OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

AI-Driven Crypto Scam Steals $1M via YouTube

August 7, 2025
— Categories: Crypto

Download IPFS

A new wave of cryptocurrency scams has exploited artificial intelligence tools and YouTube to siphon over $1 million from unsuspecting users, according to findings published by SentinelLABS.

The scheme revolves around fraudulent smart contracts falsely presented as MEV (Maximal Extractable Value) arbitrage trading bots. Victims were misled into funding and deploying

these contracts under the illusion of quick profits. Instead, the funds were routed to attacker-controlled wallets through hidden and deliberately obscured code.

Scammers took advantage of AI-generated avatars and voiceovers to mass-produce YouTube tutorials while keeping production costs low. The videos were uploaded on aged YouTube accounts filled with unrelated, often recycled content, giving them the appearance of legitimacy. In some cases, the videos were left unlisted and distributed privately via Telegram or direct messages to avoid detection.

In a recent report, SentinelLABS outlined how these deceptive tutorials instructed users to use Remix, a widely known Ethereum development environment, to deploy the malicious contract, fund it with ETH, and initiate a seemingly harmless “Start()” function. However, behind the scenes, the contract rerouted the crypto to a concealed wallet through sophisticated code manipulation techniques, such as XOR obfuscation and hexadecimal conversions.

“Each contract sets the victim’s wallet and a hidden attacker EOA (Externally Owned Account) as co-owners,” noted researchers at SentinelLABS. “Even if the victim doesn’t activate the main function, fallback mechanisms allow the attacker to withdraw deposited funds.”

The nature of the scam makes fund recovery highly unlikely. The obfuscation techniques used to disguise destination wallets, along with the bulk movement of funds across secondary wallets, have made it nearly impossible to trace the stolen ETH effectively.

While most wallets associated with the scam only managed to steal four or five figures’ worth of ETH, the main account tied to Jazz_Braze accounted for the lion’s share of the haul.

SentinelLABS issued a firm warning to crypto users, urging them to steer clear of any so-called ‘free trading bots’ promoted via social media, especially those requiring manual smart contract interaction. Even testnet deployments should be treated with caution, as the underlying malicious techniques are easily transferable across blockchain networks.

As AI continues to be adopted across industries, its misuse by cybercriminals raises growing concerns about security gaps on major platforms like YouTube. Despite repeated incidents involving crypto fraud, tech giants have struggled to clamp down effectively on such content.