Allnodes compromises 100% of their clients on most pos networks

therefore there are messes on 67 chains

This document originally focused on Luna classic. There is a list of affected chains below. It's everywhere.

This document is being updated in real-time.

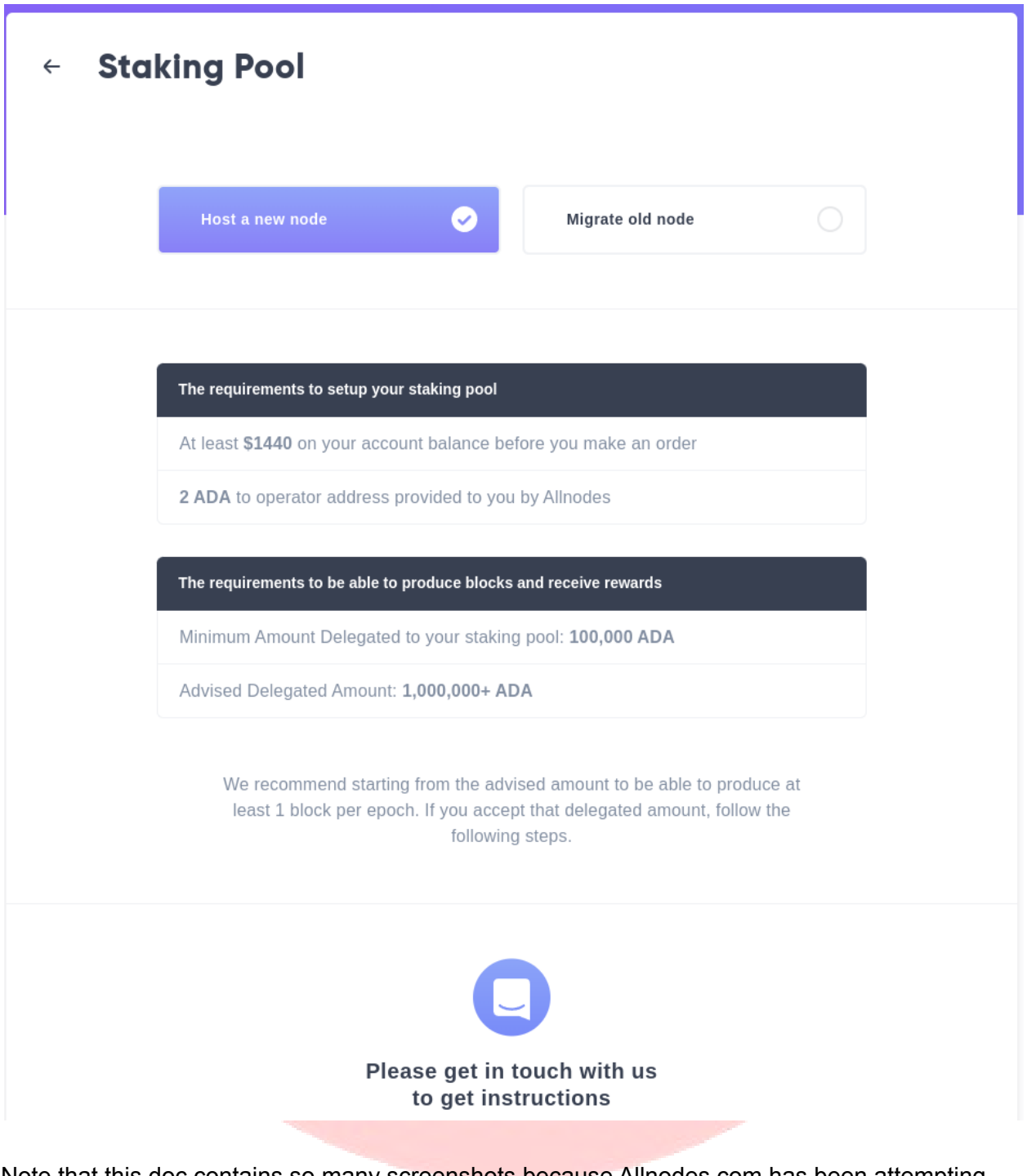
Author: Jacob Gadikian from Notional
twitter.com/gadikian
twitter.com/notionaldao

Jan 23, 2023

happily accepting donations for this work, which is unfunded.
Another way to fund it is to delegate to Notional

How it works

Allnodes.com has a default user flow for most networks which includes allnodes creating the operator seed phrase. They even claim that they're givintg you "free" tokens, here is an illustration:



Note that this doc contains so many screenshots because Allnodes.com has been attempting (poorly) to cover their tracks. If you know a way of archiving the entire site, that would be helpful I think.

