# Cyber Gang Uses Malware to Target Crypto Users in Russia

Meta Description: ***The Russian gang "Crazy Evil" targets cryptocurrency users with phishing scams, stealing digital assets through malware and social engineering.***

A Russian-speaking cybercriminal group called “Crazy Evil” has been identified in a recent cybersecurity report. Crazy Evil runs multiple phishing operations specifically targeted towards cryptocurrency users. The criminals employ deceptive social engineering methods to trick victims into downloading malicious software. The malware intrudes to steal cryptographic wallet keys together with essential, important information.

The criminal organization has been operating since 2021. NFTs, along with other digital assets, compose the main objects of interest for this cybercriminal operation. The attackers do not only focus on stole cryptocurrencies but also extend their operations to gaming accounts and payment cards. The digital asset theft operations of the group rely on malware instruments which include Angel Drainer and Atomic macOS Stealer. People estimate that Crazy Evil obtained millions of dollars through their illegal activities.

The criminal organization functions as an assembly of direction steering teams. The group serves the function of funneling authentic traffic through deception into false landing pages. The phony websites specifically target victims by stealing their valuable information. The subteams in Crazy Evil work independently to run six different phishing campaigns. The organization maintains a public CrazyEvilCorp Telegram channel, which currently gathers over 3,000 subscribers.

## "Crazy Evil" Cyber Group Targets Crypto Influencers and Gaming Professionals

The primary targets of Crazy Evil include influential figures in cryptocurrency and technology as well as gaming professionals. The group concentrates on "mammoths" which refer to their high-value targeting objectives. Before starting their scams, the group allocates numerous days or potentially weeks to accumulate necessary data. The eight-to-twelve-month attack preparation process enables greater success for their attacks.

The online group uses its operations to exploit both Windows and macOS environments. The capacity of Crazy Evil to operate on Windows and macOS simultaneously enhances their threat potential. The malware known as Crazy Evil currently spreads across numerous thousands of devices operating throughout the world. The scams carried out by this group have caused devastating consequences throughout the cryptocurrency industry.

The group carries out three major scams known as Voxium, Rocket Galaxy, and DeMeet. The scams perpetrated by this group have resulted in numerous major attack incidents. The group remains present and conducts strikes against users individually and organizations collectively.

Insikt advises users to use endpoint detection and response solutions which actively detect Crazy Evil-linked malware for defense against such attacks. Security tools with web monitoring and filtering functions should be deployed to prevent the access of users to malicious domains managed by the group. Security professionals are advising cryptocurrency owners to stay alert and implement protective measures since the group continues to expand its influence.