

Forum:[Hack Forums](#)

Thread: [TikTok Hack: Over 900,000 Usernames and Passwords Allegedly Exposed by Hackers](#)

JoseMar - April 28, 2025, 1:14 am

TikTok Hack: Over 900,000 Usernames and Passwords Allegedly Exposed by Hackers

A hacking collective, under the name as R00TK1T, has claimed responsibility for a gigantic information breach affecting TikTok, purportedly exposing the personal information of more than 900,000 users.

According to the group's explanations, they have discharged a test of 927,000 TikTok client records into the wild, portraying it as "proof of their vulnerabilities".

R00TK1T expressed that they had already cautioned ByteDance and TikTok about security vulnerabilities, but were ignored.

"We warned ByteDance and TikTok, but their silence speaks volumes. Despite our clear message, they've ignored the cries of users locked out, suspended, or erased from the platform," the group declared.

R00TK1T Exposes User Credentials

According to a post on a prevalent dark web gathering, the programmers characterised this information dump as just "a taste of what's coming," warning that "the following stage will hit harder, uncovering their most profound privileged insights and shattering their systems".

The discharged data supposedly contains usernames, passwords, and possibly other sensitive account information from the platform's backend systems.

According to cybersecurity specialists, if confirmed, this breach would suggest a noteworthy security occurrence for the platform. The programmers claim they accessed an unreliable cloud server containing client accreditations and stage code.

While the correct assault vector remains unverified, past TikTok vulnerabilities have included uncertain API endpoints and insufficient server-side approval protocols.

This is not R00TK1T's to begin with high-profile claim. The group has already charged effective breaches of different organisations, including Maxis' organize in Kulim, Settle, and Qatar Aviation routes. The bunch has a design of making emotional claims that some at times, outpace unquestionable evidence.

"R00TK1T has a track record of exploiting vulnerabilities across various sectors, leveraging both technical weaknesses and insider knowledge," notes one investigation of their past activities.

TikTok's Response

Unfortunately, as of the distribution time, TikTok has not formally responded to these particular affirmations. In any case, the company has already denied comparative breach claims, expressing that its security groups found no evidence of security breaches in its systems.

In later explanations of their security pose, TikTok has emphasised that "protected U.S. user data is

stored in the Oracle Cloud, with controlled and monitored gateways that only approved personnel have access to”

Security specialists recommend that TikTok clients take prompt preparatory measures: Change passwords immediately

- Enable two-factor authentication

- Monitor accounts for suspicious activity

- Be on alert for potential phishing endeavours leveraging the spilt data

As examinations proceed, this occurrence highlights continuous concerns approximately information security on major social platforms and the determined risk posed by advanced danger on-screen characters in the digital scene.

Don't forget to stay safe and update!?

Additional sources to explore: You can also search directly on Google for more information:

<https://x.com/efani/status/1915799214522875947>

https://www.linkedin.com/posts/dlross_hackers-allegedly-breach-tiktok-exposing-activity-7321600096754716672-aJCn

<https://cyberpress.org/hackers-claim-tiktok-breach/>

Nostre - April 28, 2025, 4:37 am

Well... they ain't lying, TikTok never answers.

Interested to see what happens in the future with this, if anything at all.

DramaKing - April 28, 2025, 5:46 am

Did they steal the algorithm?

JoseMar - April 28, 2025, 12:06 pm

(Apr 28, 2025 04:37 AM)Nostre Wrote: [\[CITE\]](#) Well... they ain't lying, TikTok never answers.

Interested to see what happens in the future with this, if anything at all.

I doubt they will respond. It seems they are just waiting for people to forget and let everything fade away.

(Apr 28, 2025 05:46 AM)DramaKing Wrote: [\[CITE\]](#) Did they steal the algorithm?

But there is no evidence that TikTok's algorithm or proprietary source code was accessed or stolen in this breach.

Depicide - April 28, 2025, 8:01 pm

I wonder if it also comes with the user categorization for targeted marketing. That would be interesting if someone could find a way to exploit it in the algorithm

Pr0m3th3us - April 28, 2025, 8:07 pm

I honestly smiled at this when i saw the headline

boondox420 - August 16, 2026, 7:22 pm

This is one of those incidents where I think the provenance of the data matters more than the size of the dump.

927,000 credential pairs sounds dramatic, but by itself it doesn't prove:

TikTok's authentication database was breached.

It only proves something meaningful once somebody independently establishes where those records came from.

The reporting I've seen still describes R00TK1T's claim as unverified, and TikTok reportedly said it had not found evidence of a breach affecting users on the scale being claimed.

So if I was analyzing this, these would be my first questions.

1. What exactly is in the dump?

"Username + password" isn't enough information.

I'd want to know:

- Email or TikTok username?

- Plaintext passwords or password hashes? Password-hash algorithm?

- Salts present? Internal numeric user IDs?

- Account creation timestamps? Last-login information?

- Phone numbers? Internal permission/status fields?

- Database column names? Backend-only metadata?

- Consistent schema across all records?

Those details tell you much more about where the information originated.

2. Plaintext passwords would actually make me MORE skeptical

If the claim is that attackers dumped a modern production authentication database and found 927,000 plaintext passwords, that deserves serious scrutiny.

