Call for crimes? Russian-language forum runs contest for cryptocurrency hacks

intel471.com/blog/call-for-crimes-russian-language-forum-runs-contest-for-cryptocurrency-hacks

At the recent 2021 RSA conference, some of the best and brightest minds the cybersecurity industry has to offer came together to present numerous ideas on how to stop cybercriminals from carrying out their crimes. At the very same time in other corners of the internet, those very same cybercriminals were holding their own formal event intended to share knowledge on how to perpetuate those crimes.

Over the past month, operators of one of the top Russian-language cybercrime forums have been running a “contest,” calling for the community to submit papers that examine how to target cryptocurrency-related technology. In the announcement made on April 20, 2021, the forum’s administrator called for papers that covered unorthodox ways to steal private keys and wallets, unusual cryptocurrency mining software, smart contracts, non-fungible tokens (NFTs) and more.

Submissions were accepted over 30 days, with the administrator saying $100,000 in prizes would be awarded to winners. Shortly thereafter, a reputable forum member added $15,000 to the prize pool.

Shortly after opening submissions, forum users started posting their own papers for the larger community to see. One entry looked at manipulating APIs from popular cryptocurrency-related services or decentralized-file technology in order to obtain private keys to cryptocurrency wallets. Another submission detailed how to create a phishing website that allowed criminals to harvest keys to cryptocurrency wallets and their seed phrases (a list of words which store all the information needed to recover lost cryptocurrency).

This contest is not the first time underground forums have done something like this. Two popular forums have called for research papers on a wide variety of topics, including mobileOS botnets, ATM and POS cracks, and fake GPS signals, among others. Prizes up to $10,000 were awarded to the “best” research, while entrants earned $50 just for submitting. Additionally, operators of various ransomware-as-a-service groups, including REvil and LockBit, have hosted their own contests where forum members submit papers on various topics that could potentially help further their crimes.

This contest is a prime example of why organizations need to proactively monitor the cybercrime underground. This forum’s effort shows that cybercriminals are keenly focusing on the cryptocurrency ecosystem, have taken note of the steadily climbing values of various cryptocurrencies, and will soon target NFTs due to their exorbitant price tags. Cybercriminals go where the money is held, and the money floating around cryptocurrency continues to climb “to the moon,” so criminals will have a desire to cash in.

The contest is also an example of how cybercriminals can be more nimble than defenders. Forums not only serve as a marketplace, but also usher in and foster new innovations and cutting edge approaches that do not need to get bureaucratic approval before being used to carry out crimes.

Attack surfaces will grow as the technology stack around cryptocurrency and decentralized finance continues to grow. As these services come online, businesses need to proactively watch the underground in order to strategize for how criminals may target their business-critical functions with information from contests, like the one discovered above, to devastate their organization.