IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Microsoft Corporation, Plaintiff, v. Does 1-10 Operating an Azure Abuse Network, Defendants.	Case No. 1-24-cv-2323

DECLARATION OF MAURICE MASON IN SUPPORT OF MICROSOFT'S MOTION TO FILE A FIRST AMENDED COMPLAINT

I, Maurice Mason, declare as follows:

1. I am a Principal investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration based upon my personal knowledge, and upon information and belief based on my review of documents and evidence collected during Microsoft's investigation and civil discovery in this action. I respectfully submit this declaration in support of Microsoft's Motion for Leave to File an Amended Complaint.

2. I have been employed by Microsoft since August 2021. In my role, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities is protecting Microsoft's online service assets from network-based attacks. Prior to my current role, I worked as a Senior Consultant on Microsoft's Incident Response Team, where I was a lead digital forensic analyst managing multiple incident response and threat-hunting engagements that included performing incident response and forensic analysis for Fortune 500, Fortune 100, and Fortune 50 companies. Prior to joining Microsoft, I held various positions, both in the private sector and in government, where I

performed digital forensic analysis, including on malware and ransomware-related matters. A true and correct copy of my curriculum vitae is on the docket in this action as Exhibit 1 to my December 19, 2024 declaration in this case.

3. As explained in my December 19 declaration, I am one of the persons responsible for Microsoft's investigation into the groups of actors described in Microsoft's filings in this case as the Azure Abuse Enterprise. The Azure Abuse Enterprise consists of distinct groups of individuals responsible for developing, maintaining, and using a set of custom tools designed to abuse generative AI services provided by Microsoft and several other companies. At a high level, the Azure Abuse Enterprise's scheme involves stealing Microsoft customer credentials, using those stolen credentials to gain unauthorized access to Microsoft's systems, and circumventing Microsoft's content filtering technology in order to generate and distribute unlawful and/or harmful images.

Defendants' Malicious Generation of Harmful Images

4. My December 19 declaration explains that harmful images generated by the Azure Abuse Enterprise include metadata comprising a digitally signed manifest which contains a set of assertions commonly referred to as Coalition for Content Provenance and Authenticity ("C2PA") Content Credentials. Through their abuse of Microsoft's Azure OpenAI Service, Defendants in this case have created thousands of harmful images with C2PA Content Credentials identifying Microsoft's technology as the source of those harmful images, even though Microsoft goes to great lengths to prevent generation of harmful content, as explained in the December 19, 2024 declarations of my colleagues Rodel Finones and Jason Lyons and reflected in Microsoft's 2024 Whitepaper entitled "Protecting the Public from Abusive AI-

Generated Content." A true and correct copy of the 2024 Whitepaper is attached hereto as **Exhibit 1**.

5. The harmful images generated by the Azure Abuse Enterprise and its end users include non-consensual intimate imagery. Consistent with the 2024 Whitepaper's discussion of the growing risk of harm from such imagery, the Azure Abuse Enterprise's malicious image generation is deeply gendered, with women most often targeted. Certain celebrities, including some male celebrities, also appear to have been a particular focus of the Azure Abuse Enterprise's malicious content generation.

6. Malicious intent to generate harmful non-consensual intimate imagery is apparent from certain Defendants' deliberate technological circumvention methods and systematic efforts to repeatedly generate content that was in many instances humiliating and dehumanizing. These Defendants engaged in a consistent pattern of abuse of Microsoft's systems in order to generate content that is obviously impermissible under Microsoft's contractual agreements and AI policy positions.

Individuals Identified to Date

7. Since I submitted my prior declaration to the Court on December 19, 2024, there have been several significant developments in Microsoft's investigation. First, Microsoft served and obtained responses to several subpoenas. Information obtained in response to Microsoft's subpoenas has furthered Microsoft's attribution efforts. Second, execution of the Court's temporary restraining order and preliminary injunction has resulted in disruption of Defendants "aitism.net" infrastructure and yielded additional data related to the users of such infrastructure. Such data has also furthered Microsoft's attribution efforts. Third, in response to service of process on Defendants and public commentary about this litigation, Microsoft has received

communications from certain Defendants and/or persons associated with Defendants. These communications have also furthered Microsoft's attribution efforts. Fourth, Microsoft has observed communications on public message boards such as 4chan and Rentry discussing this litigation, Microsoft, and its counsel. These and other developments have allowed Microsoft to ascertain the true identities of several people named in Microsoft's original complaint, and to identify several new individuals involved with the Azure Abuse Enterprise.

8. The individuals Microsoft has identified fall into three general categories. The first category of individuals, referred to in Microsoft's proposed First Amended Complaint as the "Infrastructure Provider Defendants," provided the tooling (e.g., the de3u application and oai-reverse-proxy software), communications infrastructure (e.g., Cloudflare tunnel and reverse proxy domains), monetization mechanisms, and instructions for using their technology and services of the Azure Abuse Enterprise. Infrastructure Provider Defendants and unnamed co-conspirators of theirs include:

- Defendant Arian Yadegarnia, who appears to reside in the Islamic Republic of Iran
- Defendant Alan Krysiak, who appears to reside in the United Kingdom
- Defendant Ricky Yuen, who appears to reside in the Hong Kong Special Administrative Region of the People's Republic of China
- Defendant Phát Phùng Tấn, who appears to reside in the Socialist Republic of Vietnam
- Doe 2, a person Microsoft has identified who appears to reside in the United States
- Doe 3, a person Microsoft has identified who appears to reside in the Republic of Austria and uses the alias "Sekrit"
- A person Microsoft has identified who appears to reside in the United States and uses the alias "Pepsi"

- A person Microsoft has identified who appears to reside in the United States and uses the alias "Pebble"

9. The second group of individuals Microsoft has identified are end users of the Infrastructure Provider Defendants' technologies who used such technologies to generate non-consensual intimate imagery, often targeting specific celebrities. These Defendants, currently identified in Microsoft's original Complaint and proposed First Amended Complaint as DOEs 4-7 include:

- A person using the alias "dazz" believed to reside in United Kingdom
- A person using the alias "Jorge" believed to reside in United States
- A person using the alias "jawajawaable" believed to reside in Turkey
- A person using the alias "1phlgm" believed to reside in Russia

Based off my investigation, "dazz", Jorge", "jawajawaable", and "1phlgm" utilize the infrastructure provided by DOEs 1-3 to create images that targeted celebrities in a harmful, offensive and misogynistic way.

