These DeFi Domains Might Be Risky to Investors

Table of Contents

Executive Report

Non-fungible token (NFT) companies like Dapper Labs and Yuga Labs were recently seen performing defensive domain registration. While this strategy is only a part of a broader brand protection program, large companies in other industries implement it as well.

WhoisXML API researchers examined how defensive domain registration looks like in the decentralized financial (DeFi) platform market. Did the DeFi companies themselves register the domains, or did other actors play a role? Among our findings are:

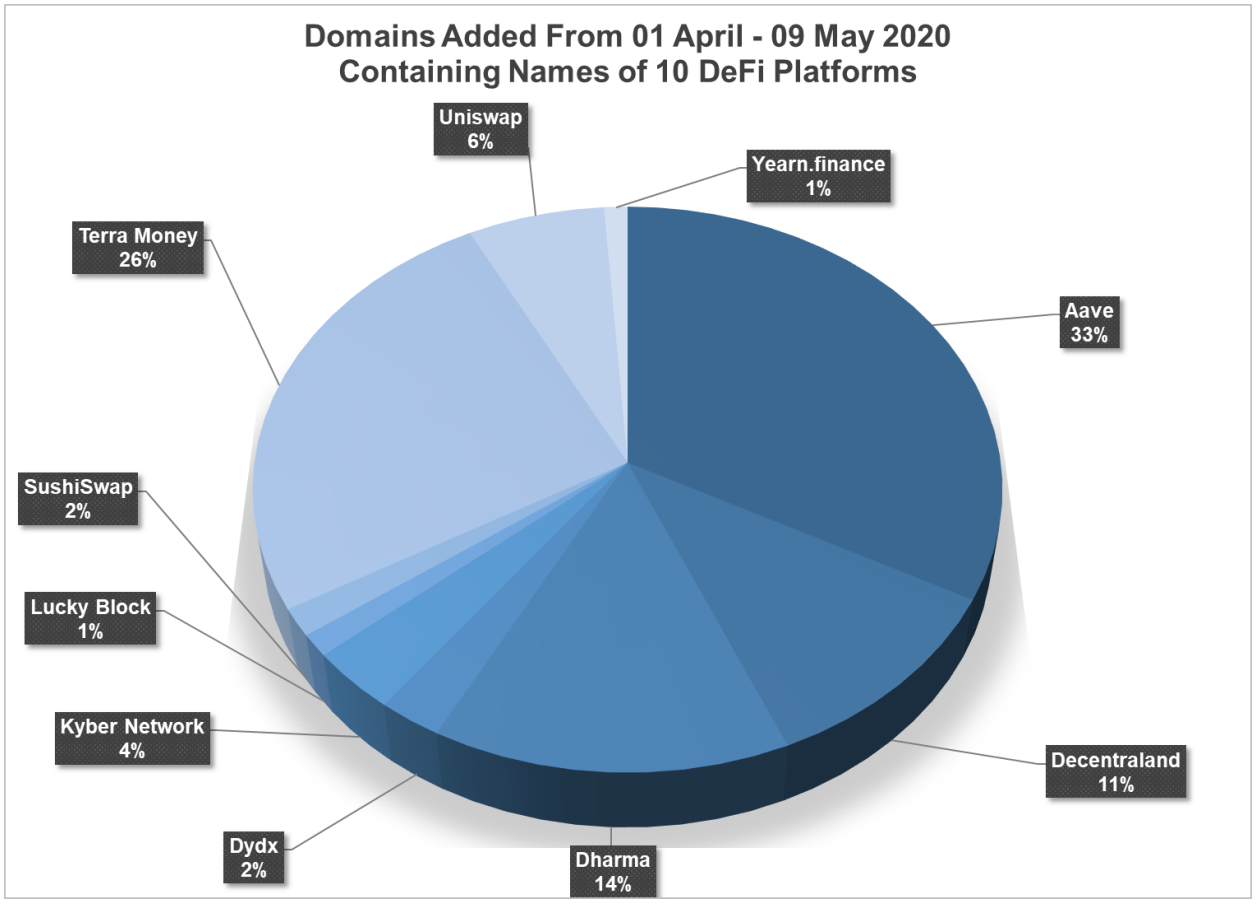
- 1,200+ domains added since 1 April 2022 contain the names of 10 of the most popular DeFi companies, namely, AAVE, Decentraland, Dharma, Dydx, Kyber Network, Lucky Block, SushiSwap, Terra, Uniswap, and Yearn.finance
- All of the platforms' official domain names had redacted WHOIS records, making attribution difficult
- None of the domains shared the same WHOIS characteristics, just the same privacy protection services, nameservers, registrars, and registrant countries
- Dozens of domains have already been flagged for phishing or malware hosting

32 DeFi Domains Registered Per Day Since 1 April 2022

Since 1 April 2022, we observed more than 1,200 domains that use the names of 10 DeFi platforms, pegging the average daily domain registration at 32 domains.

In some cases, we used the full domain names as search strings to reduce the number of false positives. For instance, we used "terra" and "money" to retrieve domains targeting Terra since "terra" alone yielded almost 4,000 domains, some of which may not necessarily be relevant to this study.