Since mentioning this issue, it is fair to say that:

- At no time has allnodes denied that it exists
-

Networks with 100% certain issues:

- Every cosmos chain listed here:
    - https://www.allnodes.com/pricing
    - Due to this investigation, Allnodes has added support for hardware wallets for operator keys on cosmos chains.
        - Hardware wallets aren't the default user flow when registering
        - Allnodes continues to tell customers that their validator operator seed phrases are un-compromised because they're "deleted"
- Polkadot and Kusama
    -

- Table of contents
    - Validators who have been compromised by allnodes
    - Known-good validators who haven't been compromised
    - Proof of compromise of all allnodes white labeled validators
    - Allnodes response
    - Effects on networks outside of LUNC
    - Conclusions

Goal

The purpose of this report is to assist validators who contracted with Allnodes in securing their operations. We are explicitly not hating on them, but feel that it is very important that providers do not know validator operator

Known Compromised Validators

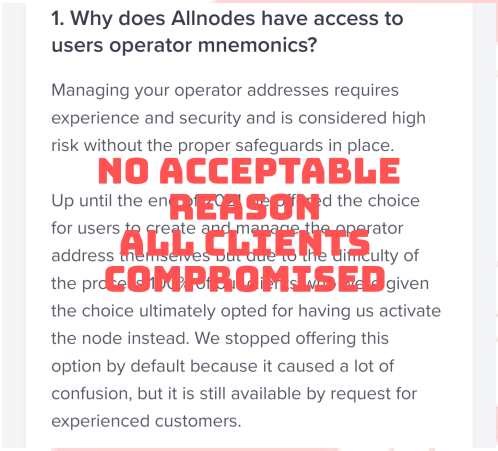
Validators whose keys have been compromised by allnodes:

Certain:

- @BetterLunc
- @LUNC808 ✅ fixing
- @MrDiamondhandz1 ✅ fixing
- @HappyCatKripto 💥 refuse to fix

- @lunc_nymph
- @davidagoebelt ✅ fixing
- @ClassyCrypto_💥 refuse to fix
- @CryptoKing_NFT
- Toxic Labs ✅ fixing
- Allnodes 🍿worst VaaS on earth

Note Well: We do not know all of the validators that are run by Allnodes. They refuse to release a client list. From their blog post, data January 24th, we are aware that 100% of their white label clients should be considered to be compromised.



What should validators do?

If you're one of the compromised validators, you should remove 100% of the stake that you delegate to yourself.

- You'll be jailed and you will no longer pose a threat to the network
- Your delegators will not be slashed
- You can then make a new validator and ensure that the priv-validator.json file and seed phrase are kept strictly private
    - There is no other way
- You MUST NOT continue to operate with another provider. The seed phrase and priv-validator.json file are compromised by allnodes, and you MUST move to a new provider.
- Know that at present, Allnodes can impersonate you entirely.
    - They can spend as you
    - They can vote as you

    - Anything
    - You are fully compromised

Ethical compromised validators
The following validators are taking immediate action towards resolution. If you delegate to them, make sure you know what their new moniker is, so you can redelegate. They are making the correct, ethical choice, and we should not nail them to the wall. Allnodes says that they are noncustodial, and this is allnodes lie.

- David Goebbels
- Toxic Labs
- lunc808

Compromised validators who refuse to fix

It is imperative for LUNC security that you re-delegate to secure validators. These folks haven't even recognized that there's an issue

- Lunclive (MrDiamondhandz1)
- Happycatcrypto
- Classycrypto

They have no place in blockchain infra

I'm a validator and shutting down my node because allnodes has my seed phrase. What should I do?

<u>If staying down</u>
The first thing that you need to ask yourself is whether or not you want to validate again. If you are simply going down, then the correct thing to do is to tell your delegators that you are going down, and why you are going down.

Then after some period of time, you would remove 100% of your delegation to yourself, you're validator will be jailed, and your delegators will not be slashed.

<u>If intending to come back up</u>

First of all thank you for making the security conscious decision to take your compromised validator down. If someone else has your seed phrase, they can completely impersonate you and the chain cannot tell the difference between you and the impersonator.

Next, let your delegators know that you will be removing your self bonded steak and why you are doing that. Also let them know that you will be coming up again and that you will use the same branding and moniker.

If you have a sizable amount of LUNC, you may consider creating your new validator, then taking the old one down. This way, migrating delegators have a target to migrate to.

All of the validators on the known good list are very happy to assist your delegators in the migration to you. This includes explaining the issue to the community, talking you through the migration, and even if need be assisting you with setting up your own validator node.

When you set up the new node, make certain that you do not reuse the private validator key or the seed phrase that you used for your old one because both are compromised. You can reuse the name and you can reuse the profile picture. While this is most certainly the more difficult path, and you absolutely could stay with all nodes, the reality is that your current credentials have been compromised and they could impersonate you at any time. Thank you for doing the right thing.

What should delegators do?
If you delegate to one of the compromised validators, you should re-delegate to one of the validators on the known-good list below.

- You'll secure the network by moving votepower away from allnodes.
- Since allnodes has the seed phrase and validator private key of every validator that they run for others, all of the compromised validators are in fact allnodes.
    - There is no "validator x"
    - There is only allnodes
- You're moving vote power away from validators who can be impersonated by allnodes, towards those who cannot

Amendments
If you are on the list of compromised validators, but have not used allnodes:

- We apologize, securing networks is of the utmost importance to us
- Please contact twitter.com/gadikian by DM or tweet

What are the possible impacts?