10. A third group of individuals Microsoft has identified are end users who appear to have used the Azure Abuse Enterprises' technology and services to generate content that is not specifically in violation of our terms of use. These individuals appear to have knowingly used the Azure Abuse Enterprises' malicious infrastructure to gain unauthorized access to Microsoft's systems, but did so to gain free services unrelated to the types of harmful content created by Does 4-7. These individuals include:

- An end user who appears to be located in Argentina
- An end user who appears to be located in Paraguay
- An end user who appears to be located in Denmark

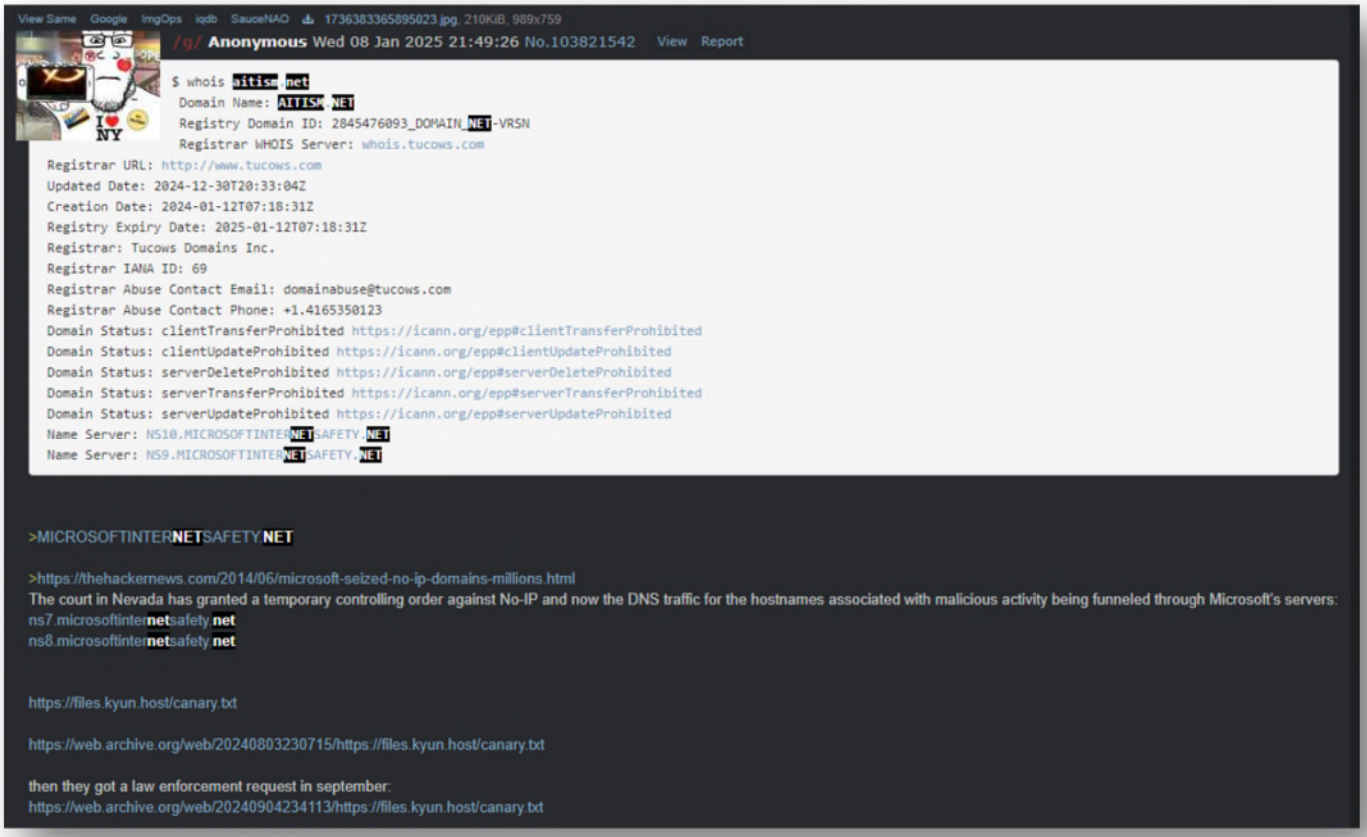
11. Microsoft's investigation is ongoing, and it is believed that Microsoft will gain further attribution evidence and may identify additional end users or infrastructure providers as discovery and investigation in this case continue.

