Friend.tech exposes 100,000+ addresses related information, how to protect user privacy of social Dapps?

Beosin · Follow

6 min read · 1 day ago

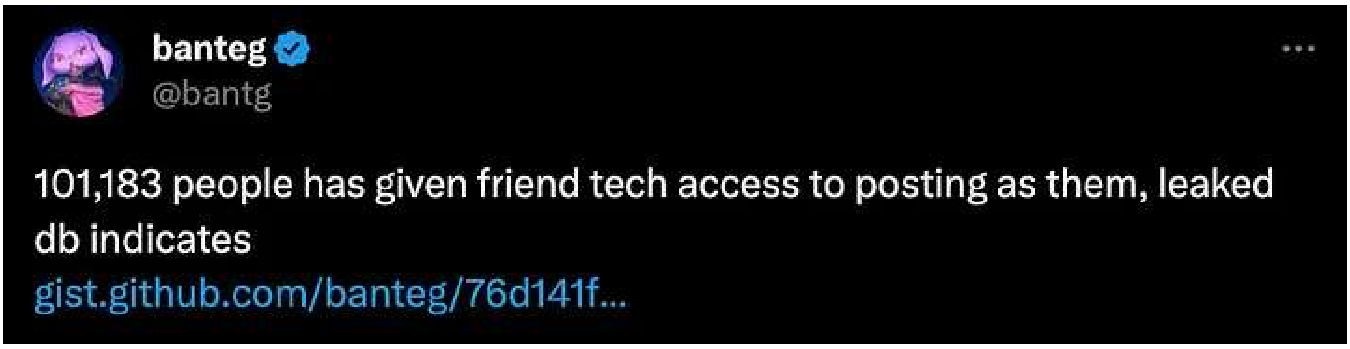
BEOSIN
Blockchain Security
Friend.tech exposes 100,000+ addresses related information, how to protect user privacy of social Dapps?

In just 12 days since its launch, Friend.Tech has attracted enthusiastic participation from Web3 users.

Friend.tech started invite-only beta testing and has quickly attracted a large number of users, even attracting the attention of big-name crypto influencers, NBA players, and OnlyFans creators.

This latest Web3 social application allows users to trade tokenized “shares” with their favorite influencers. Amidst the frenzy, some security crises have drawn attention.

On the afternoon of August 21, banteg, Yearn core developer, tweeted that more than 100,000 Friend.tech user information had been leaked. The leaked information included users’ wallet addresses and Twitter information, which caused huge controversy and attention.



banteg
@bantg

101,183 people has given friend tech access to posting as them, leaked db indicates
gist.github.com/banteg/76d141f...

