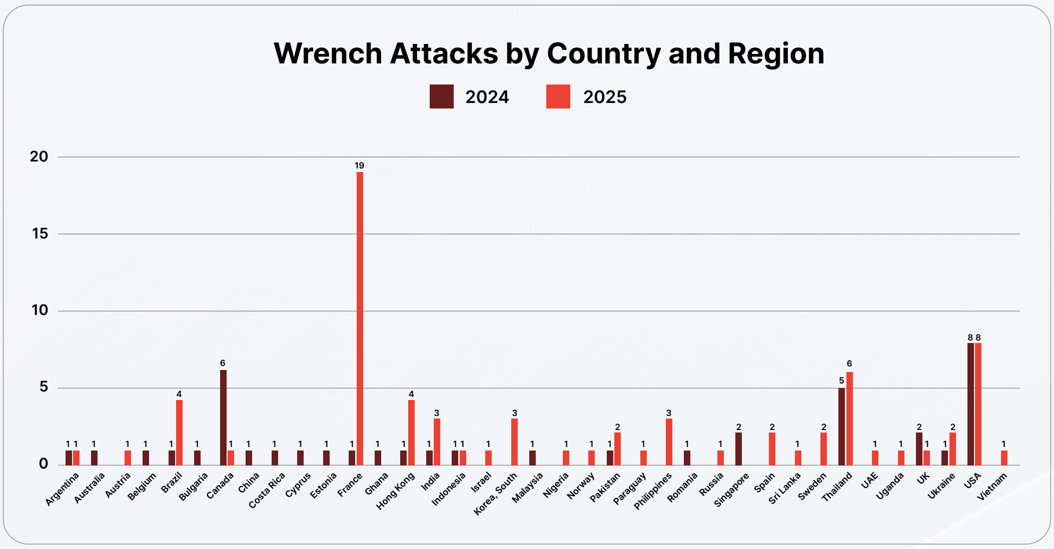
The geographical distribution of attacks has shifted significantly. The most notable trend is the explosion of violence in Europe.

In 2024, Europe accounted for **22%** of global incidents with 9 attacks, but in 2025, this figure exploded to **40.3%** with **29 attacks**, making Europe the single most dangerous region for crypto-holders. This surge is driven by the proliferation of crypto-jacking groups in Western Europe, specifically in France, Spain, and Sweden. In 2025, France is the country with the highest number of incidents in the world with **19 attacks**, far ahead of the USA with **8 recorded incidents**.


Wrench Attacks Total Incidents by Regions

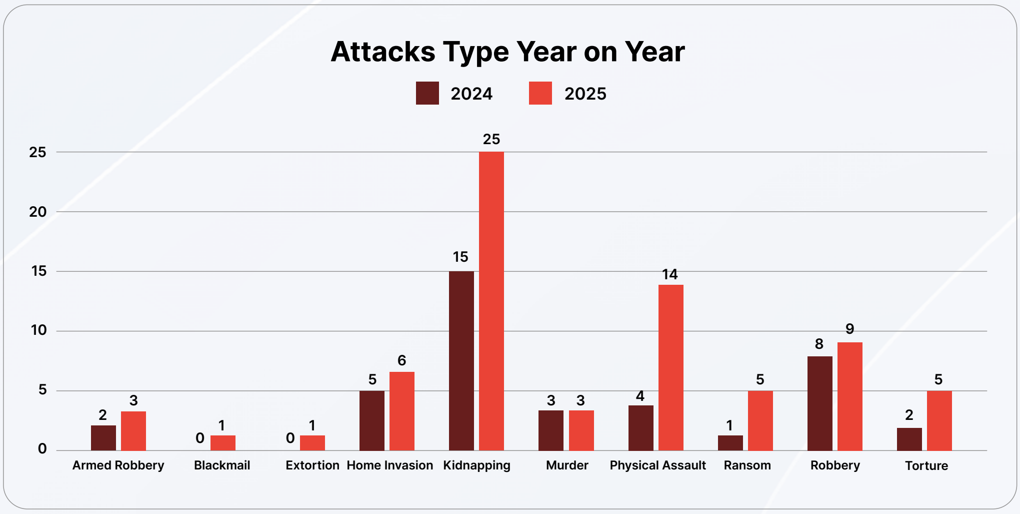
In terms of the percentage share of wrench attacks by region, North America saw a drop from **36.6%** of attacks in 2024 to **12.5%** in 2025, dropping from **15 to 9 incidents**. This does not necessarily imply that the US is a safer place, but rather that the global volume has expanded elsewhere.