That said, about 33% of the domains we uncovered contained the string “aave,” followed by “terra money,” at 26%, “dharma” at 14%, and “decentraland” at 11%. The chart below shows the distribution of the domains.



The chart includes domain names that look very similar to the companies’ official domains aave[.]com and terra[.]money, such as aave[.]id, aaveu[.]com, aaave[.]co, terrag[.]money, lterra[.]money, and ttterra[.]money. We observed the same theme across the other domains, with most differing from the legitimate ones by only one or two characters.

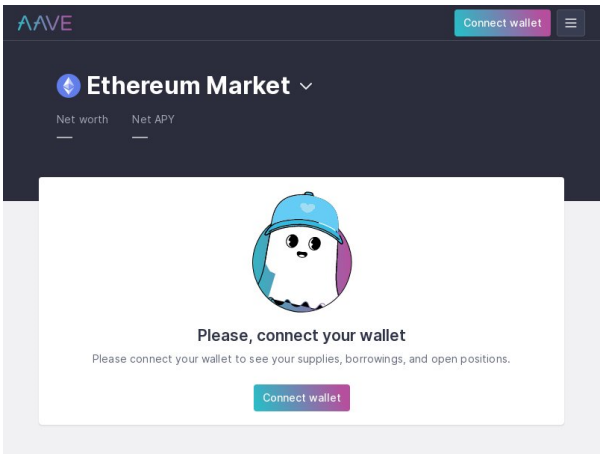
Who Owns the DeFi Domains?

All 10 DeFi companies used privacy redaction services, according to their WHOIS lookup results, making it challenging to attribute the possibly connected domains publicly. However, based on recurring WHOIS characteristics, such as registrars, nameservers, registrant countries, and privacy redaction service providers, we can only credit one domain each to Aave, Kyber Network, and Uniswap.

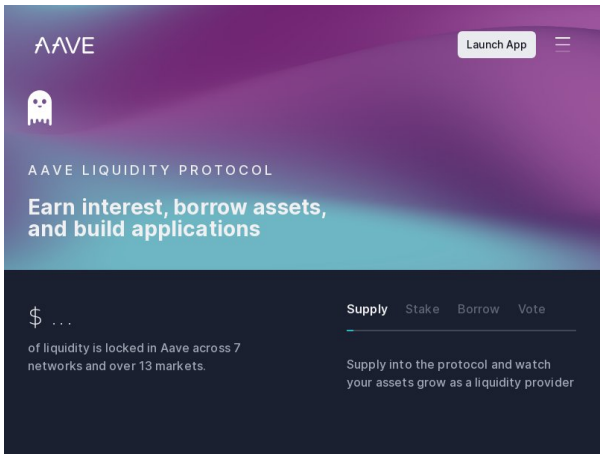
The rest of the domains may still have been registered by the companies, but we can't leave the possibility of malicious actors behind some of them. In fact, 40 domains have already been flagged as malicious as of 9 May 2022.

What Content Do the Domains Host?

One of the malicious domains, aaaave[.]com, continues to host content similar to the official Aave website. Here's a side-by-side comparison taken from Screenshot API.



Website screenshot of aaaave[.]com (malicious domain)

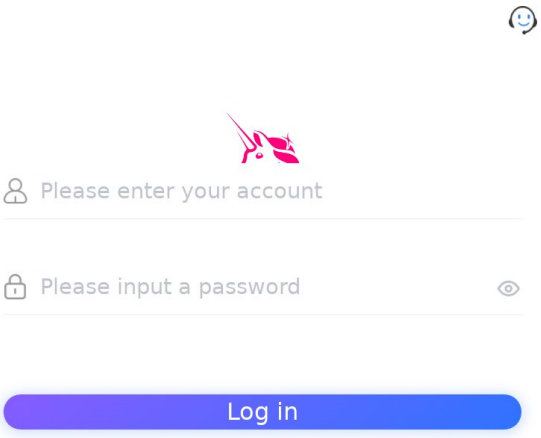


Website screenshot of aave[.]com (legitimate domain)

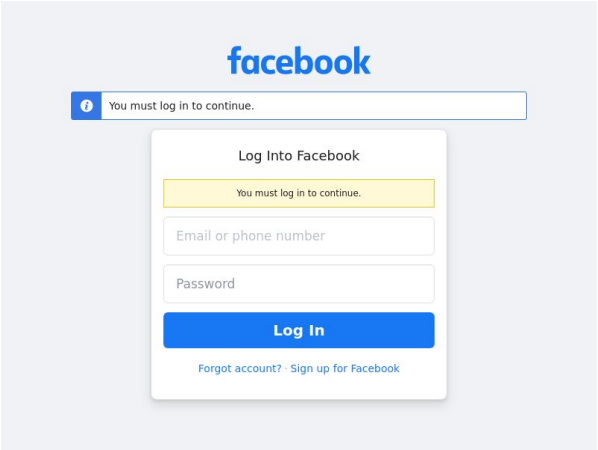
Other domains that hosted precisely the same content as the malicious domain include:

- aavee[.]fun
- aaveji[.]com
- app-aave-open[.]xyz
- app-aave[.]pw
- aypaave[.]com

Some domains hosted login pages, which can serve as vehicles for credential theft. Below are two examples.