Additional Evidence Developed Since December 2024

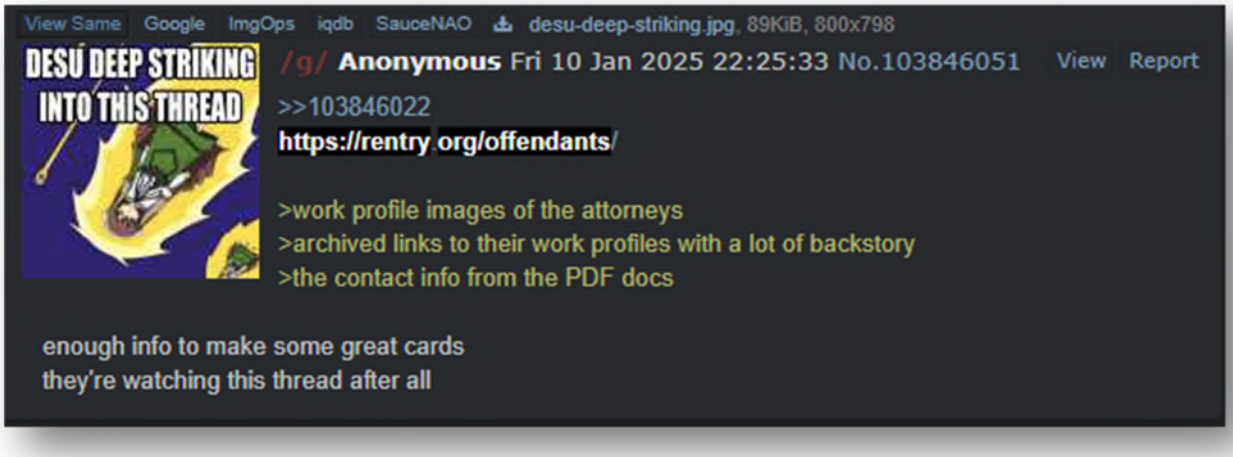
12. Microsoft has developed substantial additional evidence since filing its original temporary restraining order ("TRO") application in December 2024. The existence of this case, the Court's TRO, discovery, and continued investigative work by my colleagues and I have put Microsoft in a position to file a First Amended Complaint.

13. For example, after Microsoft served Defendants with the complaint and TRO in this action, Microsoft observed communications on 4chan starting on January 7th, 2025. In one such communication, a 4chan user user referring to DOE 1 aka "Fizz" stated "They got him" and another responded "maybe OpenAI and co.?" A true and correct screenshot of communications on 4chan dated January 7th, 2025 is included below and attached hereto as **Exhibit 2**.

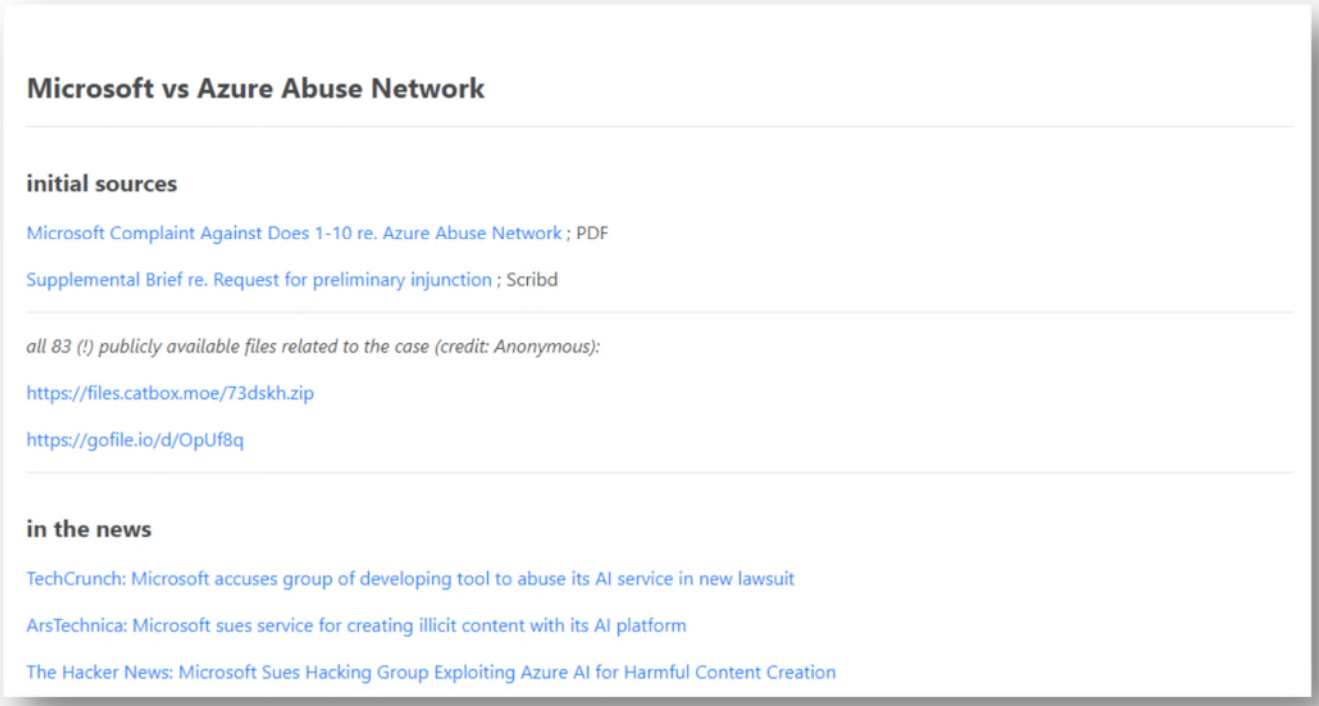
14. In another online communication, an apparent user of the reverse proxy service described in Microsoft's original complaint noted the apparent seizure of the "aitism.net" domain by Microsoft. A true and correct screenshot of this communications is included below and attached hereto as **Exhibit 3**.



15. In another online communication, an anonymous user posted a link to a website doxing the Microsoft attorneys responsible for prosecuting this case. A true and correct screenshot of this communications is included below and attached hereto as **Exhibit 4**.



16. A compilation of true and correct screenshots of portions of the doxing webpage described above is provided below and attached hereto as **Exhibit 5**.