- Allnodes can impersonate validators because they have the seed phrases
- Allnodes can halt lunc because they control >33% of VotePower
- Allnodes can spend from the validator operator wallets
- Allnodes can participate in governance as their clients
- At 66% of VotePower, IBC fraud becomes possible. Allnodes is at around 41% currently.
    - But we really don't know how much vp they have. They refuse to release their client list

Known Good Validators

Delegators should re-delegate to one of the known-good validators to ensure that Allnodes cannot halt the network, or take over governance. From our assessment, they can currently do both. Further, because their key management practices have been made public, there are risks to the allnodes CEO, because it is public knowledge that he has the seed phrases to numerous validators on numerous blockchain networks.

- ~~CryptoCrew~~
    - ~~Experienced relayers hosted on bare metal cloud~~
    - Note: they have taken another ethical route, and have chosen to leave lunc
        - Delegate to them on other chains, they're great
- Aperion Nodes
    - We running on our own infrastructure on ovh,hetzner and home hosted servers (bare metal)
    - Our validator name is Apeiron Nodes and running on terra classic,omniflix,huahua
- PFC
    - Experienced validator, unknown hosting provider
    - Offers white label services
        - Won't compromise your keys
- Onyx
    - White labeled by PFC
        - PFC doesn't compromise keys
- ~~Notional~~
    - ~~Self-hosted on bare metal in Hanoi, Vietnam~~
    - ~~Experienced relayer~~
    - ~~Experienced software development team~~
    - ~~Does not offer or use white label services~~
    - ~~Author of this document~~

    - Sam as crypto crew, we are leaving Luna classic because security issues are not taken seriously there.
- Luncdao
    - dedicated bare metal cloud server
    - runs nodes on 7 chains
    - do not offer / white label services
    - harnesses the power of asparagoid, the spiritual guru of Jacob, PFC and SCV
    - 123,000 CEOs
        - Offers all CEOs holy wafers, then renegs
- Luncdevfund
    - Details pending
- TerraCVita
    - Hosted by HighStakes_CH
- NovaValidator
    - https://twitter.com/NovaValidator/status/1617577350996320258
- Lunc-validator
    - https://twitter.com/Tluncvalidator/status/1617598736355692544
- Lunapunks.io
- Orbital Command
- Blockscape
    - https://twitter.com/BlockscapeLab/status/1617810457070563329
    - We are @BlockscapeLab, your enterprise-grade, professional validator node operator for PoS blockchains, running world-class infrastructure on many cutting-edge blockchain projects.
    - We are operating in 20+ chains, with a main focus on the cosmos ecosystem.
- Orion
    - twitter.com/orionstaking
    - Experienced dev team and dedicated sys admin engineer for our validators
    - Validators run on dedicated cloud servers, backup infrastructure in the bare metal datacenter
    - Running validators for 1.5 year+ with high uptime, never slashed or jailed, never used or use white-labeling,
    - Running validators on Terra, Terra Classic, Oasis, Injective, Mars
- Smart stake
    - Multi chain validator in cosmos
    - Reasonable takes on Scrt
    - Uses multiple bare metal providers for stability
    - Requests that delegators make delegations to smaller validators to improve decentralization
- Diamond Nodes:
    - London Hosted on Digital Ocean, Storage Optimised server with True NVME 8 Cores 2TB SSD. Latest version Ubuntu, Firewall with all ports locked down apart from 26556 open for all p2p connections to talk to other nodes.
    - Sole operator

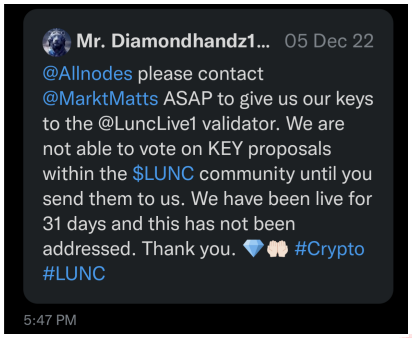
        - https://twitter.com/AntBentinck?t=OI3gkBRwOGTffGk-jPNNLA&s=09
- Synergy Nodes
    - supports IBC relayers for 13 chains.
    - High uptime on lunc and luna classic