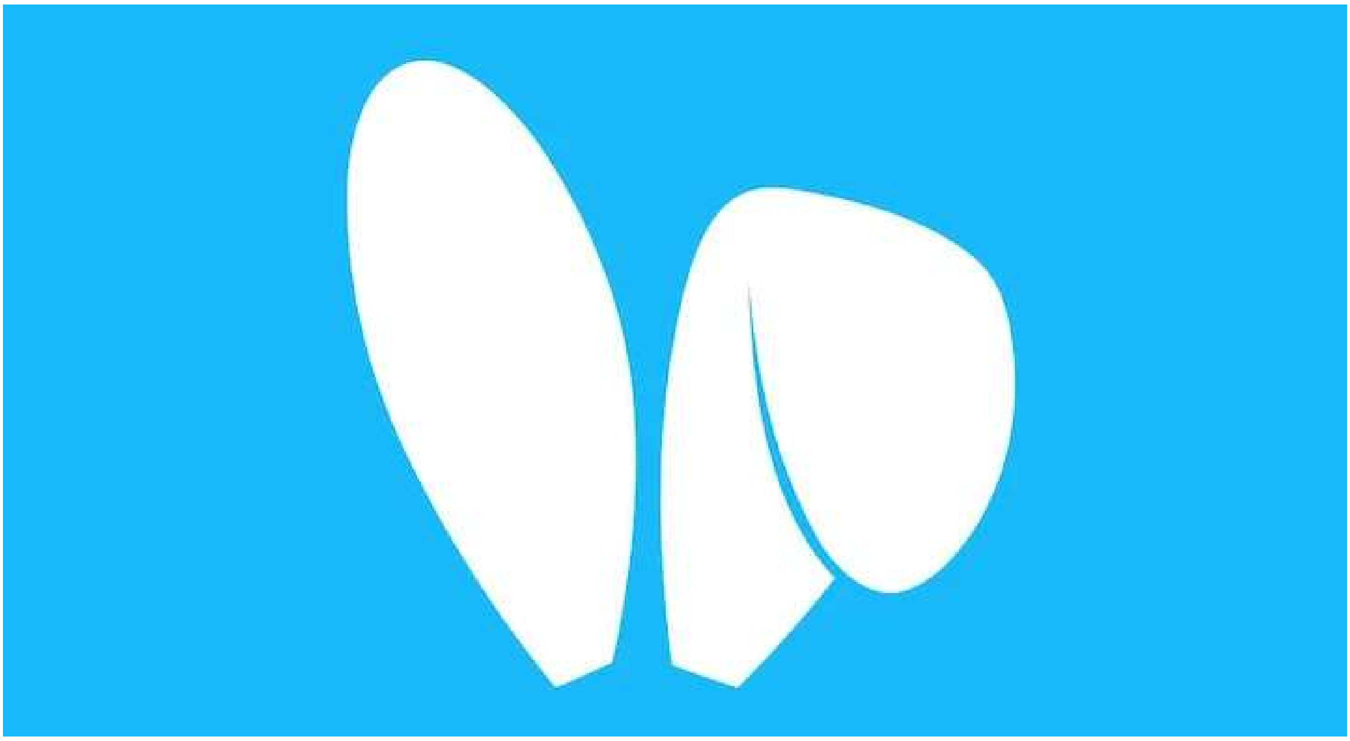
Beosin investigated the information leakage incident at the first time, and also conducted a detailed analysis of the Friend.tech project. The following is our analysis.

Base’s Hot New Dapp: What’s Friend Tech?

Friend.tech is a decentralized social application built on the Base blockchain. Users need to use Friend.tech by binding their Twitter accounts and crypto wallets to make profits. Friend.tech is to tokenize users’ influence, and users can purchase other users’ “shares” to obtain the right to communicate directly with other users. Yuga Cohler, a senior software engineer at Coinbase, emphasized in a tweet that Friend Tech is a decentralized social media platform for crypto users. **The core of Friend Tech’s innovation lies in the use of**

“shares” as digital assets. These shares symbolize ownership when interacting with crypto users. This concept mirrors the ownership principles of the stock market, where owning stock is equivalent to owning a stake in a particular company.

At present, the official website of Friend.tech is relatively simple, and the white paper and roadmap have not yet been released. **It is currently known that the increase of shareholder of each token will lead to the price increase and each transaction needs to pay an additional 10% transaction fee, of which 5% goes to the protocol and 5% goes to the creator**. At present, Friend.tech has more than 100,000 users. Cobie, a crypto KOL with more than 700,000 fans, and Ansem, a trader, have joined Friend.tech and the transaction volume of shares has exceeded $34 million.



What are the reasons for the explosion of Friend.tech?