Asia remains a persistent high-risk zone, showing stability moving from **31.7%** in 2024 to **33.3%** in 2025. The threat here remains concentrated on crypto-tourists and expats in hubs like Thailand and Hong Kong.


Wrench Attacks by Country and Region

4.3 Year on year evolution (2024 vs 2025)

Physical attacks have evolved from opportunistic crime to highly organized extortion. Of the **72 incidents** reported in 2025, **kidnapping** remains the dominant vector this year with **25 incidents**, a sharp increase from 2024 (**15 incidents** at an increase of **66%**). Violent attacks (**Physical Assault**) have also increased from **4 recorded incidents** in 2024 to 14 in 2025, representing a **250% increase**.


Attacks Type Year on Year

5. MOST NOTABLE CASES

David Balland & Wife (France)

On January 1, 2025, David Balland, Ledger's co-founder, was abducted alongside his wife from their residence in Méreau, France. The attack was executed by a highly organized transnational crew. The kidnappers demanded a ransom of 10 million euros in cryptocurrency. The attackers employed extreme brutality, severing one of Balland's fingers and sending video evidence to his business associates via a Southeast Asian WhatsApp number accessed through a VPN. The crisis ended after a 48-hour manhunt involving 230 GIGN operatives. Balland was ultimately rescued, wounded but alive, while his wife was discovered bound in the trunk of a stolen vehicle. Ten suspects were arrested and charged, revealing a sophisticated network operating out of Morocco.

Danylo Kuzmin (Austria)

In December 2025, 21-year-old Danylo Kuzmin, son of a Ukrainian politician, was murdered in Vienna, Austria in a honey pot trap. He was lured to the Sofitel Vienna hotel garage by a trusted 19-year-old acquaintance. Once in the underground parking lot, he was ambushed by the acquaintance and a 45-year-old accomplice. Kuzmin was subjected to severe torture to force him to reveal the passwords to two specific wallets. The attackers successfully drained approximately $200,000 in crypto before murdering him and setting his car on fire to destroy evidence. The suspects fled to Ukraine but were detained shortly after, with authorities recovering substantial amounts of cash converted from the stolen crypto.

Roman & Anna Novak (UAE)

In October 2025, Roman Novak, a crypto-entrepreneur linked to the Fintopio platform, and his wife Anna were lured to a business meeting in Hatta, UAE. This ambush was meticulously planned, involving multiple decoy vehicles to separate the couple from their driver. The attackers tortured them with the goal of stealing $500 million in private keys. When the extracted wallets failed to yield the expected liquidity, however, the kidnappers executed both victims. Seven suspects, primarily Russian nationals, were later arrested.

6. ATTACKER PROFILES & MODUS OPERANDI

6.1 Attacker profiles

The vast majority of recorded and analyzed attacks are carried out by **groups of men**, ranging from **minors** as young as 16 to individuals well into their 50s. Over the years, a certain professionalization of these attacks has emerged. The groups operating on the ground are often the armed wing of sponsors who are sometimes located outside the country where the attacks take place.

6.2 Tactics, Techniques & Procedures (TTPs)

The standard operating procedure for a wrench attack has evolved into a meticulous process. **Surveillance** has shifted from physical tailing to digital exhaust analysis. Attackers exploit data from various leaks combined with real-time location data. For **home invasion breaches**, impersonating delivery drivers or utility workers remains the most successful entry method exploiting the victim's psychological readiness to open the door. Once inside, the **extractio**n phase can last from a few hours to several days.

6.3 Social engineering playbooks

Social engineering has migrated from digital phishing to physical entrapment, with the **Honey Pot** technique. Victims are lured to physical locations under the guise of romantic dates, business partnerships, or OTC deals, only to be ambushed in controlled environments. **Trusted Insider** attacks have also been observed, where acquaintances act as spotters for criminal groups.