Microsoft vs Azure Abuse Network

initial sources

Microsoft Complaint Against Does 1-10 re. Azure Abuse Network ; PDF

Supplemental Brief re. Request for preliminary injunction ; Scribd

all 83 (!) publicly available files related to the case (credit: Anonymous):

https://files.catbox.moe/73dskh.zip

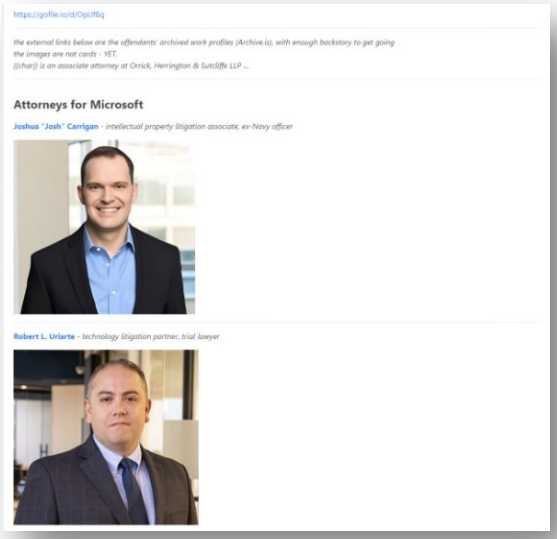
https://gofile.io/d/OpUf8q

in the news

TechCrunch: Microsoft accuses group of developing tool to abuse its AI service in new lawsuit

ArsTechnica: Microsoft sues service for creating illicit content with its AI platform

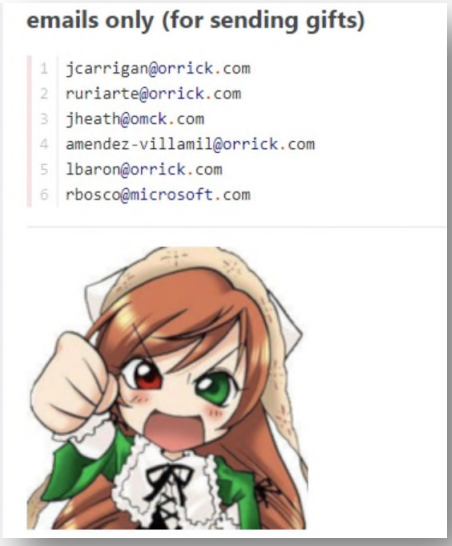
The Hacker News: Microsoft Sues Hacking Group Exploiting Azure AI for Harmful Content Creation



Attorneys for Microsoft

Joshua "Josh" Carrigan - *intellectual property litigation associate, ex-Navy officer*

Robert L. Uriarte - *technology litigation partner, trial lawyer*

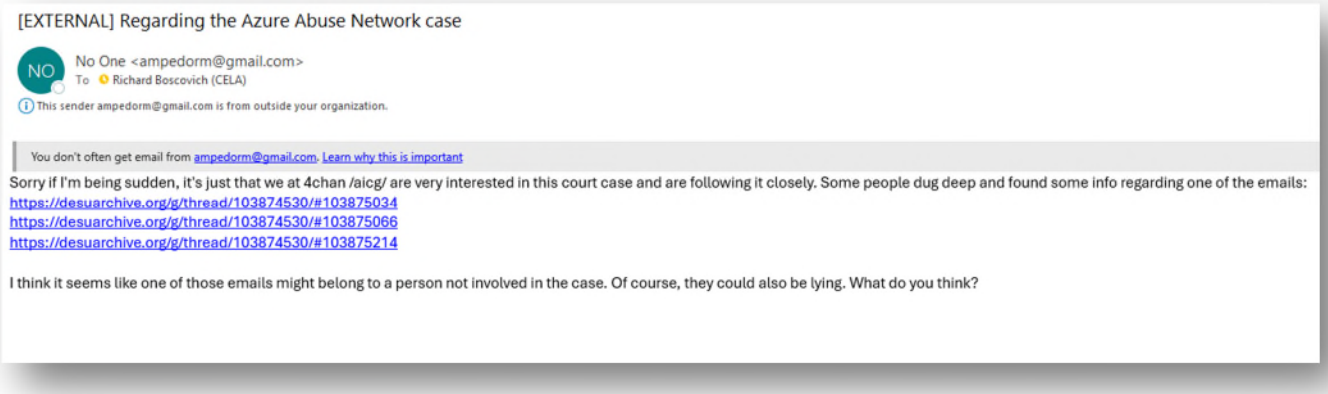


emails only (for sending gifts)

```
jcarrigan@orrick.com
ruriarte@orrick.com
jheath@omck.com
amendez-villamil@orrick.com
lbaron@orrick.com
rbosco@microsoft.com
```

17. In another 4chan communication dated January 11, 2025, an anonymous user discussed the true name of the online persona known as "Fiz." A true and correct screenshot of this communications is included below and attached hereto as **Exhibit 6**.

18. In addition to communications observed on 4chan, Microsoft attorneys received direct communications from persons who appear to be involved with, or at least aware of, the conduct and technical infrastructure described in Microsoft's original complaint. A true and correct screenshot of one such communications is included below and attached hereto as **Exhibit 7**.



19. In addition to the communications described above, Microsoft also observed conduct by certain individuals that helped further Microsoft's investigative efforts. For example, Microsoft observed efforts by certain Defendants designed to obfuscate relevant evidence. I understand from certain subpoena responses that after Microsoft provided notice of this action to email addresses associated with Defendants, persons associated with those email addresses began deleting webpages and source code repositories related to the conduct described in Microsoft's complaint.