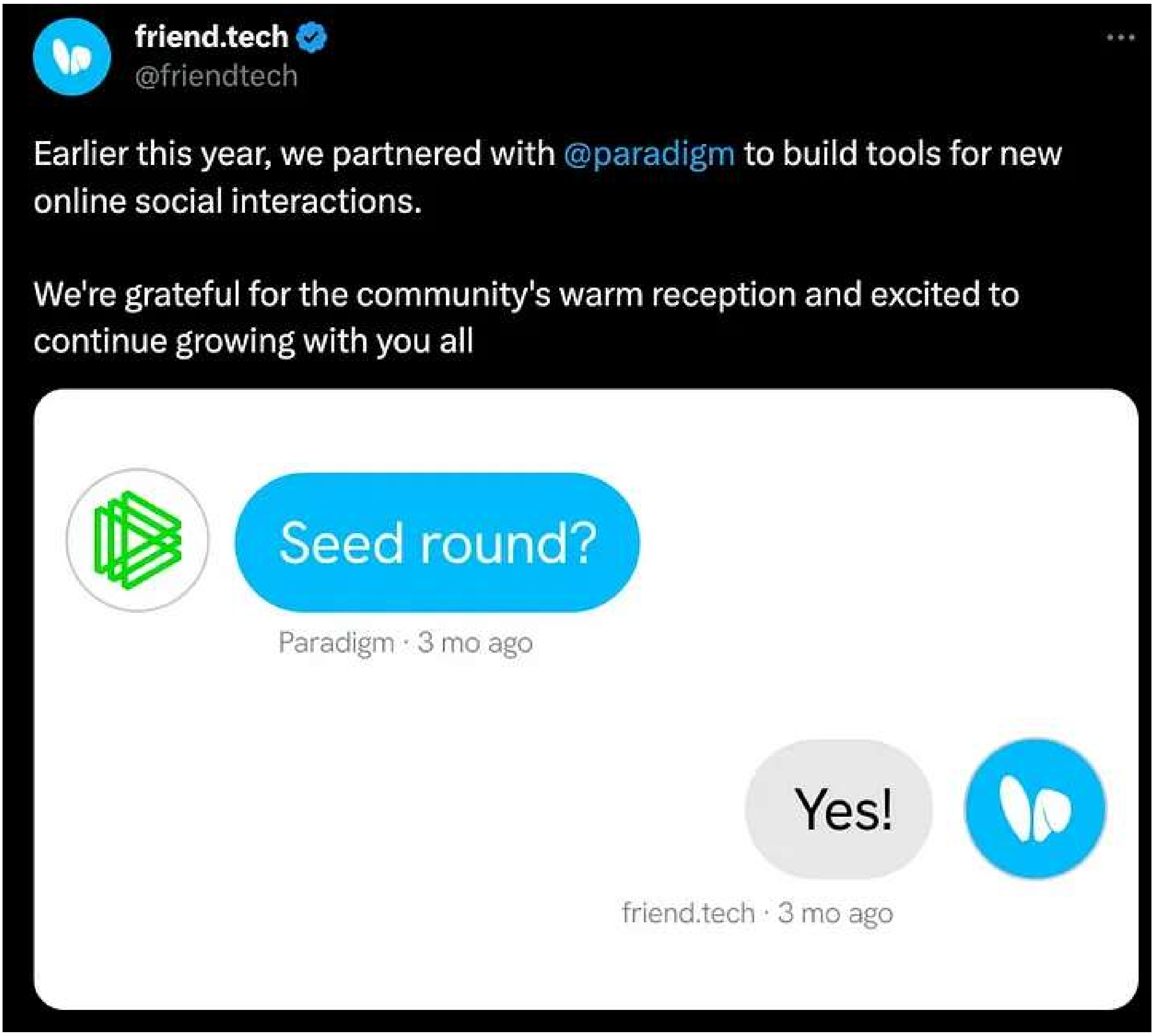
1. Twitter KOLs bring huge influence to Friend.tech

As a social product, Friend.tech offers considerable benefits by tokenizing influence into KOLs. Every time a user purchases Shares, the corresponding

KOL will receive 5% of the transaction fee. Therefore, Friend.tech is very attractive to influential KOLs. KOLs can benefit from their fan economy through Friend.tech, and the presence of KOLs has brought an increase in the number of users and popularity of Friend.tech.

2. Airdrop Expectations

On August 19, Friend.tech announced on Twitter that Paradigm will participate in its seed round of financing and Friend.tech will cooperate with Paradigm to build advanced social tools.



friend.tech
@friendtech

Earlier this year, we partnered with @paradigm to build tools for new online social interactions.

We're grateful for the community's warm reception and excited to continue growing with you all

Seed round?

Paradigm · 3 mo ago

Yes!