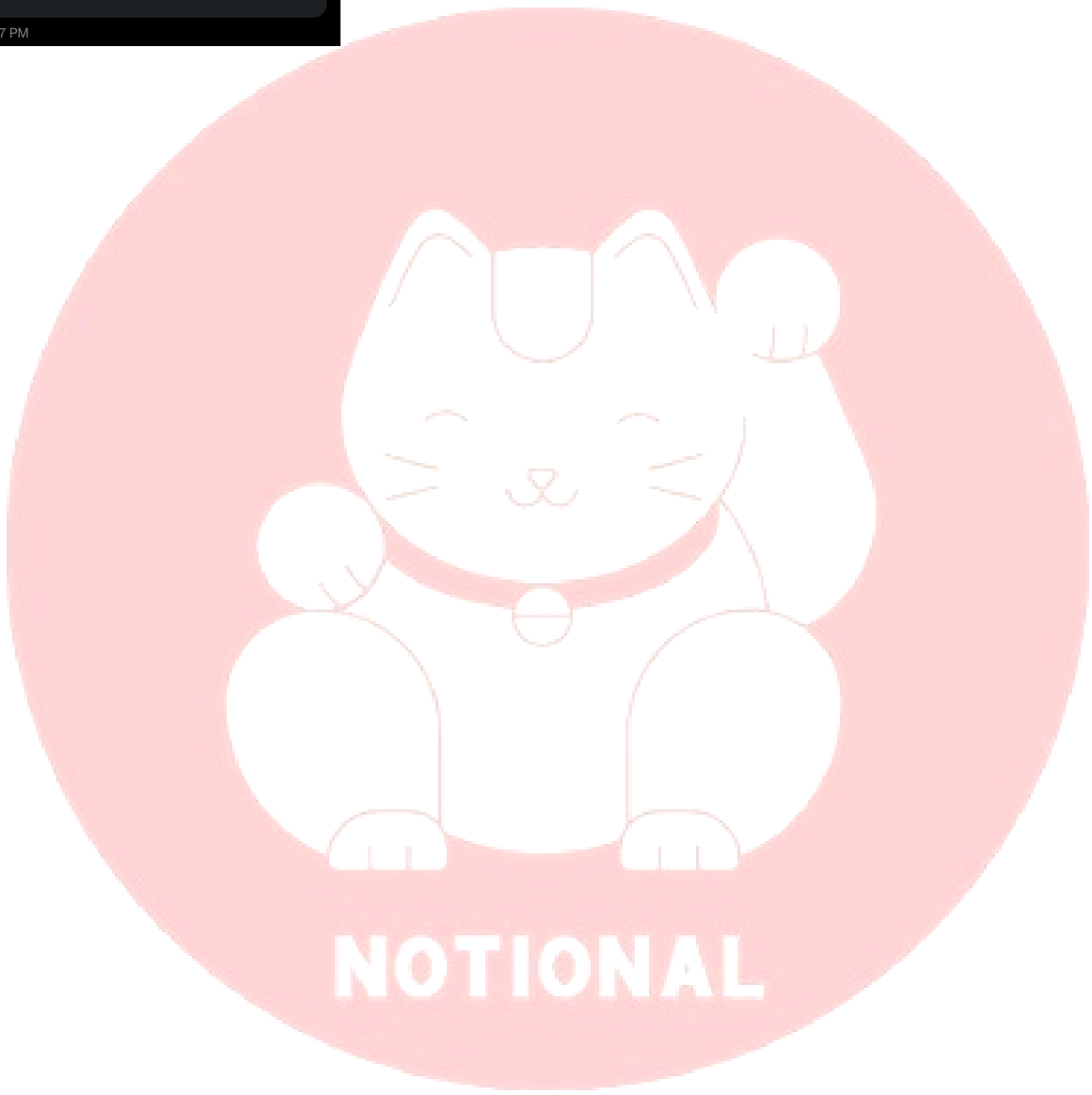
Listing your Validator
If you have not used allnodes, and are willing to disclose some operational details about your validator, we are happy to add you to the list of known-good validators for $lunc. Please just send a DM to twitter.com/gadikian.