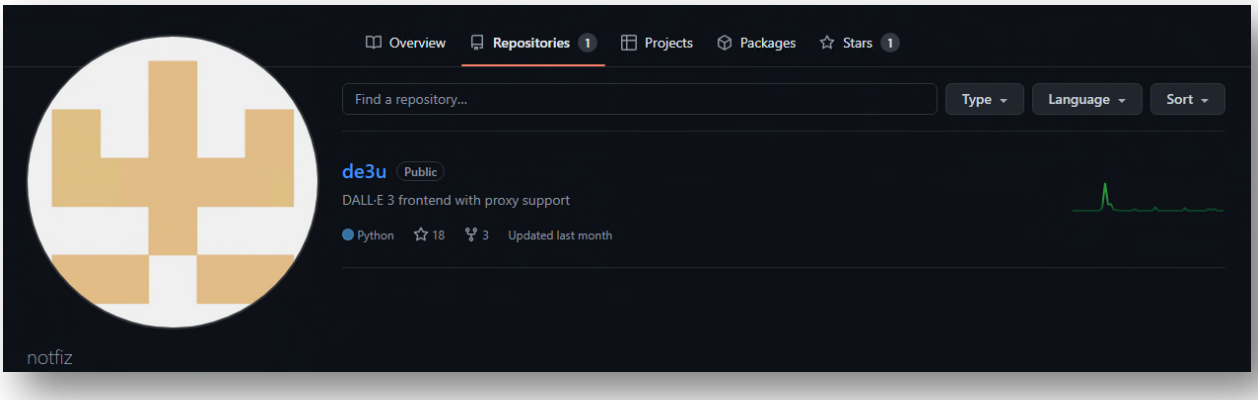
20. In conjunction with the developments described above, Microsoft has continued its investigative efforts and has uncovered significant additional attribution evidence. Although Microsoft's investigation is ongoing, the evidence Microsoft has developed to date establishes the true identities of the following DOE defendants described in the Complaint.

DOE 1 is Arian Yadegarnia aka "Fiz."

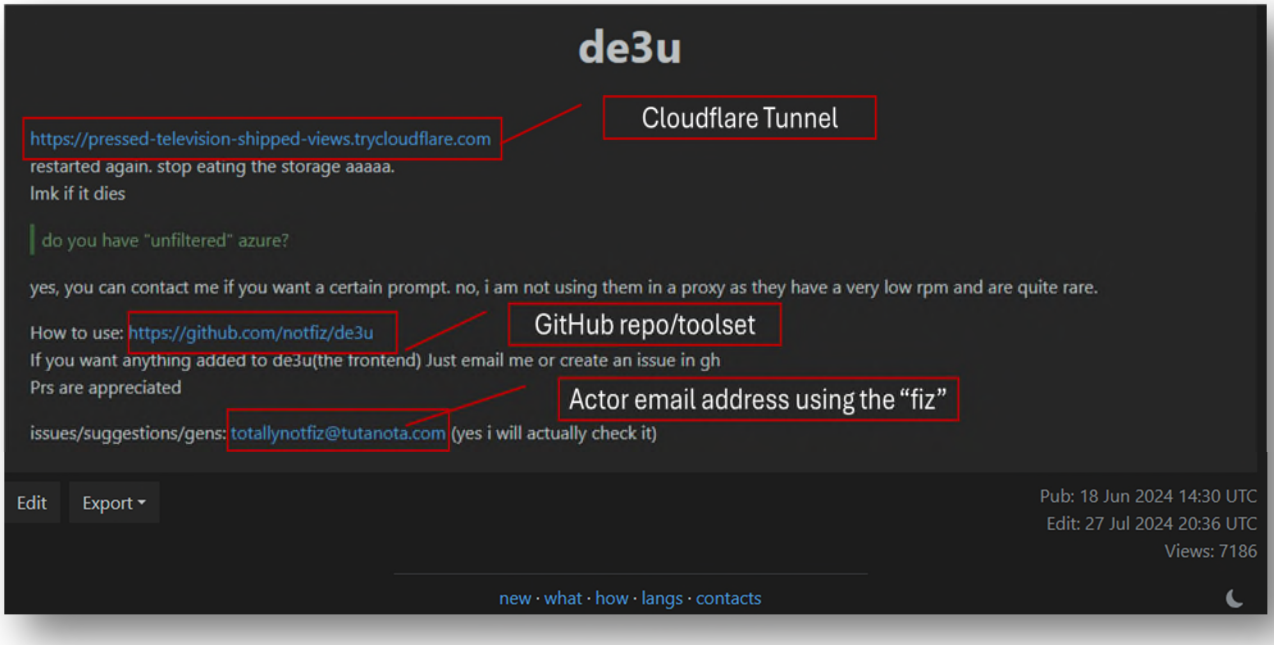
21. The individual described in Microsoft's original complaint as DOE 1 is a natural person named Arian Yadegarnia aka "Fiz." Yadegarnia appears to reside within the Islamic Republic of Iran. Microsoft's continued investigation has identified that Yadegarnia created client-side software tool referred to by Defendants as "de3u" and controlled the websites https://rentry.org/de3u and the source code repositories located at https://github.com/notfiz/de3u, which was used to u carry out Azure Abuse Enterprise. Additional analysis identified that Yadegarnia forked[1] the oai-reverse-proxy source code initially authored by "Khannon" and provided it on their own personal Gitgud page https:// gitgud.io/fiz1/oai-reverse-proxy. Reviewing data from discovery Microsoft revealed that Yadegarnia was recently visiting the "aitism.net" website on January 10, 2025. This website was a part of the static infrastructure used to operate the Defendants' scheme.

