— BRIEFING / 017 · SEPTEMBER 2026

THE FRONT DOOR, NOT THE FIREWALL

Mid-year data on violent crypto attacks confirms a migration ERS has watched build for three years. The attack surface is no longer the exchange, and increasingly it is not the street. It is the residence.

EXECUTIVE RISK SERVICES

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

info@executiveriskservices.com · referral or invite only

— 01 / THE NUMBERS

THE NUMBERS

Chainalysis' mid-year review of violent, physically coercive crypto incidents counts 46 documented cases globally through late June 2026, compared with 40 at the same point in 2025. Value stolen in these attacks reached a record $58 million in 2025 and stands at roughly $30 million at mid-year, a pace that threatens the record. Within the incident mix, the composition is the real finding. Kidnappings have held a stable share year over year. Home invasion robberies have grown from 26 percent of incidents in 2023 to 37 percent in 2026. Every serious observer of this category also notes undercounting: victims often stay silent, and cases surface only when investigations conclude.

37% OF 2026 INCIDENTS ARE HOME INVASIONS, UP FROM 26% IN 2023

46 VIOLENT INCIDENTS DOCUMENTED THROUGH LATE JUNE

$30M TAKEN BY FORCE IN SIX MONTHS, AGAINST A $58M RECORD YEAR

— 02 / WHY THE MIGRATION WAS PREDICTABLE

WHY THE MIGRATION WAS PREDICTABLE

For a decade, the industry invested against digital theft. Exchange security, cold storage, multisignature controls, withdrawal allowlists, and transaction monitoring all raised the cost of attacking the technology. Those investments worked, and their success changed the attacker's arithmetic rather than ending the threat. A holder who cannot be hacked can still be coerced, and coercion requires access to the person. The person is most predictable, most isolated, and most surrounded by leverage, meaning family, at home. The migration from firewall to front door is not a surprise. It is the market clearing.

— 03 / THE SOPHISTICATION SIGNAL

THE SOPHISTICATION SIGNAL

Chainalysis' on-chain analysis of proceeds adds a second finding that program owners should weight heavily. Laundering behavior across these cases spans a spectrum, from attackers who cash out directly at centralized exchanges, which suggests improvisation, to routing through laundering infrastructure in ways consistent with embedded organized crime. The presence of the capable end of that spectrum means planning, patience, and repeatability are in the market. Programs designed against opportunists underprice the threat.

— 04 / WHAT IT CHANGES FOR RESIDENTIAL PROGRAMS

WHAT IT CHANGES FOR RESIDENTIAL PROGRAMS

ERS draws four program implications. First, the residential risk assessment is no longer optional for digital asset principals; it is the control that addresses where the threat actually presents. That assessment should cover the property, its approaches, and the data exposure that makes the address findable. Second, detection belongs ahead of the perimeter, not at the bedroom door. Time is the resource every response plan spends, and detection is where time is bought. Third, the household protocol must include everyone who lives or works at the address, because coercion cases consistently use whoever is present as leverage. Fourth, duress procedures for the principal should assume family members are in scope, since the data says they increasingly are.

— 05 / THE STRATEGIC READ

THE STRATEGIC READ

Boards and family offices should read the mid-year data as a resourcing question. Spend on the digital layer succeeded and should continue. But the marginal dollar of protection for a digital asset principal now buys more at the residence than at the exchange, and the gap between digital and physical maturity is itself a signal attackers act on. Closing that gap is the work.

SOURCES AND METHOD

This briefing draws on Chainalysis' 2026 mid-year analysis of violent crypto incidents and ERS caseload observation. We cite aggregate figures only, detail no individual incidents, and describe protective principles rather than security configurations. Restraint here is policy, not omission.