Twitter Thread by Markus Amalthea Magnuson ❄■

Markus Amalthea Magnuson ❄■
@scifiagenda

I did more research into the Parler dump. What probably happened was not so much a "hack", but this: When Twilio/Okta shut them down, they just disabled email/phone verification to create an account. This means anyone could directly create huge amounts of accounts via their API.

Someone also found out that fetching Parler posts could be done by enumerating IDs (e.g 1, 2, 3) instead of random IDs that can't be guessed. Unclear if this was via the ordinary API endpoint, or that they found a separate one by monitoring app network traffic.

So you combine these two things and you can create a script to scrape all the posts on the entire platform, using a lot of different accounts to avoid suspicion. Anyone could download and run this script to spread it out over many IP addresses as well.

What I'm still not sure about is whether deleted (meaning flagged as deleted, it's common that services never actually delete data) posts could be fetched without any special handling.

The verdict: The people who wrote Parler are fucking amateurs.

This Reddit comment is a good, and from what it seems, correct, summary: https://t.co/SfJQFQQG2h

Using sequential IDs was supported because the Parler API had an endpoint to convert them to the UUIDs used to fetch posts. Easy to find endpoint via network monitoring, and didn't require any special authentication. ■

Here's that specific function in @donk_enby library parler-tricks: https://t.co/kKQT2KCac1

It also seems like they did not have any kind of rate-limiting. This just gets better and better.