Yuma Validator - 2025.03 Incident Report

Miner Relaying Detected Through Yuma Validator on SN20

Team Rizzo was made aware of suspicious activity relating to Miner Relaying occurring on Subnet 20 and potentially a number of other subnets throughout the ecosystem. Team Rizzo came up with a plan to identify the validity of these claims by setting a 'trap' to obtain proof of this relaying activity. In early March of 2025, the trap was triggered and captured evidence of Miner Relaying from the Yuma Validator.

What Occurred

A respected miner on Subnet 20 informed our team that they believed their model had been stolen by another miner and was being used to gain unfair emissions. Team Rizzo was able to confirm both sets of miners were using the same model weights and configuration. The Rizzo Validator operators looked back over the previous five (5) weeks and determined that the only validators on SN20 querying miners were Rizzo, Crucible Labs, Opentensor Foundation, RoundTable21, and Yuma Validator. Our team worked with the miner to set a trap to determine which validator (of those 5) had stolen the model from the other miner. The trap was triggered and showed that the miner's model was retrieved by the Yuma Validator and put into the hands of other miners on SN20.

Investigation

EFFECT: As an effect of the Miner Relaying, there is a miner (or cabal of miners) that is successfully taking over a number of subnet miner UID slots with the work of another miner. This is preventing the affected subnets from further innovation due to limiting other participants (miners) from competing in a fair and decentralized manner.

THE TRAP: Team Rizzo had the respected miner create 5 top-performing models with different signatures to send to each of the 5 validators. Knowing that the validators each have a different, unique model they are evaluating from the miner, it is only a matter of time before the top model is stolen and provided to the other mining team.

OUTCOME: A couple weeks pass and the model with a signature that was only ever sent to the Yuma hotkey shows up in the ecosystem running from another miner that is unrelated to the originating model owner.

MOTIVE: In this case, the motive is clearly monetary. Abusing the privileges of the Yuma Validator to steal innovation and to take over subnet mining has shown to be extremely profitable.

MITIGATION: Team Rizzo is reaching out to leadership at Yuma to inform them of this suspected action being exercised under their validator. Upon receiving this information, Yuma’s leadership promptly shut down their validator on Subnet 20 and began an internal investigation. They subsequently completed a validator hotkey swap across all subnets and introduced new, unique hotkeys for each subnet to strengthen security and prevent further issues of this nature.

Conclusion

While the investigation revealed miner relay activity tied to the Yuma Validator’s hotkey, the source of the suspected compromise remains under investigation. Yuma has responded swiftly and constructively, implementing measures to mitigate any ongoing risk and reinforce validator integrity moving forward.