Current NIST guidance says centrally stored passwords should be protected with salted password hashing rather than stored as recoverable plaintext.

That doesn't make plaintext impossible — companies can implement security badly — but it creates another possibility:

Maybe these aren't passwords extracted from TikTok's password database at all.

They could potentially be:

- infostealer logs

- phishing results credential-stuffing lists

- old combo lists data aggregated from multiple breaches

If an infostealer grabs:

`user@email.com : password123`

while the victim logs into TikTok, that credential pair can be perfectly valid while TikTok itself was never breached.

That's an extremely important distinction.

3. How many records are actually unique?

927,000 rows doesn't necessarily mean 927,000 newly compromised users.

I'd want someone to deduplicate:

usernames emails
password combinations repeated records
previously leaked credentials

Then compare them against older credential collections.

If 70% of the records already existed in older dumps, the story changes significantly.

If virtually everything is new and accompanied by TikTok-specific internal metadata, that becomes much more interesting.

4. Can the dataset be tied specifically to TikTok?

This would probably be the biggest question for me.

Suppose a record looks like:

`username | email | password`

That's weak provenance.

But imagine records instead contained consistent internal attributes such as:

`internal\_user\_id | account\_state | registration\_timestamp | region | auth\_metadata`

with relationships matching TikTok's internal systems.

That would be considerably stronger evidence.

The question shouldn't just be:

> "Do these credentials work?"

It should be:

> "Is there information here that realistically could have come only from TikTok's internal infrastructure?"

That's the difference between validating credentials and validating a breach source.

5. The account deletion claim needs separate proof

The threat actor reportedly also claimed they could delete TikTok accounts.

Even if screenshots show accounts being deleted, that doesn't automatically prove backend/database access.

If attackers possessed valid credentials or session material, individual account takeover could potentially explain some account modifications.

I'd want evidence distinguishing:

normal account-level access

from

privileged administrative/backend access.

Those are massively different levels of compromise.

6. What does the alleged cloud-server access actually prove?

Another claim being repeated is that an insecure cloud environment exposed credentials and platform code.

That's potentially huge — if independently demonstrated.

But I'd want technical evidence such as:

cloud provider indicators

directory structure service configuration

internal application artifacts code relationships

database schema infrastructure metadata

timestamps that establish when access occurred

Screenshots from the attacker aren't enough by themselves.

Threat actors have every incentive to make a compromise appear larger than it actually is.

7. I'd also separate three possible incidents

People sometimes combine these into one thing when they're actually very different.

Scenario A — TikTok backend breach

Attackers actually gained access to TikTok infrastructure and extracted user authentication data.

This would be extremely serious.

Scenario B — Third-party/cloud exposure

Something connected to TikTok leaked data because of a misconfigured service, vendor or storage environment.

Still serious, but technically different.

Scenario C — Credential aggregation

The attackers collected TikTok credentials from stealers, phishing, malware or previous breaches and marketed the collection as a "TikTok database."

TikTok infrastructure may never have been compromised.

All three could produce a headline saying:

“900,000 TikTok credentials leaked.”

Only one necessarily means TikTok itself was hacked.

8. R00TK1T's credibility matters too

The group has made multiple high-profile claims, and reporting on this particular incident noted that evidence had not conclusively supported the TikTok claim at the time.

That doesn't prove the claim is false.

It means the correct security-research position should probably remain:

unverified until independently corroborated.

9. What evidence would convince me?

For me, convincing evidence would probably involve several independent indicators:

Strong evidence:

- Internal TikTok-only database fields
- Consistent backend schema Newly exposed records
- Internal source code/infrastructure connected to the dataset Independent researchers validating provenance
- TikTok eventually confirming unauthorized access

Weak evidence:

- Telegram screenshots
- screenshots showing account deletion working username/password combinations
- threat-actor statements a giant text file containing credentials

Working credentials prove those credentials exist.

They don't necessarily prove where they were stolen.

10. Users should still respond defensively

Even if this turns out to be credential aggregation rather than a TikTok breach, valid leaked credentials are still dangerous.

I'd recommend:

- unique TikTok password changing reused passwords elsewhere
- enabling 2FA reviewing logged-in devices
- revoking unknown sessions checking connected applications
- watching for targeted phishing
- * monitoring the associated email account

Credential reuse could turn a completely unrelated compromise into a TikTok account takeover.

My current view

I'm not comfortable calling this:

"TikTok hacked — 927k passwords stolen"

based only on the evidence presented publicly.

I'd call it:

"Threat actor claims possession of 927k TikTok credentials; origin of the dataset still needs independent verification."

That's less exciting, but technically it's a much more important distinction.

The number of records isn't what I'd be investigating first.

I'd be investigating provenance.

If anyone has actually analyzed a sample, I'd be interested in knowing:

Were the passwords plaintext or hashes?

Did the records contain TikTok-specific internal fields?

How many records were unique/new?

Was any internal infrastructure independently tied to the dataset?

Because if those questions can't be answered, we may be looking at a credential collection being presented as a backend breach rather than evidence that TikTok's authentication database itself was compromised.

djexio - August 30, 2026, 1:29 am

I need one