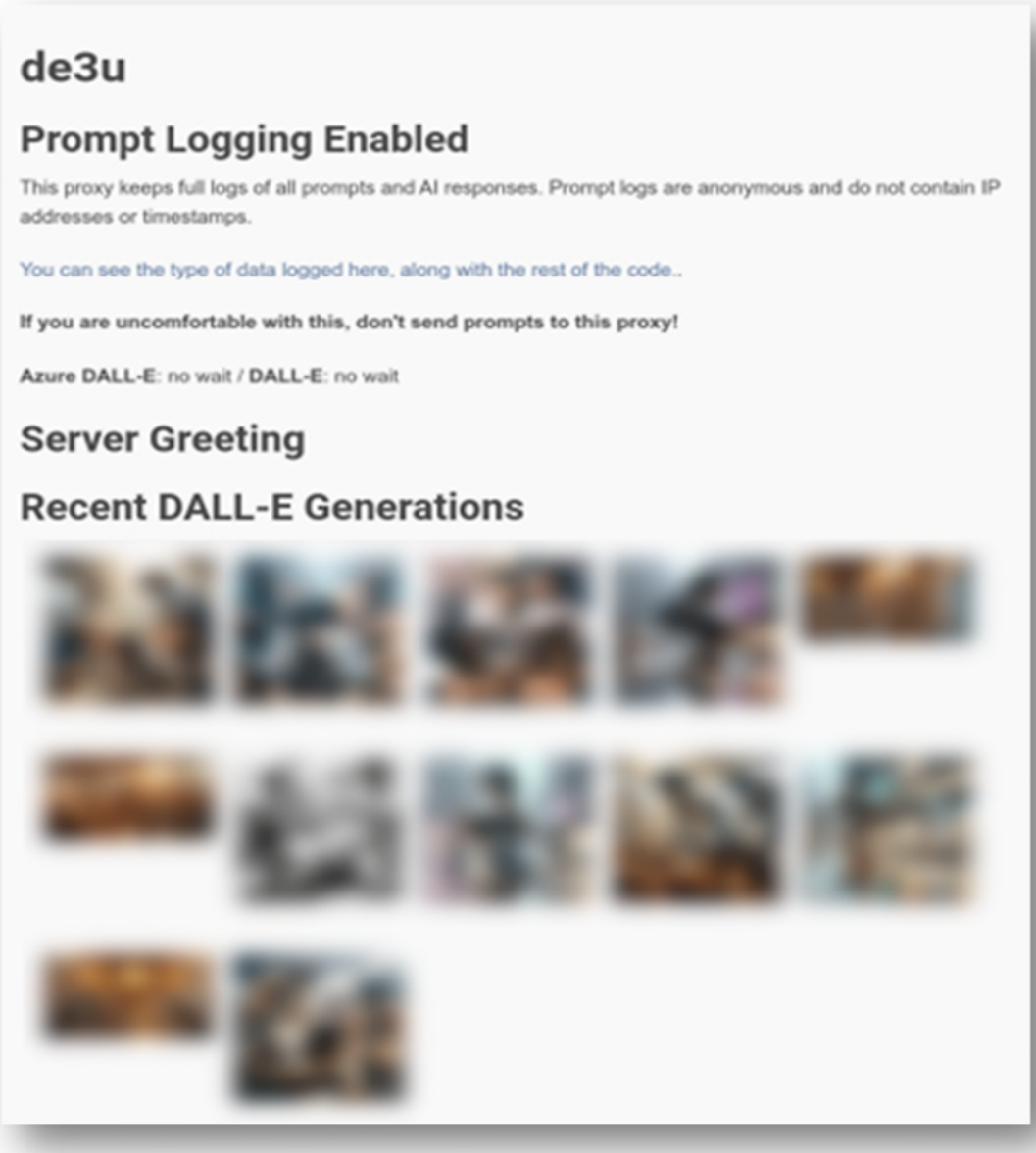
22. A true and correct screenshot of Yadegarnia's GitHub page containing de3u source code is included below and attached hereto as **Exhibit 8.**

[11] In the context of computer programing, "forking" generally refers to making a copy of a source code repository (the one being forked) and starting a new branch of source code development.



23. A true and correct compilation of screenshots from Yadegarnia's de3u webpages used to operate the Azure Abuse Enterprise is included below and attached hereto as **Exhibit 9.** Offensive images contained in one of the screen captures below have been obfuscated to protect the victims of the Azure Abuse Enterprise and the public.





de3u

Prompt Logging Enabled

This proxy keeps full logs of all prompts and AI responses. Prompt logs are anonymous and do not contain IP addresses or timestamps.

You can see the type of data logged here, along with the rest of the code..

If you are uncomfortable with this, don't send prompts to this proxy!