friend.tech · 3 mo ago

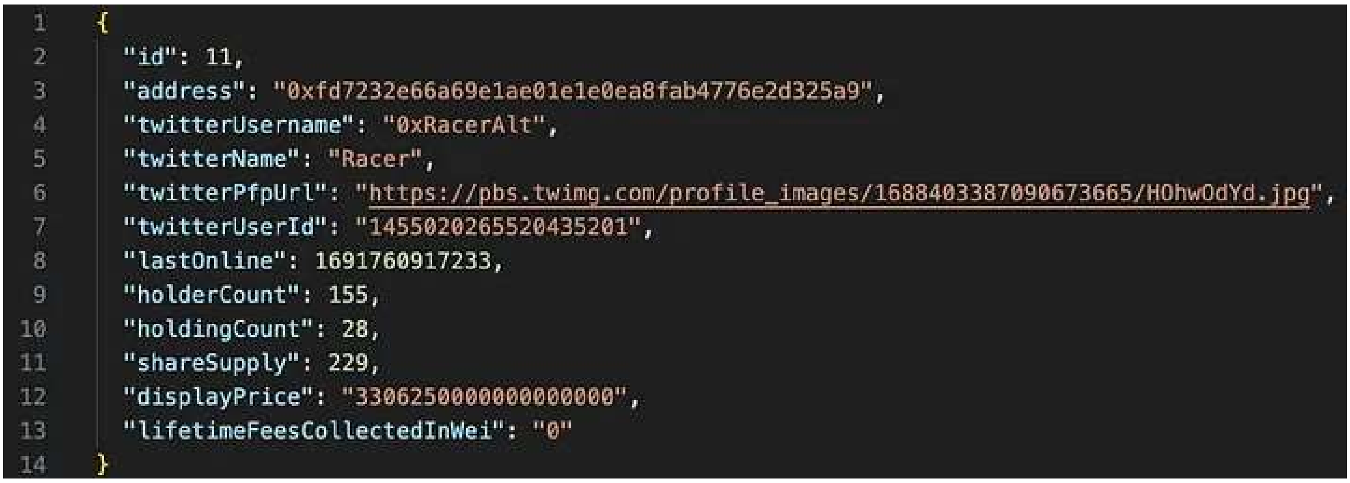
Users will get points when using Friend.tech. Friend.tech announced that these points will be used for special purposes after the 6-month test period ends, and the airdrop will refer to users' activities. Therefore, Friend.tech currently attracts a large number of airdrop hunters to contribute to Friend.tech's statistics.

Friend.tech Privacy Controversy

On August 21, more than 100,000 user data of Friend.tech were leaked. The reason is that the API provided by Friend.tech can directly query the user's wallet and the binded Twitter account. The queryable API link is as follows: https://prod-api.kosxxxx.com/users/0xfd7232e66a69e1ae01e1e0ea8fab4776e2d325a9

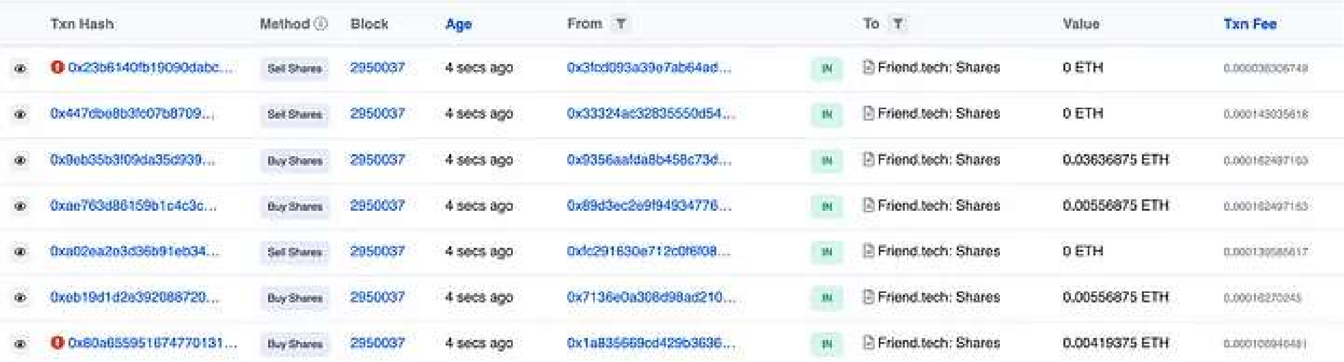
(The full link to the API has been hidden for security reasons)

Just replace the address in the link (the address of the founder of Friend.tech) with other addresses that interact with Friend.tech to find more information. The query results of the above API link:



```
{
  "id": 11,
  "address": "0xfd7232e66a69e1ae01e1e0ea8fab4776e2d325a9",
  "twitterUsername": "0xRacerAlt",
  "twitterName": "Racer",
  "twitterPfpUrl": "https://pbs.twimg.com/profile_images/1688403387090673665/HOhwOdYd.jpg",
  "twitterUserId": "1455020265520435201",
  "lastOnline": 1691760917233,
  "holderCount": 155,
  "holdingCount": 28,
  "shareSupply": 229,
  "displayPrice": "3306250000000000000",
  "lifetimeFeesCollectedInWei": "0"
}
```

Although Friend.tech responded that the information was scraped by Friend.tech's public API, it is irresponsible for reports of information leakage. The information includes wallet address and Twitter account, that is, on-chain information and off-chain information, which is enough for hackers or centralized institutions to locate the entity information of a wallet.



	Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
👁	❗ 0x23b6140fb19090dabc...	Sell Shares	2950037	4 secs ago	0x3fcd093a39e7ab64ad...	IN	Friend.tech: Shares	0 ETH	0.000038306749
👁	0x447dbe8b3fc07b8709...	Sell Shares	2950037	4 secs ago	0x33324ac32835550d54...	IN	Friend.tech: Shares	0 ETH	0.000143035618
👁	0x9eb35b3f09da35d939...	Buy Shares	2950037	4 secs ago	0x9356aafda8b458c73d...	IN	Friend.tech: Shares	0.03636875 ETH	0.000162497163
👁	0xae763d88159b1c4c3c...	Buy Shares	2950037	4 secs ago	0x89d3ec2e9f94934776...	IN	Friend.tech: Shares	0.00556875 ETH	0.000162497163
👁	0xa02ea2e3d36b91eb34...	Sell Shares	2950037	4 secs ago	0xdc291630e712c0f6f08...	IN	Friend.tech: Shares	0 ETH	0.000139585617
👁	0xeb19d1d2e392088720...	Buy Shares	2950037	4 secs ago	0x7136e0a308d98ad210...	IN	Friend.tech: Shares	0.00556875 ETH	0.00016270245
👁	❗ 0x80a655951674770131...	Buy Shares	2950037	4 secs ago	0x1a835669cd429b3636...	IN	Friend.tech: Shares	0.00419375 ETH	0.000100946481

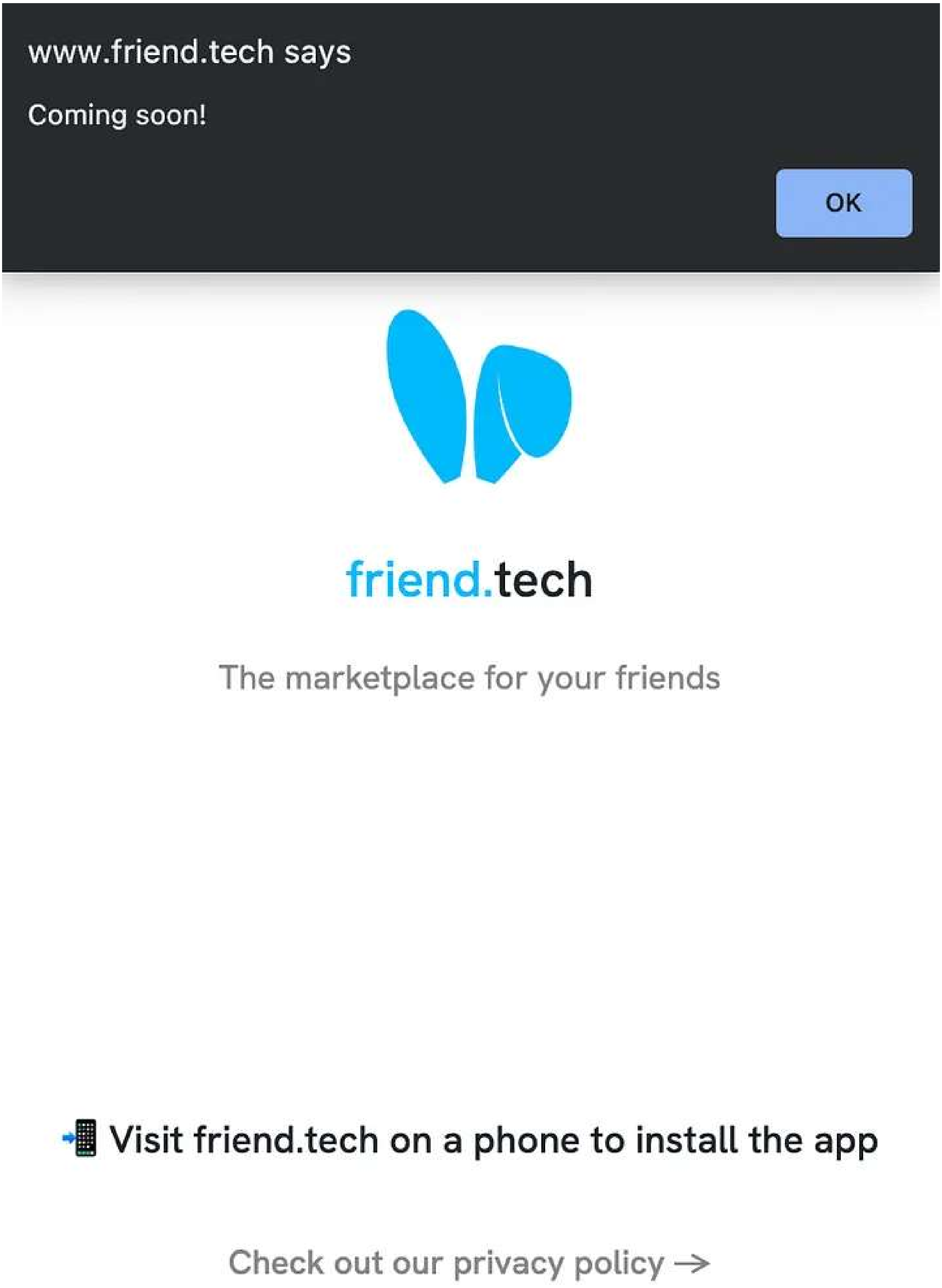
In addition, MEV bots can use the information provided by the current Friend.tech API and the information on the Base blockchain to monitor whether influential KOLs join Friend.tech, so as to frontrun their shares as soon as they join. At present, MEV bots on Friend.tech are already flooded, which is a harm to real users.