6.4 Technical infrastructure & OpSec

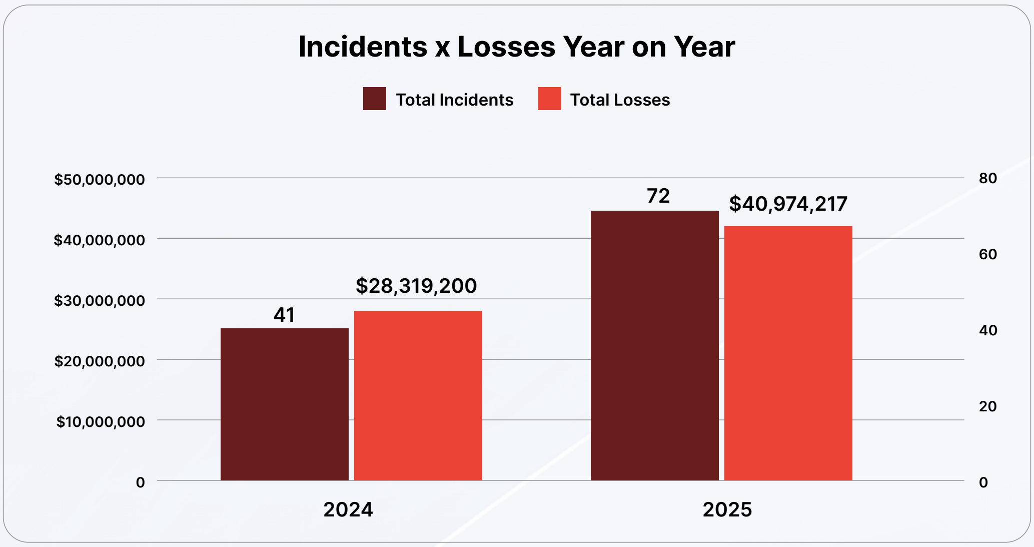
Attackers utilize a technical stack to evade detection during and after the crime. To communicate, they employ encrypted messaging apps on burner phones, often routing traffic through multiple VPNs. Physically, they can deploy **Faraday bags** and signal jammers during home invasions to isolate the victim's devices from cellular and Wi-Fi networks. If necessary, they also isolate the victim from the rest of the family in order to extract valuable information.

7. IMPACT ASSESSMENT

It is important to note that accurately quantifying the financial impact of these crimes remains extremely complex. The figures presented in this section rely on available public data, which may remain unreported or confidential. These numbers aggregate confirmed thefts, funds that were potentially frozen, ransom demands that may have been partially paid, etc. The totals should be viewed as indicative figures.

7.1 Financial impact

In 2024, total recorded losses from physical attacks stood at approximately **$28.3 million** across **41 incidents**. In 2025, this figure jumped to over **$40.9 million** across **72 incidents**, representing a **44% increase** in stolen value.



The data indicates that attackers are no longer focused only on whales, but also on individuals with modest holdings, simply because they are known to own crypto.

7.2 Psychological/reputational impact

The psychological fallout is perhaps the most damaging long-term effect. The rise in extreme violence has created a climate of **fear** that is driving high-net-worth individuals into hiding. Founders and early adopters are scrubbing their digital footprints, withdrawing from public events, or **relocating** to jurisdictions with lower crime rates.

7.3 Ecosystem-wide effects

The normalization of physical violence is altering behavior across the sector. There is a resurgence of pseudo-anonymity. **Publicly doxxed** profiles are now viewed as a liability rather than an asset.

8. DETECTION & MITIGATION STRATEGIES

8.1 Red flags & early warning indicators

Recognizing pre-attack indicators can provide the time needed to evaluate the situation or alert authorities:

- **Unexpected 2FA:**
  Receiving unsolicited Two-Factor Authentication codes indicates that an attacker has already compromised your digital credentials and is probably trying to locate your physical device or assess your responsiveness.
- **Physical Anomalies:**
  A delivery driver arriving for a parcel not ordered, workers checking meters without appointment, or repeated hang-up calls to a landline to check occupancy schedules.
- **Honey Pot:**
  Unexpected contact from long-lost acquaintances or new business opportunities that require an in-person meeting.