Azure DALL-E: no wait / **DALL-E**: no wait

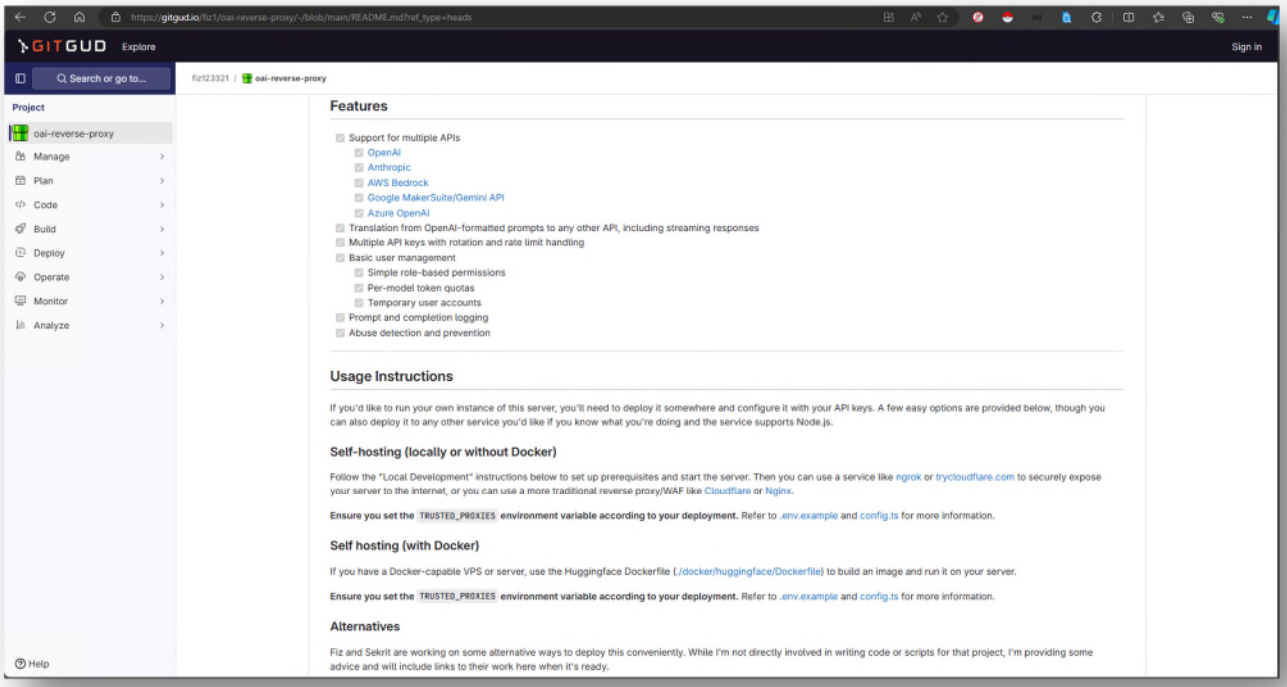
Server Greeting

Recent DALL-E Generations

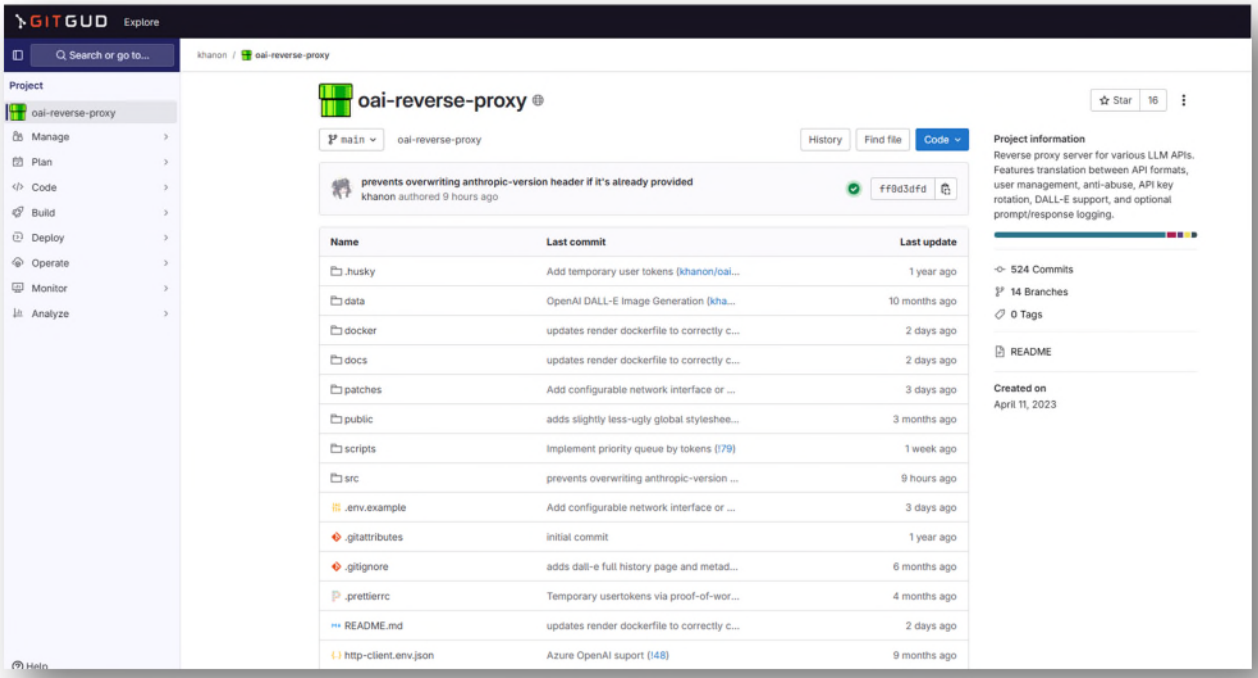
DOE 2 is "Khanon"

24. The individual described in Microsoft's original complaint as DOE 2 is a natural person who resides in the State of Illinois. As explained in Microsoft's prior papers, DOE 2 contributed to the Azure Abuse Enterprise the "oai-reverse-proxy" service used to operate the Azure Abuse Enterprise. Microsoft is aware of Khanon's true identity but is not proceeding with civil claims against him to avoid entanglements between this civil action and any potential criminal proceedings.

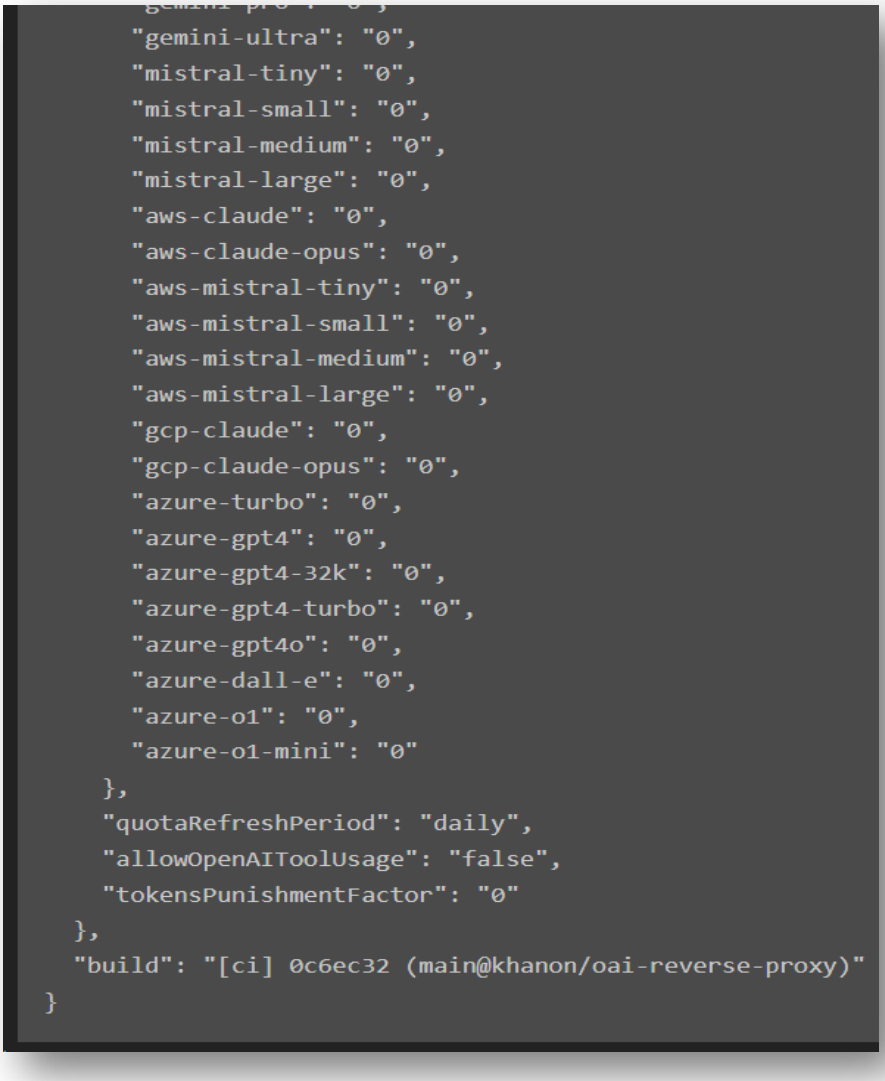
25. A true and correct screenshot of Yadegarnia's GitGud page containing source code authored by Khannon and forked by Yadegarnia is included below and attached hereto as **Exhibit 10.**



