PIXELS • CRYPTOCURRENCIES

Hacking of the Platypus cryptocurrency platform: the two accused acquitted by the courts

Presenting himself as an "ethical hacker", Mohammed M. was arrested in February. He was finally released on Friday, just like his brother, accused of receiving stolen property.

By Louis Adam

Published yesterday at 6:55 p.m., modified yesterday at 7:21 p.m. • Reading 3 min.

Article reserved for subscribers

On February 16, 2023, the decentralized finance platform Platypus had the equivalent of 8.3 million euros siphoned from one of its *"pools"* , a shared reserve of cryptocurrencies made available to investors wishing to trade digital assets. That day, Mohammed M. took advantage of an error in the code to withdraw all of the assets, without offering the slightest consideration.

Hacks of this type are not a rarity in this sector of decentralized finance, which proposes to automate operations concerning cryptocurrencies such as buying, selling or lending using blockchain technologies, eliminating the need for a human intermediary. Because the other side of the coin is that the slightest flaw in the writing of the programs which govern the operation of these services, the *"smart contracts"* , can be exploited to steal funds.

It was a phone call from the cryptocurrency exchange Binance that put investigators from the Central Office for Combating Crime Linked to Information and Communication Technologies on the right track. In the space of a few days, they managed to analyze the financial flows and identify two brothers, Mohammed and Benamar M., arrested on February 24 in Aubervilliers (Seine-Saint-Denis). Mohammed M. is then indicted for accessing and maintaining an automated data processing system, fraud and money laundering, while his brother is accused of receiving stolen property.

Read also: Hacking: two French people arrested for theft of cryptocurrencies

The defense of the "ethical hacker"

Eight months later, on October 26, at the Paris court, Mohammed M. does not dispute the facts but claims to have acted in good faith. He presents himself at the bar as an *"ethical hacker"* who wanted *to "recover the endangered funds from the Platypus platform to return them later"* . He thus hoped to obtain a *"bonus",* paid by the company, of *"around 10% of the total amount"* .

This 22-year-old self-taught person, without a diploma or training but with a strong taste for IT and the world of cryptocurrencies, claims to have found the flaw by chance, while " *trying to understand how the protocol worked"* . By observing the way in which the Platypus loan system is structured, he then observes an error in the source code of the "emergency withdrawal" function. And it is this flaw, by a sleight of hand with another cryptocurrency platform, that he then thinks he can exploit.

First there were several unsuccessful attempts. Following a mistake on his part, the equivalent of 7.8 million euros remains blocked in a wallet that is now completely inaccessible to anyone. But he ultimately manages to extract the equivalent of 263,000 euros in cryptocurrencies, which he sends to a wallet over which he has control. This loot is then quickly disseminated: part of the funds is exchanged and distributed between different wallets, another is sent to an anonymization service

(what we call a *“mixer”*), a last part, the equivalent of 12 000 euros, is transferred to his brother, Benamar M.

“Not a blank check”

Underlining the new nature of this type of delinquency and the “enormous” damage of the case, the deputy prosecutor had requested a sentence of five years in prison, including two years with a committal warrant for Mohammed M., and six months suspended sentence with a fine of 20,000 euros for Benamar M.

But on Friday, December 1 , the court finally ruled in favor of the defense arguments, according to which Mohammed M. had only taken advantage of *“a machine which gives more than it must give”* : the heads of accusation linked to access and maintenance in an automated data processing system do not hold up, Mohammed M. having simply interacted with the *smart contract* offered by Platypus, without fraudulently accessing a computer system belonging to the company .

The court also considered that the use of the “emergency withdrawal” functionality could not be qualified as a fraudulent maneuver or deception allowing the scam to be qualified, “ *even if the* smart contract *was poorly coded, so that it allowed Mohammed M. to benefit from it* . Through a domino effect, the suspects were also cleared of charges related to concealment and money laundering.

While pronouncing the acquittal, the magistrates brushed aside any label of *"ethical hacker"* , specifying for Mohammed M.: *"You still have a debt linked to the loan, and Platypus will probably turn against you in civil proceedings . This decision is therefore not a blank check, simply, the charges do not hold up on a criminal level. »*

Read also: Cryptodetectives: from specialized companies to amateurs, they trace the blockchain

Louis Adam

Waffle makers

The best waffle makers

See more