



— BRIEFING / 016 · SEPTEMBER 2026

THE ADDRESS STAYS HOT

Three crews attacked the same rural French house in under a month this summer. The family living there owns no cryptocurrency. The targeting file that sent the attackers was two years out of date, and it did not matter.

EXECUTIVE RISK SERVICES

Prepared for worst-case scenarios. So you don't have to.

info@executiveriskservices.com · referral or invite only

THE CASE

A young couple bought a modest house in the Somme department of northern France about two years ago. The previous owners, a retired couple, had built an estimated one million euros in cryptocurrency, and at some point their tax records and home address were exposed and circulated on the dark web, flagged as belonging to high-value crypto holders. The file kept working long after the facts changed. Over roughly one month this summer, three separate groups attempted to enter the property in search of wealth that no longer lived there. In the second attack, residents were restrained and assaulted. The third attempt failed when an alarm the couple had installed after the second attack triggered a fast police response. In August, a court in Amiens sentenced two men for their role in that final attempt. One had reportedly been recruited for the job through a messaging app. The couple, who have no connection to cryptocurrency, are now reportedly trying to sell the house.

3 HOME INVASIONS IN UNDER A MONTH

2 YRS SINCE THE FLAGGED OWNERS MOVED

77 CRYPTO-LINKED PHYSICAL INCIDENTS IN FRANCE, H1 2026

THE FILE POINTS AT A PLACE, NOT A PERSON

The uncomfortable insight in this case is not that criminals use leaked data. It is that the leaked data has a shelf life measured in years, and that its unit of targeting is the address. Researchers tracking these attacks describe a shift toward data-driven targeting, in which crews merge tax leaks, breach dumps, exchange records, and residential data into standing files of households believed to hold crypto. Once an address enters such a file, nothing removes it. Sales, moves, and changed circumstances are invisible to the marketplace where the file trades. Whoever occupies the flagged address inherits the exposure.

The numbers around this case say it is not isolated. French authorities counted 77 crypto-related physical incidents in the first half of 2026, up from 45 in the same period a year earlier. Verified home invasions in the global dataset rose from a single case to twenty year over year. The address layer is doing real work in that growth.

WHO INHERITS THE RISK

Three groups carry exposure they did not create. Buyers of properties previously owned by visible or leaked crypto holders, who inherit a hot address with the deed. Sellers who move but whose old address still anchors their leaked identity, and whose new address can be joined to it through routine records. And families or staff who live at a flagged address without any connection to the assets at all. None of these groups shows up in a conventional threat model built around the principal's current holdings. All of them show up in the criminal file.

WHAT BROKE THE PATTERN

It is worth being precise about the one protective fact in this case. The first two attacks succeeded in reaching the residents. The third failed, because after the second attack the couple installed an alarm, and the response it triggered led to arrests and sentences. A single detection layer, added late, changed the outcome and imposed real cost on the attackers. That is the general lesson ERS draws across the residential caseload: detection and response layers do not need to be elaborate to be decisive, they need to exist before the attempt rather than after it.

THE PROTECTIVE READ

Four disciplines follow. First, treat address history as live exposure. A residential risk assessment should cover not just the current property but what leaked and public data says about every address tied to the family. Second, when buying or selling a notable property, include data exposure in diligence, the same way title and survey are included. Third, layer detection at the residence and connect it to a response you have actually rehearsed. Fourth, maintain a household protocol that everyone at the address knows, including people with no connection to the assets, because the file does not distinguish and neither will the crew.

SOURCES AND METHOD

This briefing draws on August 2026 reporting from The Block, IBTimes UK, Crowdfund Insider, and French court coverage, alongside H1 2026 incident data from blockchain security researchers and French authorities. We do not identify the family, describe entry methods, or detail the property's security arrangements. The pattern is the point, and the pattern is what protects the next address on the list.

© 2026 Executive Risk Services, LLC.