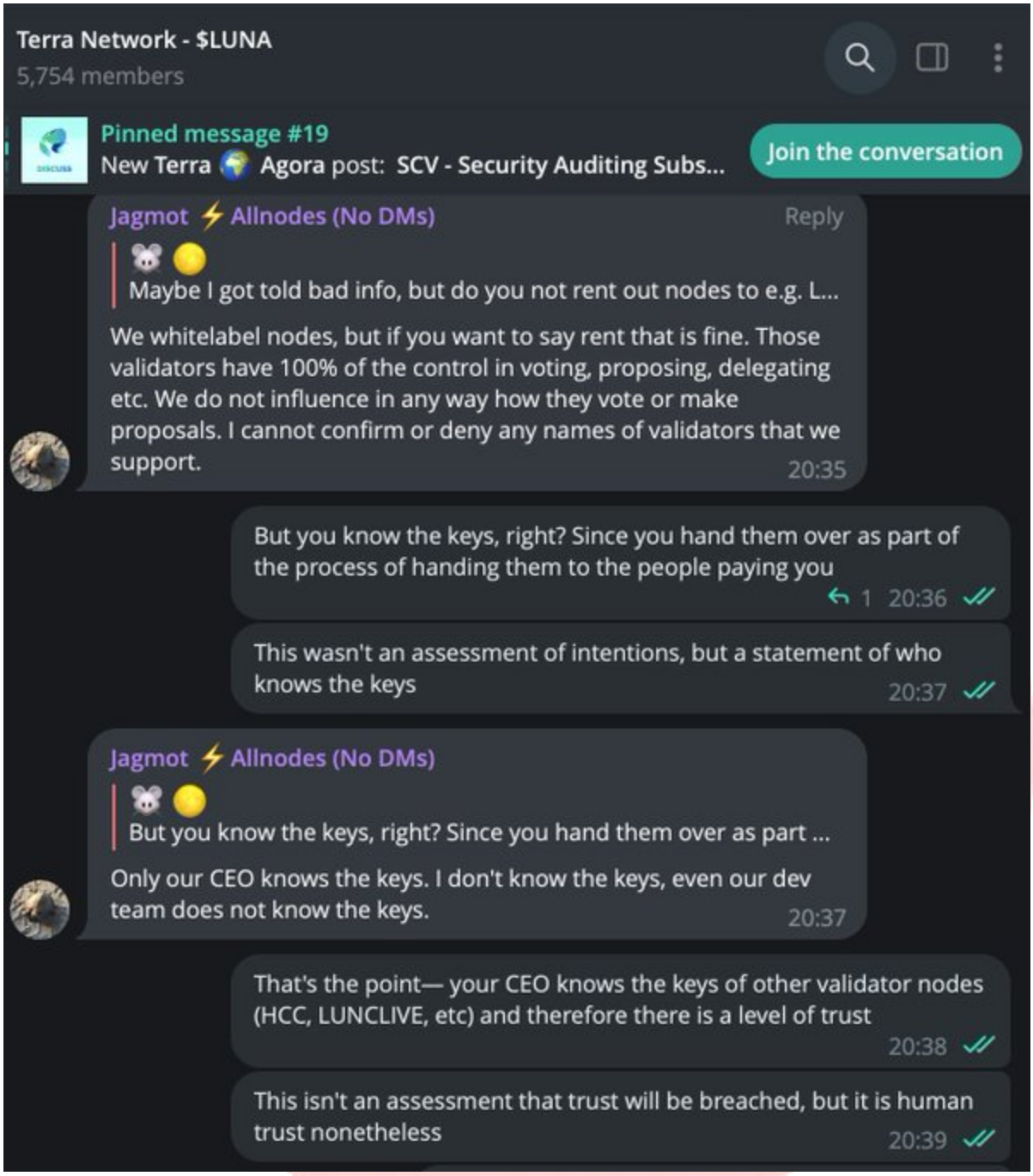
Proof of compromise:

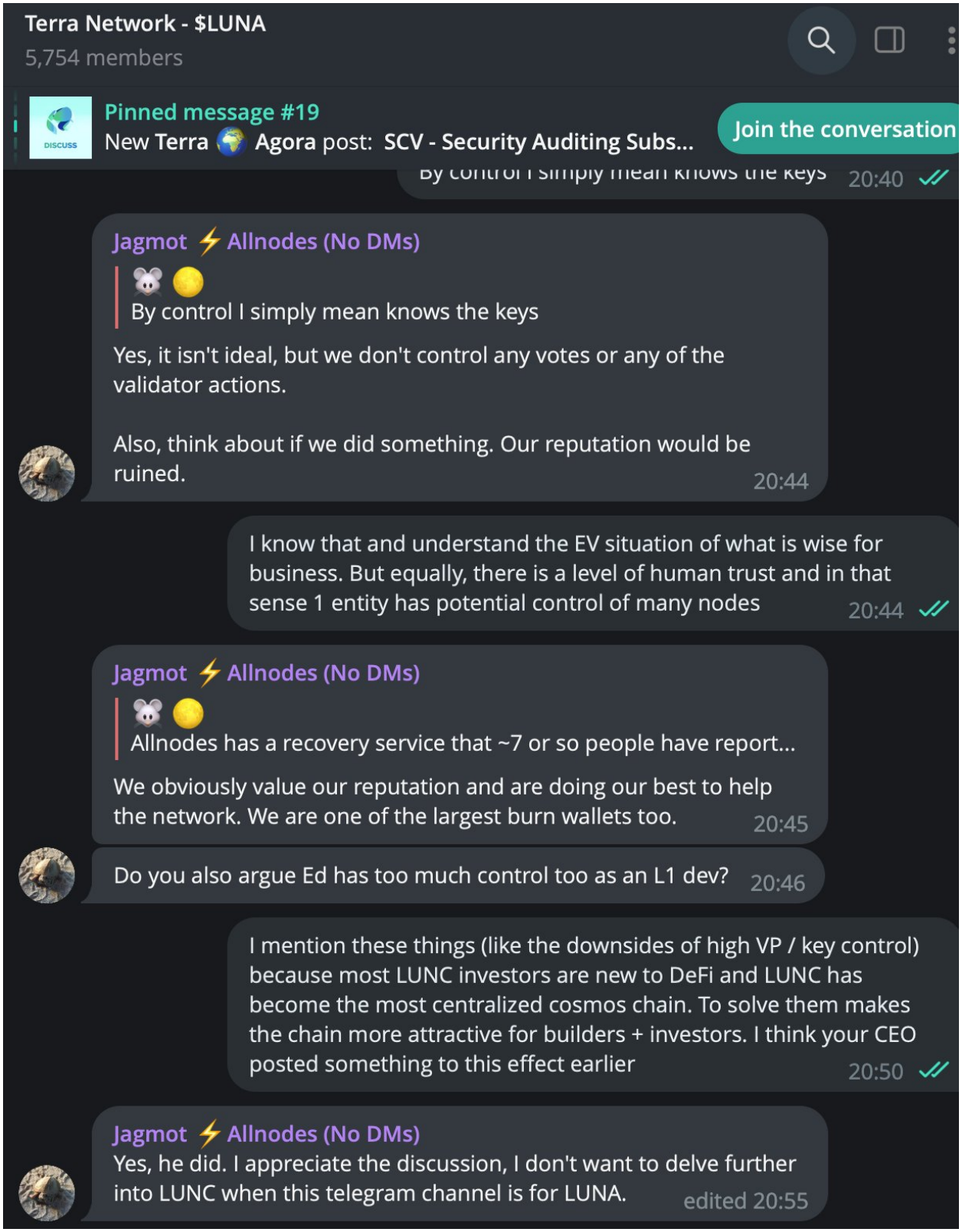
Per their team's own admission, the CEO of allnodes has both the seed phrase and priv-validator.json of all validators that are white-label hosted by allnodes.