8.2 Best practices for individuals

For individuals, the goal is to make physical coercion futile. A **decoy wallet** is a viable option: maintain a wallet with a small but plausible amount of funds that can be surrendered immediately. Never keep the seed phrase and the hardware wallet in the same location. Ideally, the seed phrase should be stored in a bank safe deposit box. Most importantly, **stop flexing**. Remove crypto-related apps from your primary smartphone used in public, and use a dedicated laptop for high-value transactions that never leaves your secure perimeter.

8.3 Advanced defense frameworks

For family and high-net-worth individuals, security must be institutionalized to remove the human single point of failure.

- **Multi-Signature:**
  Implement a 2-of-3 or 3-of-5 signature scheme.
- **Time-Locked Contracts:**
  Use smart contracts to enforce a mandatory delay on any withdrawal over a certain threshold.

9. EXPECTED THREAT EVOLUTION

For the years to come, we anticipate a shift toward more psychologically coercive and highly scalable threat models. Attackers will increasingly rely on **deepfake extortion**, leveraging harvested biometric data to generate hyper-realistic proof of life content, such as video calls from a supposedly kidnapped child or spouse demanding an immediate ransom. In parallel, **AI-driven social engineering** will reach industrial scale, with autonomous agents capable of managing thousands of simultaneous honeypot interactions (fake relationships, fabricated investor meetings, etc).

10. RECOMMENDATIONS

These recommendations prioritize reducing the feasibility of coercion and reducing targetability.

10.1 For individuals

- **Minimize doxxing surface:**
  avoid posting wallets addresses, portfolio screenshots, travel plans, or identifiable routine markers tied to crypto activity.

- **Build a setup:**
  maintain a decoy wallet and a separate primary vault architecture so coerced access does not equal catastrophic loss.

- **Enforce geographic separation:**
  never co-locate seed material and signing devices; avoid keeping recovery material at home.

- **Reduce mobile single-point-of-failure:**
  use a travel phone with minimal accounts, disable lock-screen previews, and keep high-value wallets off daily devices.

10.2 For institutions

- **Multi-party control:**
  Use multi-signature or MPC with policy controls (whitelists, limits, and delayed withdrawals).

- **Implement transaction friction:**
  Time-delays for large withdrawals.

- **Formalize executive protection:**
  Threat modeling for leadership and travel security standards.

- **Proxy-target resilience:**
  Extend security training and response protocols to family, close friends, employees, etc.

CONCLUSION

2025 confirmed that **wrench attacks** have become a distinct category of incidents within the ecosystem. They are characterized by increasingly aggressive coercion tactics and the strategic targeting of victims' close associates. Although reported losses and incident counts have risen sharply, these metrics likely represent only the visible portion of a broader phenomenon. With **72 major verified incidents**, the industry faces a true humanitarian crisis. As we enter 2026, the era of exclusive reliance on seed phrases is over. More than ever, humans remain the single point of failure.

Check out the **Skynet** platform today and elevate your Web3 journey by learning more about the security insights of the projects highlighted in this report and reading more on the CertiK blog hub.

Protect your community and your organization today. Visit **CertiK.com** or get in touch at **bd@certik.com**.

CERTIK SKYNET

COMPANY INTRO

Founded in December 2017 in New York by two professors from Yale University and Columbia University, CertiK is the largest Web3 security service provider.

CertiK offers a wide range of products and services to support the Web3 industry, project teams, and users alike. CertiK's products and services span the entire lifecycle of project development, from incubation and early stages, to growth and maturity.

With a highly skilled technical team, CertiK stands out for its expertise in formal verification technology, artificial intelligence, and academia. CertiK's leaders also collaborate closely with global government bodies to develop supportive Web3 compliance and regulatory frameworks.

>$600B
ASSETS SECURED

180,000+
VULNERABILITIES DETECTED

5,000+
CLIENTS SERVED

>70% OF TOP 500 CMC PROJECTS AUDITED

DIVERSITY IN ECOSYSTEMS