Rizzo Validator - 2024.06 Incident Report

Coordinated Blacklisting of Rizzo Validator on SN5 - 2024-06-07

The Rizzo Validator was the target of a coordinated attack on the Bittensor network. As a known and trusted community member, the Rizzo team would like to offer facts and findings to provide transparency to the community.

Incident Reports are a common outcome of issues that arise in companies like ours related to IT. Whenever there is a crash or attack or when any issue arises on our client systems, we document what occurred, what was done to mitigate the issue and any relevant information for future reference. Here's our 2024.06 Incident Report …

What Occurred

On May 22nd, we were first alerted by our monitoring that showed a decline of our Rizzo vTrust:
Line 21112: [2024-05-22T15:22:00] error : **'sn5'** status failed (1) -- Alert: Subnet 5 vTrust is **0.88475**
Line 22489: [2024-05-22T17:46:28] error : **'sn5'** status failed (1) -- Alert: Subnet 5 vTrust is **0.49108**

We quickly realized that the validator was being blacklisted. Blacklisting started to increase on 5/21/2024 with **60** miners and continues presently (6/7/2024) with **142** miners.

There are legitimate reasons to blacklist a validator, such as performance issues. We confirmed with the Subnet 5 owner that the Rizzo validator was performing optimally and without issue.

On May 31st, we had not found any issues and the blacklisting continued to increase. We reached out to SN5's community to raise the issue and ask that the Rizzo validator be taken off the miners' blacklist. This was additionally followed by the Subnet owner's request that the Rizzo validator be taken off of the miners' blacklist.

Today, on June 7th, it has been a week since the miners have been requested to remove Rizzo from their blacklists and the miners have shown no reduction in blacklisting.

After a thorough analysis, it was discovered that 134 of the miners are responding to the Rizzo Validator with the same blacklist reason: HotKey is in BlackList. What's interesting about this is that "HotKey is in BlackList" is not in the SN5 repo, it's not in the Bittensor repo and in fact, it's not appearing in a search across public repos on github.

Noting this, it's clear that "HotKey is in BlackList" is custom and **unique to 134 miners on SN5**.

This leads to a very concerning conclusion that 57% of SN5 is being mined by 1 team and that this team is coordinating an attack against the Rizzo Validator.

Mitigation

EFFECT: As an effect of the blacklisting, our delegates noticed a significant drop in performance compared to other validators on the network. It was communicated by a few of our top delegators that if we didn't improve performance, they would be forced to move to a better performing validator.

OPTIONS: If the coordinated miners refuse to take us off their blacklist, we have 2 options:

1. Leave everything 'as-is' and watch our delegates flee to better performing validators.
2. Weight Copy on SN5 to mitigate the attack.

Despite several community leaders being vocally in favor of weight copying, it goes against everything we stand for and is a shame that it has come to this.

ACTION TAKEN: The Rizzo Team came up with a hybrid response. Once we understood that this was a malicious and coordinated attack against the Rizzo Validator, we found a balance allowing us to (a) keep validating on the network legitimately, while also (b) restoring our performance on SN5. Additionally, this solution acted as a 'trap' for the bad actors (miners) on the network.

We wrote custom code for our SN5 Rizzo Validator that recognizes the attacking miners and only for those miners, looks to other validators for the correct answers (copies weights for the attacking miners). We continue to validate on SN5 with our data center and our resources and we submit to the network, in real time, the weights of the legitimate miners along with the weights of the attackers.

As miners remove us from their blacklists, the code we've implemented will commence evaluation of those miners as if they were legitimate miners.

OUTCOME: This solution immediately restored performance.

We also realized that the only people/person that would notice would be the attacker(s) themselves. Essentially, whoever called the Rizzo Validator out first would be the likely culprit(s).

On 6/6, the Rizzo validator was 'called out' and there were immediate calls for it to be 'blacklisted everywhere', labeled as a "Weight Copier", and direct calls to the OTF to intervene. It was coordinated and clearly manipulated.

At this point in time, we welcome alternative solutions to resolve these challenges.

MOTIVE: As pointed out above, an attack like this will reduce a validator's total stake (delegates leaving for better performing validators). It will also force the validator to weight copy to keep

performance. So the motive was to take stake from our validator and/or find an opportunity to label us as a weight copier.

Who is capable of this that would also benefit from it?
Why try so hard to label someone who has strongly opposed weight copying as a weight copier?

While we have our assumptions and you likely have your assumptions, we are not here to point fingers, cause drama, or create FUD. We are here to do good business and grow the Bittensor ecosystem.

CONCLUSION: We would like to request that everyone try to work together as a team. There is no reason to attack, slander, or promote malice in this amazing project. We will continue to put our best foot forward in ensuring Bittensor's growth and success. If I or my team has done anything to upset anyone in this community, please reach out to me to discuss. My commitment to you is that I will be open-minded about any issues you are having and try to bring them to resolution. We do not have to agree completely on everything, we just need to agree to continue working toward the vision and goals set forth by the OTF to make this the greatest AI project in the world. Thank you for your time and understanding.

Now let's get back to building!

-Frank Rizzo

P.S. We will no longer engage with those that have a one-track mind towards destruction, those conducting witch hunts and those that have no interest in finding common ground or working on a solution.