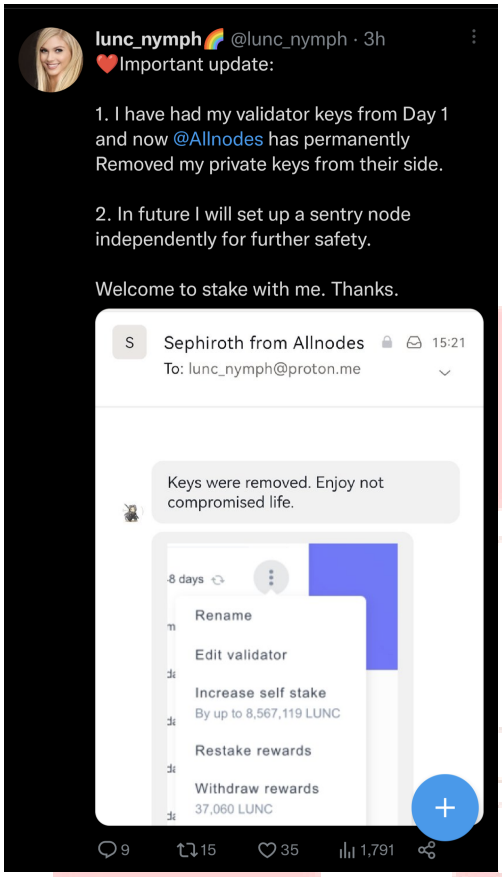
Photos below for proof:

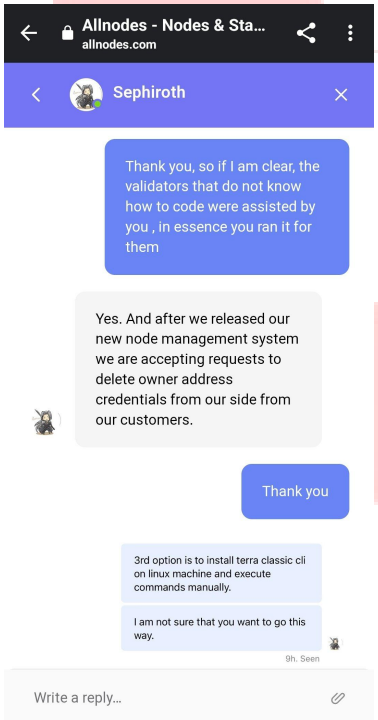

Mr. Diamondhandz1... 05 Dec 22
@Allnodes please contact @MarktMatts ASAP to give us our keys to the @LuncLive1 validator. We are not able to vote on KEY proposals within the $LUNC community until you send them to us. We have been live for 31 days and this has not been addressed. Thank you. 💎🙌 #Crypto #LUNC
5:47 PM


NOTIONAL


Terra Network - $LUNA
5,754 members
Pinned message #19
New Terra 🌍 Agora post: SCV - Security Auditing Subs...
Join the conversation
Jagmot ⚡ Allnodes (No DMs)
Reply
Maybe I got told bad info, but do you not rent out nodes to e.g. L...
We whitelabel nodes, but if you want to say rent that is fine. Those validators have 100% of the control in voting, proposing, delegating etc. We do not influence in any way how they vote or make proposals. I cannot confirm or deny any names of validators that we support.
20:35
But you know the keys, right? Since you hand them over as part of the process of handing them to the people paying you
1 20:36
This wasn't an assessment of intentions, but a statement of who knows the keys
20:37
Jagmot ⚡ Allnodes (No DMs)
But you know the keys, right? Since you hand them over as part ...
Only our CEO knows the keys. I don't know the keys, even our dev team does not know the keys.
20:37
That's the point— your CEO knows the keys of other validator nodes (HCC, LUNCLIVE, etc) and therefore there is a level of trust
20:38
This isn't an assessment that trust will be breached, but it is human trust nonetheless
20:39


