From Dark Web Portals to Prison: How Czech Investigators Exposed a Crypto-Enabled CSAM Scam

The Police of the Czech Republic

Region
Europe

Industry
Law Enforcement

Products Used
TRM Forensics

Problem

Criminals used fraudulent dark web portals to scam CSAM consumers

Results:

- Operator jailed in Czech Republic
- Second suspect identified abroad
- Hundreds of CSAM consumers flagged to Europol

The National Organized Crime Agency (NCOZ) is a specialized branch of the Czech Police's Criminal Police and Investigation Service, operating nationwide to tackle serious and organized crime. Within NCOZ, the Cyber-Enabled Crime Division functions as the country's central hub for responding to digital threats – including financial crime, network intrusions, and illicit cryptocurrency activity.

Radek Matějka, senior cryptocurrency investigator, describes his team's mission as providing expertise across the country: "We trace for our agency, but we also provide tracing for other police agencies. We are the main methodology experts on virtual currency investigation for all Czech law enforcement agencies." His role has been critical in building investigative capacity, developing seizure methodologies, and training colleagues to handle the challenges of tracing funds on both traditional cryptocurrencies and emerging smart contract-based platforms.

From the dark web to Prague

In 2023, investigators from NCOZ were alerted to suspicious activity linked to hidden web portals on the Tor network. These portals distributed child sexual abuse material (CSAM) in order to convince buyers to pay for expanded access to content that in reality didn't exist. The operators accepted cryptocurrency payments but did not deliver any content, knowing that their scam would not be reported.

The initial intelligence came from blockchain analysis identifying more than ten interconnected dark web portals accepting cryptocurrency payments. "We saw that all of these sites were depositing funds into the same wallet at the same time," recalled Carolina Christofoletti, TRM's blockchain intelligence analyst responsible for the CSAM threat category. "That told us we weren't looking at isolated scams but a coordinated network that could be disrupted with a single trace."

For Matějka, the suspicious transactions were a signal worth pursuing. "It was the point where I started the investigation and tried to identify the operator," he recalled. His team began piecing together what initially looked like scattered deposits and withdrawals but soon revealed the outlines of a larger operation.

The case quickly crossed into his specialty: cryptocurrency — with payments tracing back to cash-out points at Bitcoin ATMs in the Czech Republic. Recognizing that these financial flows could provide a path to the perpetrators, Matějka's unit launched an inquiry to connect the blockchain evidence with real-world identities.

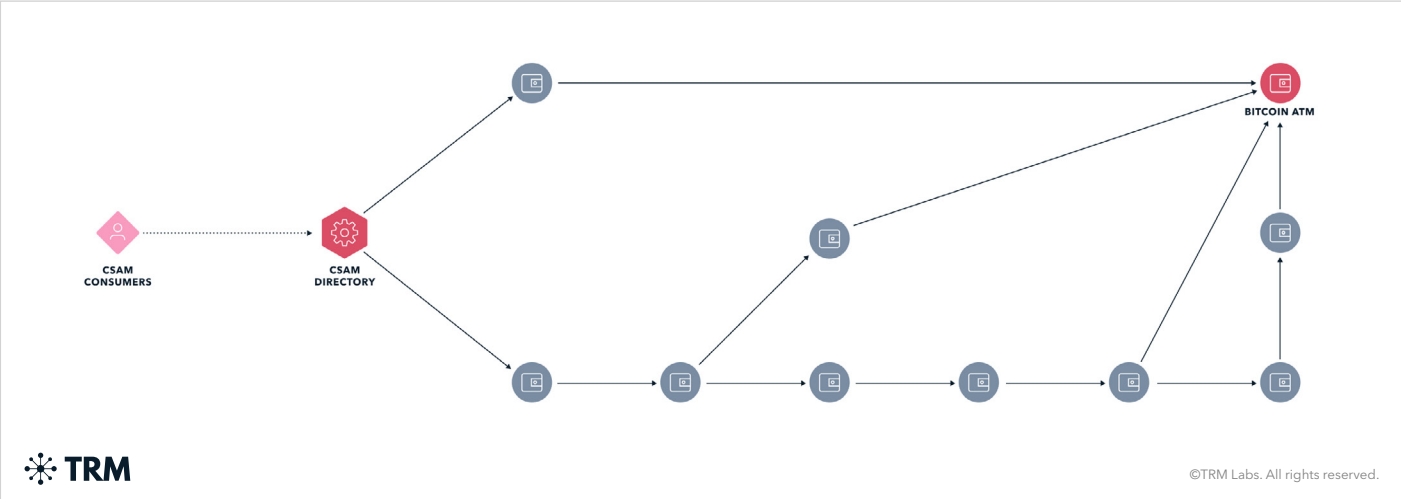
The investigation: Linking wallets to faces