In addition, through further analysis of information provided by the current API and the leaked 100,000+ information, hackers may be able to obtain more transaction information and identity information about users who may face potential social engineering attacks.

How to solve the issues?

1. Clarify the privacy policy as soon as possible

Friend.tech has been live for 12 days, but its privacy policy still hasn’t been released. If Friend.tech continues to provide the current API access service, then Friend.tech should clearly state in its privacy policy that the API will provide your wallet information and twitter account information to everyone. If Friend.tech subsequently modifies the API access service, it also needs to declare in its privacy policy which API services Friend.tech will provide to which users, and which information will be provided to API callers.



www.friend.tech says

Coming soon!

friend.tech

The marketplace for your friends

📲 Visit friend.tech on a phone to install the app

Check out our privacy policy →

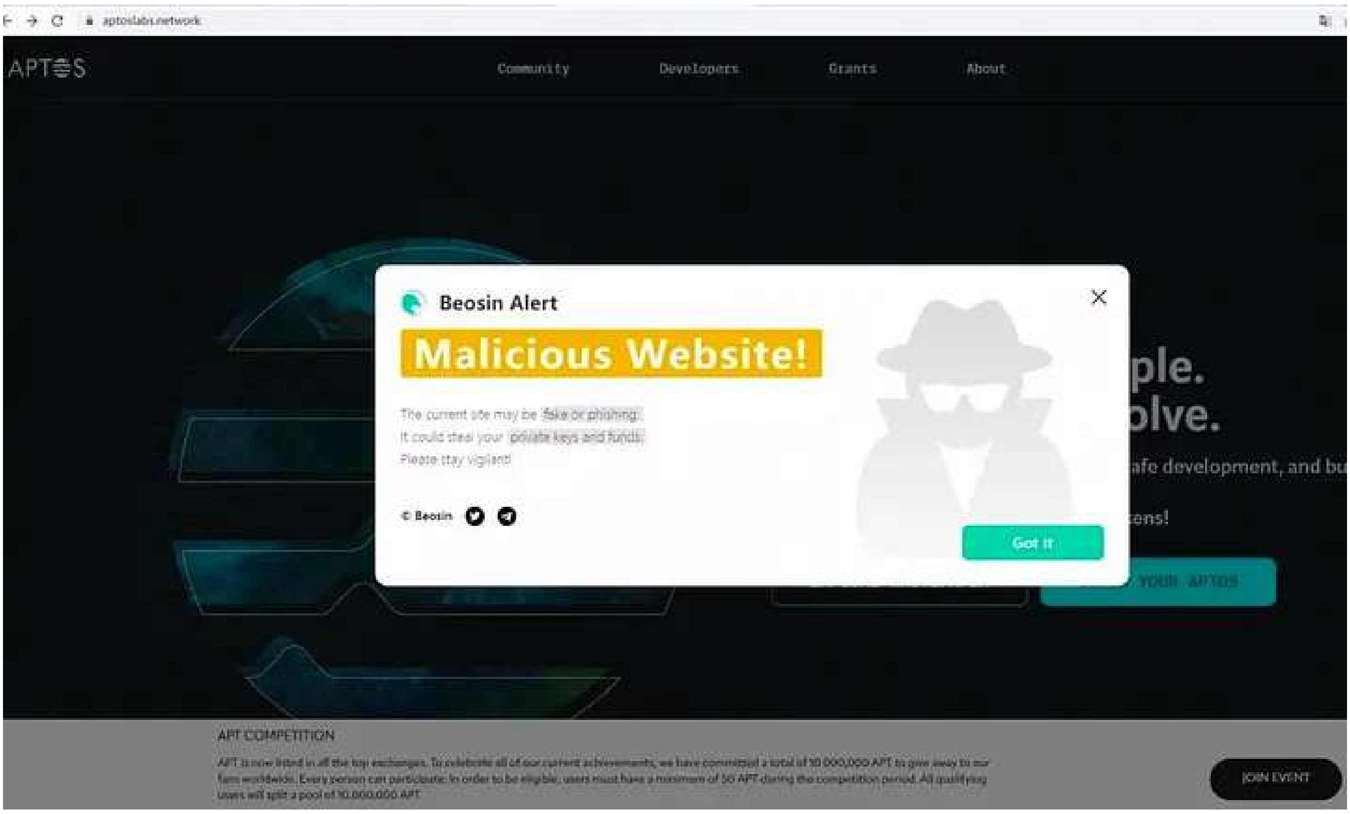
Friend.tech currently has no privacy policy

2. Adjust API access permissions

Although the addresses that interact with the Friend.tech contract are publicly available on the blockchain, this does not mean that Friend.tech should expose the addresses and associated Twitter accounts to everyone. Beosin suggested that Friend.tech's publicly accessible API should not include users' wallet information and Twitter account information at the same time. In addition, Friend.tech should restrict the non-holders of certain shares from viewing the corresponding user's wallet and Twitter account, which can prevent MEV bots from identifying influential users in advance and frontrunning. It is expected that Friend.tech can formulate more API access rules to better protect user privacy and provide a better user experience.