Terra Network - $LUNA
5,754 members
Pinned message #19
New Terra Agora post: SCV - Security Auditing Subs...
Join the conversation
By control I simply mean knows the keys 20:40
Jagmot ⚡ Allnodes (No DMs)
By control I simply mean knows the keys
Yes, it isn't ideal, but we don't control any votes or any of the validator actions.
Also, think about if we did something. Our reputation would be ruined. 20:44
I know that and understand the EV situation of what is wise for business. But equally, there is a level of human trust and in that sense 1 entity has potential control of many nodes 20:44
Jagmot ⚡ Allnodes (No DMs)
Allnodes has a recovery service that ~7 or so people have report...
We obviously value our reputation and are doing our best to help the network. We are one of the largest burn wallets too. 20:45
Do you also argue Ed has too much control too as an L1 dev? 20:46
I mention these things (like the downsides of high VP / key control) because most LUNC investors are new to DeFi and LUNC has become the most centralized cosmos chain. To solve them makes the chain more attractive for builders + investors. I think your CEO posted something to this effect earlier 20:50
Jagmot ⚡ Allnodes (No DMs)
Yes, he did. I appreciate the discussion, I don't want to delve further into LUNC when this telegram channel is for LUNA. edited 20:55





This reflects their updated policy. Before 1/27/2023, 100% were compromised.

NETWORKS OUTSIDE OF LUNC

Allnodes validates many blockchains, and it is our assumption (not proven) that they offer white label services on all of these chains. Allnodes does not offer secure white label services.

Notional has reached out to allnodes.com in order to help them to provide secure white label services. For cosmos chains, it is critical that a white label provider does not know the seed phrase for the validator operator account. Otherwise it is possible for the provider to impersonate you.

Chains validated by allnodes

1. Ethereum - someone with more eth experience should check
    a. Rocket Pool - maybe unaffected
    b. Native - maybe unaffected
2. Cosmos hub
3. Evmos
4. Osmosis
5. Lunc
6. Luna
7. Tron
8. Near
9. Cardano
10. Solana
11. Polygon
12. Crypto.org
13. Cronos
14. Fantom
15. Huobi
16. Helium
17. Kava
18. NEM
19. Fetch.ai
20. Kusama
21. Gnosis
22. DefiChain
23. Moonbeam
24. Symbol
25. Horizen
26. Syscoin
27. Juno
28. Persistence
29. Shentu

30. Kujira
31. Akash
32. Moonriver
33. Divi
34. Stargaze
35. Regen
36. Firo
37. Irisnet
38. MAP
39. Rizon
40. Energi
41. Comdex
42. Asset Mantle
43. Sentinel
44. Territori
45. BitCanna
46. Sifchain
47. Wagerr
48. Stride

Summary

- Notional does not recommend using a white label provider, or even a cloud service, at any time, for any reason
- If you must use a white label provider, then
    - They will need to know your tendermint key in most cases
    - <u>They must not know your seed phrase</u>
        - If your white label provider knows your seed phrase, your node is compromised and you should shut it down by removing your self bonded stake from it.
            - Your node will be jailed
            - Your delegators will not be slashed
            - Feel free to create a new node
- If you aren't sure what to do, please contact twitter.com/gadikian by tweet or DM.

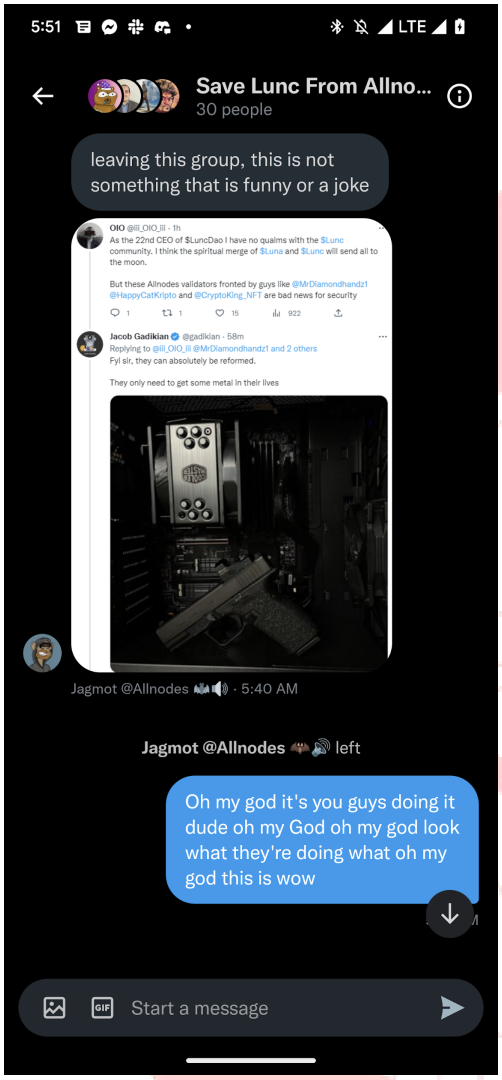
Addendum

Response

The allnodes team, as opposed to having a discussion of their security practices, have claimed that the logo of a group I run, the bare metal alliance, is meant to threaten them.

