

Text made by KhanZanon.

Tiktok is vast used globally, by people of almost every country in the world, and it's inserted in a big data concept. It appears to be only one more social media, and an entertainment tool used by teenagers and adults. But, it's not...

First thing is the algorithm, is not like Facebook, instagram and YouTube that are advanced and put in the content based on each user preferences. This tiktok system, has a powerful I.A, and scripts that classify you, in real time by a bot. This bot can save and analyze all data of the user, not only the user Face. But more complex tags, such as body anatomy, muscles, and even kind of clothes. That makes possible to know the user gender, race, and if the person is fat, thin, or has muscles. And opens a huge opportunity to understand a huge concept of big data that makes possible, to make complex conjuncts, and put a hierarchy of conjuncts, sub conjuncts that categorize the social media users, and posts classified on each specific kind of group.

On a running exploit of the system, a 16 year old teenager girl, account that had one video that went viral. Without making any marketing campaign, and without the user using tags, so the person could have more views.

I've run some exploits on tiktok lite app, and i got fragments of the algorithm. (For example, people that like football, will have #football tagged on it.)

It appears to be everything ok. But, a real danger appeared. On this post the girl was classified by the algorithm with tags, and those were included "cleavage", "blonde", "latina". on a error.txt file that splash on screen, freezes, and close the app after trying to do another action.

Those kind of uses, are usual to be made on XXX websites. But, it's something new, to a bot and not a person, as "expected" to make an organization of the content, make recommendations, and analyze the contents based on the liked content. Consequently, increasing the chances of a post getting viral, and recommending your post to other people, based on the "viral" stats, that the algorithm prefers.

If the algorithm high the views of +18, and sexualization posts, is easy to know that it will have a conjunct of people and posts that will be recommended by those people. Nonetheless, an innocent teenager post, can be a subject to a community of people, that share and like sexualized content. Even not explicit. But, highly classified.

There are some videos, that i have the proofs, showing how it works.

Well, you thought that it was very bad? there is more.

There are some apps, that "leaked" personal user data, those apps, most of the times had high requirements of access. such as avast antivirus, faceapp and the list goes on. As expected, tiktok is on this list too. This app, leaves residuals, and achieves that the most powerful cleaners on today's virtual market, can't clean.

Those residuals, mark your device, and what account you logged in; It will know what you used to like, your IP, your content and etc. This kind of tiktok policy, everything that you upload to the social media, becomes a tiktok subject. And not "yours", if the tiktok corp, consider that your post, is not something that they would like, they can remove it, or it can become their property. An usual kind of data leaking, and can make a huge market of Personal data. This app can appear just an app for "kids" to make dances, some funny things, and make some friends online. But, only appears... If you are a dad, or mother that have a children that uses this app, don't make them to force quit it.

Try make a dialogue, and tell them to use another social media and expose them the dangers of the tiktok.

Everyone can be studied, and have his data, analyzed by a super I.A. and get recommended by bad people.

Error on tiktok app: found on 07/04/2020

Platforms: tiktok lite (android), still testing but didnt appear on IOS, and web ones.

Summary: information leak, and showing an .log file as a error screen, showing the users, info about their physical appearance, nation, race, and body parts. that the user dint tag on it; none less, it exposes the algorithm.

-If a friend of the user, search and try to download a video of that one. And make 3, actions (will be explained detailed on the complete log.). makes a error, that makes the video downloader to stop working, and exposes the person ids, and shows where the user is set, on a specific group of people. this user should be recommended, viewed and what type of people her "class" and "content" belongs.

To enter in one part of the algorithm. So it can classify you, you will need to like, and search for a certain content 3-5 times, I had tested it 6 times. Doesn't matter your age, the content you search, you will be categorized for.

I have tried to be categorized in +18 years old content, with a 14 years old account, it was very easy to enter on it, and get recommendations about this kind of content. And the comments on the posts, are just as expected...

Something very important to say is that the classes are dynamic. But, in most of the content you will try to enter on it, you will see the same content creators, being recommended to you most of the time.

Facebook sucks doing that too. But tiktok, get the number 1 spot, without a doubt.

Accounts that "bad" values were found:

febrell "all her body classes, on tags"

nimsay "also all her body classes"

vaimonroe "viral", "famous"=(celebrity, because of the amount of followers), and 5 more.

Exploit:

using android, linux, windows, using software such as "bluestacks" to emulate tiktok lite. In a normal mode, or forced mode;

1- choose a target.

2- search for a post of this one that the music used, have been removed by the artist, or rights owner.

3- click on download, go to a place where the wifi can work, but still connected to internet; wait for error message.

4- stop the download, try again, wait for the error message open 4- to 7 times. Then, the video downloader, bugs and send a message flashing on screen with the user tags, characterized by the algorithm...

\$ more exploits, coming soon... Stay tuned...

Anonymous, KhanZanon -06/08/2020