Former Electrician at Center of $150 Million Brazilian Bank Heist

João Nazareno Roque sold his password for $3,000, then helped hackers steal from six financial institutions

João Nazareno Roque spent 20 years as an electrician, installing cables and reading building blueprints. At 42, he decided to start over, and got into technology.

Three years later, the 48-year-old, who became an IT operator, would become the inside man in one of Brazil's largest financial cyberattacks. Police arrested him last week for selling his corporate password and helping hackers steal more than $100 million from the country's banking system.

C&M Software Was His Company

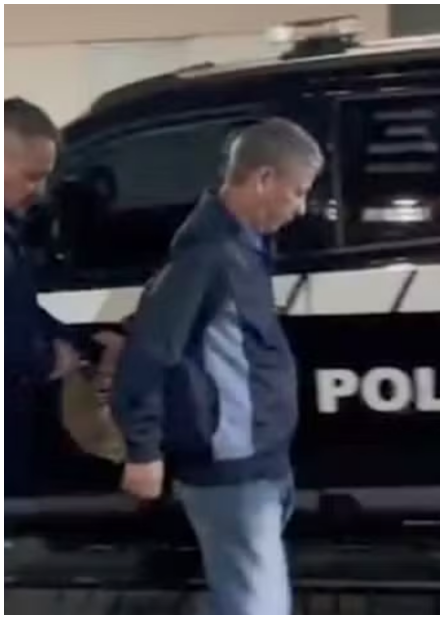
The attack targeted C&M Software, a company that connects smaller banks to Brazil's Central Bank systems, including PIX, the instant payment network used by 76% of Brazilians. Hackers exploited Roque's access to drain money from six financial institutions in a single night.

Brazilian authorities have frozen **$50 million** linked to the scheme. But much of the stolen money was quickly converted into Bitcoin, Ethereum, and other cryptocurrencies through Latin American exchanges, making it hard to trace.

The case shows how criminal groups target employees with system access, often through social engineering rather than technical hacks.

Roque told police that strangers approached and recruited him outside a São Paulo bar earlier this year in March.

How An Electrician Turned Fraudster



According to Brazilian newspapers, Roque's LinkedIn profile tells the story of a career changer.

He worked as a residential electrician and cable TV installer for NET before deciding to pursue higher education in technology.

"I am at an age where many expect to already be in leadership positions, but I am here with a great desire to start over," he wrote on social media. He described himself as having "little experience with technology, related to connecting cameras, computers and distributing extensions."

After graduating in 2023, he landed a job as a junior back-end developer at C&M. His role involved building and maintaining the hidden parts of financial systems that customers never see.

That access made him a target.

According to police reports, the hackers who approached him knew specific details about his work at C&M, suggesting they had researched the company's employees.

The $3,000 Deal That Cost Millions

The criminals made their first offer through WhatsApp in March. They would pay 5,000 Brazilian reais (about $1,000) for Roque's corporate login credentials.

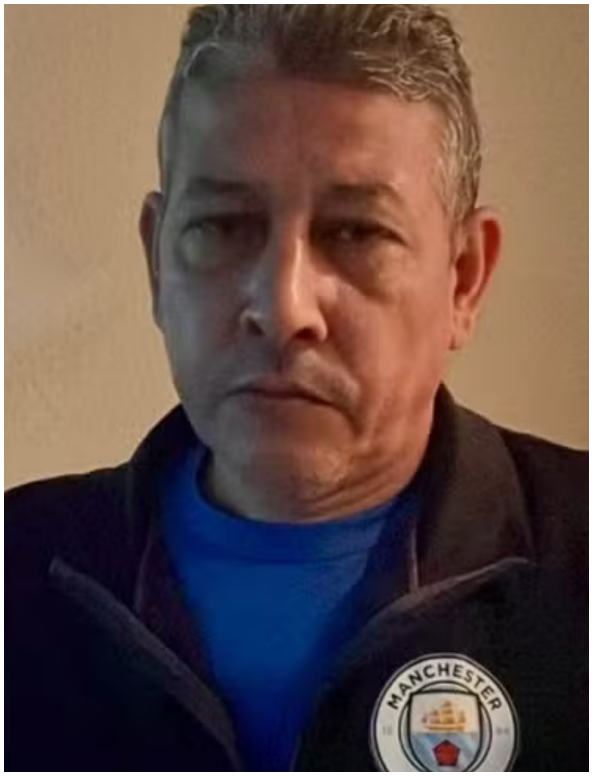
A motorcycle courier delivered the cash and collected his username and password. Two weeks later, the hackers offered another 10,000 reais ($2,000) if Roque would execute commands on C&M's systems from his own computer.

Roque agreed and created an account on the Notion platform to receive instructions. He told police he changed his cell phone every 15 days to avoid being tracked and never met the criminals in person.

The attack came on June 30. Hackers used Roque's access to create fake PIX transactions, moving money from the reserve accounts that banks keep at Brazil's Central Bank.

The fraudulent transfers continued for nearly two and a half hours before BMP, one of the affected banks, noticed suspicious activity. BMP alone lost about $74 million, though it recovered $30 million.

Cryptocurrency Laundering Network



Once stolen, the money moved quickly into digital currencies. Blockchain investigator ZachXBT tracked large sums flowing through Latin American over-the-counter crypto desks and exchanges.

The rapid conversion made recovery difficult. Unlike traditional bank transfers, cryptocurrency transactions can be hard to reverse, especially when moved through multiple exchanges and converted into different digital assets.

Internal Fraud Is Greatest Vulnerability

C&M Software said the breach resulted from "social engineering techniques" rather than flaws in its technology systems. The company noted that its security monitoring helped identify the source of improper access.

But the incident exposed how a single employee's credentials can compromise an entire financial network. C&M connects numerous smaller banks and fintech companies to Brazil's Central Bank infrastructure.

Brazil's Central Bank suspended parts of C&M's operations after the attack. The bank said it issued instructions to "suspend C&M Software's platform access for all institutions immediately post-incident to contain the damage."