Website screenshot of uniswap[.]homes



Website screenshot of luckyblock[.]pl

—

DeFi platforms and their users have become prime targets of cyber attacks, with two DeFi companies recently losing US$90 million to hackers. Some of the DeFi domains we found can be used in similar malicious campaigns, including phishing, malware-based attacks, and scams.

While defensive domain registration may not be the most scalable and practical cybersecurity practice, domain monitoring and investigation can help DeFi platforms detect threats early.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Domains

Sample DeFi Domains Created from 1 April to 9 May 2022

- aave[.]id
- saave[.]me
- xn--ave-8ka[.]com
- aaveu[.]us
- aaves[.]us
- aaave[.]co
- aaves[.]co
- aavee[.]fun
- aaver[.]fun
- aavey[.]fun
- decentraland[.]bi
- decentraland[.]my
- decentraland[.]sn
- decentraland[.]fi
- decentralland[.]me
- decentralland[.]cc
- decentralland[.]eu
- decentralland[.]pl
- decentragno[.]land
- 0decentraland[.]com
- dharmam[.]ga
- dharmaya[.]lk
- bedharma[.]co
- dharmakey[.]co
- dharma[.]my[.]id
- dharma-x[.]com
- dharmati[.]com
- dharmaps[.]com
- sirdharma[.]com
- dharmakan[.]com
- dydx[.]to
- dydx[.]id
- dydx-a[.]com
- dydx-z[.]com
- wpdydx[.]com
- svdydx[.]bar
- dydxdz[.]xyz
- dydx-b[.]com
- dydx-s[.]com
- dydx-c[.]com
- kyberrr[.]com
- kyberai[.]com
- kyberwolf[.]cz
- kyberswap[.]pw
- kyberlabs[.]sk
- kyberswep[.]io
- kybersec[.]net
- kyberdao[.]xyz
- kyberfive[.]com
- kyberswaps[.]pw
- luckyblock[.]pl
- luckyblocks[.]tk
- luckyblock[.]army
- luckyblock[.]club
- luckyblockbnb[.]com
- www-luckyblock[.]com
- luckyblockmeta[.]com
- metaluckyblock[.]com
- luckyblockdrop[.]live
- babyluckyblocks[.]com
- swapsushi[.]us
- sushiswap[.]cn
- swapsushi[.]org
- swapsushi[.]xyz
- sushiswaps[.]xyz
- swapsushi[.]site
- swappsushi[.]com
- sushiswapp[.]net
- sushiesswap[.]com
- sushiswapv2[.]com
- xn--trra-bpa[.]money
- terrag[.]money

- lterra[.]money
- terray[.]money
- terrad[.]money
- terrau[.]money
- terravm[.]money
- terrase[.]money
- terraxc[.]money
- terrasv[.]money
- uniswape[.]co
- xn--uiswap-bfb[.]app
- uniswap[.]llc
- uniswape[.]app
- swap-uni[.]com
- 0uniswap[.]com
- uniswappg[.]com
- uniswapv3[.]xyz
- uniteswap[.]com
- uuniswapp[.]org
- yearnfi[.]finance
- yearnfinance[.]cf
- finance-yearn[.]us
- yearn-finance[.]cc
- finance-yearn[.]cc
- yearn-finance[.]us
- finance-yearn[.]top
- finances-yearn[.]us
- yearne-finance[.]us
- finance-yearn[.]xyz

Malicious Properties Flagged during the Malware Check Dated 9 May 2022

- aaveu[.]com
- aaves[.]fun
- aavejs[.]com
- aaaave[.]com
- loaave[.]xyz
- aaveeee[.]com
- aqy-aave[.]com
- aaave[.]online
- aaaves[.]online
- open-aave[.]com
- aavecollection[.]online
- decentralandsell[.]com
- kyberswep[.]com
- acessoterra[.]xyz
- servicosterra[.]com
- personterrace[.]com
- remindterrain[.]top
- terraa-monneyy[.]com
- bridge-terra[.]cloud
- editerraneanse[.]xyz
- terraforms8y2[.]buzz
- plankenterras[.]online
- terrapia-kinesio[.]com
- terrastationapp[.]money
- josephineterrance[.]net
- terra-plus-burgau[.]com
- docs-terrastation[.]xyz
- terracecompression[.]top
- wvvvv-terrastation[.]xyz
- terrastation-verify[.]tk
- 932mayappleterrace[.]com
- terrainfabrication[.]top
- terramareristorante[.]xyz
- terra-statlon-wallettt[.]tk
- terrastation-wallet-web[.]gq
- hunterrainbootsfactoryoutlet[.]com
- subterraneanlyunprayerfullyfluttered[.]com
- uniswap-pos[.]monster
- swapnfts-community[.]com
- yearne-finance[.]us