That photo of a gun in a computer has been used by me to promote bare metal validation for the past 18 months or so. It's not my gun and it is not my computer. I am not threatening the

allnodes team, but I believe that they pose a threat to their clients because of the clients of theirs that I have spoken to, 100% of them are not the sole custodian of their seed phrase.



I believe that a serious team that scaled a validator group to 70 different chains along with white label provision services, would either admit that they had serious security problems or, quite frankly, would actually know how key management works. In fact, if they couldn't manage keys, then they couldn't have scaled to that degree. Thus, they chose to make their clients less secure.

Given that this was their response, I strongly urge every client of allnodes to immediately remove all self-bonded steak on their validator, or pursue other means of deactivation. On the cardano network, account rekeying is possible.

What I'm trying to say is that allnodes.com does not recognize that they have serious problems, and is now trying to paint me as a bad actor. I strongly recommend that validators empty

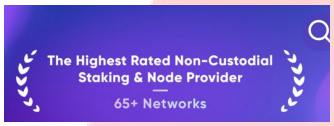
wallets that they know the seed phrases to, immediately. At that time they should also decommission their nodes.

Profile of Allnodes clients

100% of the allnodes clients that I spoke to were not the sole custodian of their seed phrases. I believe that allnodes sends their clients seed phrases upon request using keybase.

100% of the all nodes clients that I spoke to were not technically sophisticated. They were influencers who had little to no understanding of the role of a validator.

Allnodes claims to be non-custodial



they have their clients keys so the funds are in their custody.

Their response blog post is insane
https://help.allnodes.com/en/articles/6926299-cosmos-based-validator-nodes-key-management-and-security

That post argues that it is okay that they have seed phrases for validators – other than their own – on 67 chains.

conclusions

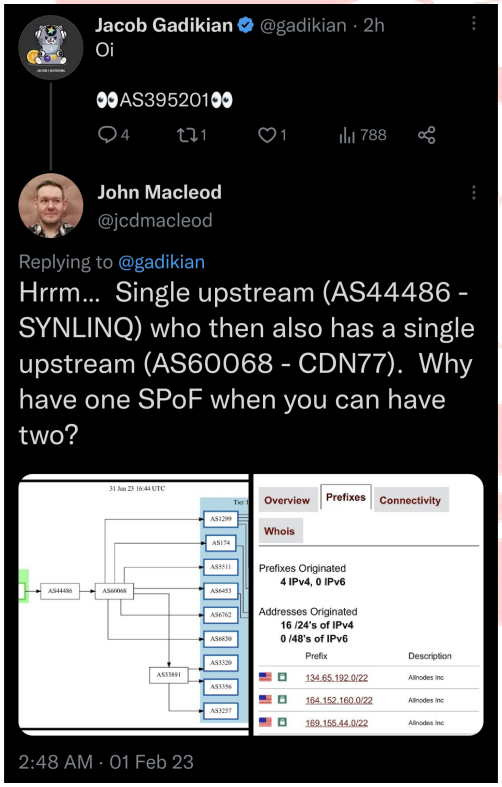
I believe that the luna classic governance on chain is fundamentally compromised. Let's go through a couple of different scenarios:

- Compromise by impersonation
    - Allnodes can impersonate validators because they have the seed phrases. We cannot trust that allnodes customers' votes are their own.
- Compromise by ignorance
    - Many validators and community members, including the group that is supposed to be working on the chain's core software, don't see an issue with Allnodes holding other validator's seed phrases.
    - This is a user education issue.
    - For the L1 working group, I believe that this is **deliberate ignorance –** they know full well the chain is compromised.
        - It is the only thing that can explain their choices.

- Implied threat
    - Allnodes has a very credible ability to harm their customers and the chain.
        - It's really clear that both validators, and the team, have said false things about this situation. Why?
            - I posit that it’s incentives.
- Implied benefit
    - Groups who seek governance funding have clear reasons not to upset allnodes. They control both chain liveness and the governance process.
        - It's really clear that both validators and the team have said false things about the situation. Why?
            - I posit that it’s incentives.

Technical Factors

Additional research has shown that allnodes has set up an autonomous system number.



While it is possible to do robust BGP routing, that's not what they're doing. Any issue in either of their BGP upstreams is likely to halt lunc.

NOTIONAL