Operation Klonen: a supplier's bad update, thirty million euros

A payment processor pushed a faulty software update. The defect sat in the booking process German online banking customers relied on. Over four days in November 2023 a criminal network took about thirty million euros out through it.

INCIDENT DETAILS · 5WH

Who Brazil's Federal Police and Germany's BKA, with Frankfurt prosecutors and authorities in Spain and Bulgaria. Four arrested in Brazil, three charged in Europe.
What A coordinated takedown, run in Brazil as Operacao Klonen, of the network behind the theft of about thirty million euros from German online banking customers.
Where The fraud struck German customers; laundering ran through Brazil and four European countries, with most cashed out in Brazil.
When The theft took four days in November 2023; arrests announced 13 to 14 Aug 2026.
Why Money. Proceeds were layered through multiple channels and, in one instance, into an election campaign.
How A vulnerability in a payment provider's booking process, introduced by a faulty software update, used to make numerous unauthorised withdrawals.

IMPACT

- Financial: about thirty million euros taken, roughly twenty-two million dollars recovered. The bank stated customers bore no loss.
- Supply chain: no control at the bank was defeated, because the opening was not at the bank.
- Identity: payment cards issued without account holders' consent were used as a laundering layer.
- Political: fraud proceeds allegedly funding an election campaign is the crossover from theft into influence.

SEQUENCE OF EVENTS

Nov 2023 The four-day theft window
Nov 2025 German arrests over fraud through payment firms
13-14 Aug 2026 Operation Klonen: 21 warrants, seven charged

1. A processor ships an update that breaks a control
2. Four days of unauthorised withdrawals
3. Funds layered through accounts, firms and crypto
4. Cards issued in other people's names move the money
5. Most cashed out in Brazil, the rest across Europe

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- Nobody attacked the bank - exposure includes the release quality of every firm in the transaction chain.
- Four days is the number to plan against: how fast would an anomalous pattern of debits be stopped?
- The bank absorbing the loss protects customers and weakens the incentive to fix the supplier.
- The laundering, not the theft, is why this took three years.