Twitter Thread by ■ Yarrow



■ Yarrow
@frodis_

Here is the text version:

1/ Here is a description of what went down according to someone with far greater technical knowledge than me:

"so a group of developers latched onto the Press Release that Twilio put out at midnight last night. In that Press Release, Twilio

2/ accidentally revealed which services Parler was using. Turns out it was all of the security authentications that were used to register a user. This allowed anyone to create a user, and not have to verify an email address, and immediately have a logged-on account.

Well,

3/ because of that access, it gave them access to the behind the login box API that is used to

deliver content -- ALL CONTENT (parleys, video, images, user profiles, user information, etc) -. But what it also did was revealed which USERS had "Administration" rights,

4/ "Moderation" rights.

Well, then what happened, those user accounts that had Administration rights to the entire platform... The hackers, internet warriors, call it what you will, was able to use the forgot password link to change the password. Why? Because Twilio was no

5/ longer authenticating emails. This meant, they'd get directly to the reset password screen of that Administration user.

This group of Internet Warriors then used that account, to create a handful of other ADMINISTRATION accounts, and then created a script that ended up

6/ creating MILLIONS of fake administration accounts.

Now that they had a way of creating admin accounts without interruption, they created a Docker Image (basically a virtual machine) called a Warrior, that anyone could download, and when fired up, would immediately start

7/ collecting data off of Parlre, in a coordinated fashion.

Consider it like SETI (Search for Extra-Terrestrial Intelligence) that people used to load up as screen savers when their computers were not being used. Same concept, crowdsourcing.

All of this data, the videos,

8/ the images, the posts, the metadata (including the GEO location of all images and videos, and the connections to the accounts that posted it, has been (since midnight) being uploaded to various cloud drives and storage arrays for the purposes of Archiving this

9/ information, for later retrieval by law enforcement, by the public, by Open Source Intelligence communities.

And the kicker. is this: all of this information was thought to be secure and private by individuals who were making the posts. A significant number of those

10/ individuals went through the process of being a "Verified Citizen" on Parler. What does that mean?

It means they uploaded a picture of the front and back of their REAL State Driver's License..... Let that sink in for a second.

I am positive the FBI has been actively

11/ soaking in this information along with the Internet Warriors, but this is how they are going to officially track down.

And it's how the FBI, DHS, and FAA have been able to immediately and exhaustively create no-fly lists. Every verified attendee of the Capitol riot where

12/ they can find a real name has been placed on No-Fly Lists.

It might seem like a small geeky glitch or hack. but in the age of Information warfare. this is the silver bullet for the people who used Parler as a place to organize their efforts.

Also, a lot of posts were

13/13 deleted by Parler members after the riots on the 6th. Turned out... Parler didn't actually delete anything.. just set a bit as deleted. Guess what has access to all "deleted" content? Administrator accounts."