3. Account Segregation

Beosin recommends that users use a new wallet to interact with Friend.tech and the funds in this wallet should be withdrawn directly from the centralized exchange to avoid leaking the associated addresses. At the same time, for users who interacted with Friend.tech before August 22, their user data has been leaked, and they should pay attention to possible targeted phishing attacks in the future. We recommend the following Beosin Alert anti-phishing extension to readers and friends, which can identify most phishing websites in the Web3 field and protect everyone's wallet and asset security.



Beosin Alert

Malicious Website!

The current site may be fake or phishing.
It could steal your private keys and funds.
Please stay vigilant!

APT COMPETITION

APT is now listed in all the top exchanges. To celebrate all of our current achievements, we have committed a total of 10,000,000 APT to give away to our fans worldwide. Every person can participate. In order to be eligible, users must have a minimum of 50 APT during the competition period. All qualifying users will split a pool of 10,000,000 APT.

Anti-phishing extension download: https://chrome.google.com/webstore/detail/beosin-alert/lgbhcpagiobjacpmcgckfgodjeogceji?hl=en

Overall, Friend.tech is hot and has amassed tens of thousands of users, which is a promising sign for the Base ecosystem. However, some legal experts also reminded that Friend.tech may attract the attention of the SEC and the security and privacy risks mentioned above cannot be ignored.

Contact

If you need any blockchain security services, welcome to contact us:

Official Website Beosin EagleEye Twitter Telegram Linkedin