The investigation began with the flow of cryptocurrency itself. Matějka noticed that deposits from the CSAM websites on the dark web were routed to Bitcoin ATMs within a few hops. Each ATM created a unique address for deposits, which was then funneled to a consolidation wallet. This pattern became the first tangible lead.

Christofoletti's analysis had already revealed a complex network of intermediary wallets connecting the portals to Bitcoin ATMs in Prague. "Even though the operators rotated wallets weekly — and later monthly — we could keep following them," she explained. "Each time they changed an address, we updated our attribution to maintain full coverage."

Next came collaboration with the ATM operator. "The CEO of the company was very helpful and proactive," Matějka recalled. The operator provided transaction records and, crucially, images from ATM cameras. These pictures allowed investigators to connect digital wallets with real people withdrawing cash.

Working jointly with Matějka, Christofoletti and a colleague mapped the ATM infrastructure to confirm that all withdrawals converged at a single machine whose transactions flowed to a centralized exchange. “Being able to link the on-chain payments to a specific ATM was the breakthrough,” she said. “It meant there was no place left for the criminals to hide when cashing out.”



The first suspect was identified when he attempted a withdrawal and — under pressure from a second-factor check — entered his own phone number. That number matched records in police databases, giving investigators a confirmed identity.

A second suspect proved harder to trace. Facial recognition software run against Czech databases yielded no results. But when investigators shared ATM images with a major exchange, the exchange’s Know Your Customer (KYC) system quickly returned a match, confirming the suspect had an account in his name. The swift identification showed how partnership between investigators and exchanges can collapse criminal anonymity on the blockchain.

In parallel, Matějka’s team discovered that the suspect had used the same wallets displayed on the CSAM websites to make payments through a Czech payment processor tied to one of the country’s largest e-commerce sites. The transactions revealed invoices connected to a registered customer account, offering a second, independent thread of evidence. “It was another way we could identify him,” Matějka noted, underscoring how multiple financial touchpoints confirmed the suspect’s identity.

With identities established, prosecutors secured a search warrant. At the suspect’s residence, investigators seized digital devices that tied him directly to the administration of the portals. “The analysis of the data from his computer showed clearly that he was the operator. The addresses we found matched exactly the ones from the websites,” Matějka explained.

Investigators discovered that the suspects had hosted the dark web servers from their own homes — a reminder of how low-tech the infrastructure behind a global network can be. “They were literally running the servers from their living rooms,” Matějka said. “It shows how critical it is to connect the blockchain side to the physical world.”

Perpetrators brought to justice, hundreds more exposed

The operation led to decisive results. The first suspect was prosecuted and imprisoned in the Czech Republic. The second suspect, a Ukrainian national, fled before prosecution but was identified and linked to the case.

For Christofoletti, seeing the case move from analysis to arrest was personal validation. "Waking up to the message that the suspects were arrested and the websites were down was amazing," she said. "It's the moment you realize that tracing crypto can actually protect children."

The case extended beyond the main perpetrators. Because the fraudulent portals collected payments from individuals seeking illicit material, investigators were able to trace hundreds of attempted users. This intelligence was shared with Europol's Analysis Project Twins (AP Twins), the unit specializing in child sexual abuse material investigations across Europe. "We identified hundreds of users who sent crypto to these addresses and provided the information to Europol," Matějka said.

For Matějka, the case underscored how blockchain investigations can turn digital transactions into actionable leads. What began as fraudulent websites on the dark web ended with perpetrators behind bars and a wealth of intelligence to support international partners. "Without professional tools and collaboration, this kind of case would be impossible to solve."

The case also illustrates how scam-based CSAM networks can be high-value targets. "If you take down one scam operator, you remove dozens of portals and the illicit material they used to lure users," Christofoletti noted. "A single trace can clean up a large part of the dark web."

Watch Radek Matějka's story

Looking for more? Explore all our case studies.