26. A true and correct screenshot from Khannon's GitGud page containing source code authored by Khannon for the oai-reverse-proxy tool is included below and attached hereto as **Exhibit 11.**



27. A true and correct screenshot from a Cloudflare tunnel used to operate the Azure Abuse Enterprise is included below and attached hereto as **Exhibit 12.**

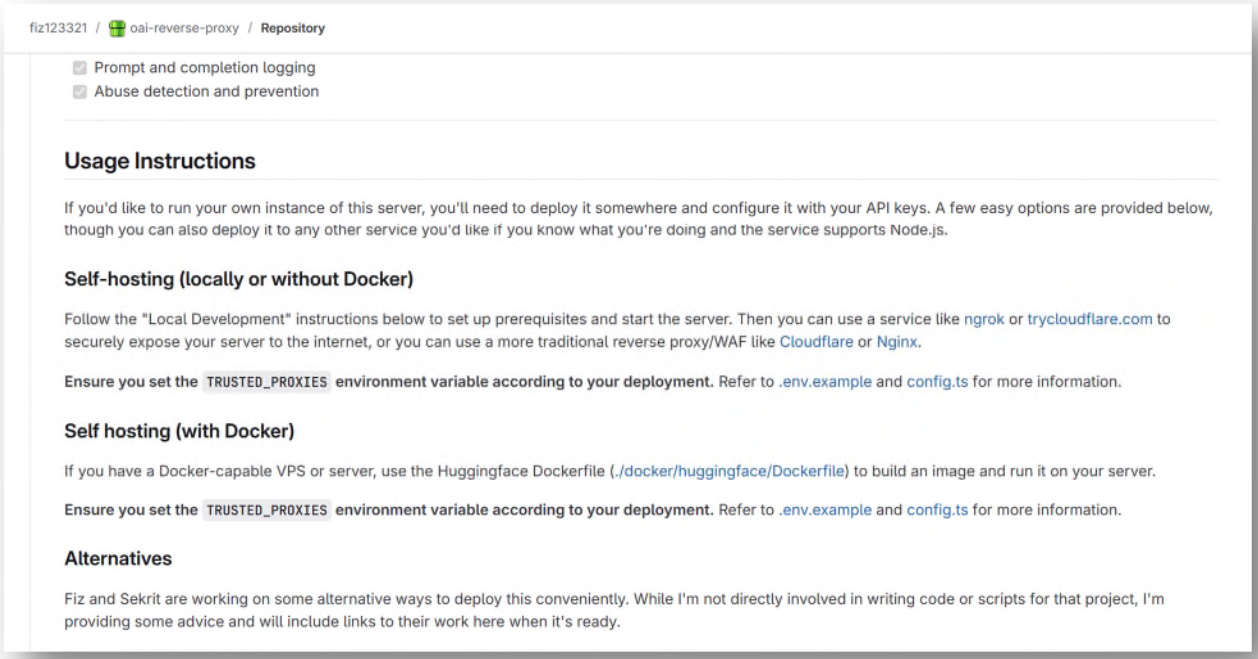


```
      "gemini-ultra": "0",
      "mistral-tiny": "0",
      "mistral-small": "0",
      "mistral-medium": "0",
      "mistral-large": "0",
      "aws-claude": "0",
      "aws-claude-opus": "0",
      "aws-mistral-tiny": "0",
      "aws-mistral-small": "0",
      "aws-mistral-medium": "0",
      "aws-mistral-large": "0",
      "gcp-claude": "0",
      "gcp-claude-opus": "0",
      "azure-turbo": "0",
      "azure-gpt4": "0",
      "azure-gpt4-32k": "0",
      "azure-gpt4-turbo": "0",
      "azure-gpt4o": "0",
      "azure-dall-e": "0",
      "azure-o1": "0",
      "azure-o1-mini": "0"
    },
    "quotaRefreshPeriod": "daily",
    "allowOpenAIToolUsage": "false",
    "tokensPunishmentFactor": "0"
  },
  "build": "[ci] 0c6ec32 (main@khanon/oai-reverse-proxy)"
}
```


DOE 3 is "Sekrit"

28. The individual described in Microsoft's complaint as DOE 3 is a person residing within the Republic of Austria and uses the alias "Sekrit". "Sekrit" is a person who appears to have been associated with the website "aitism.net" that was a part of the static infrastructure used to operate the Defendants scheme. Microsoft's continued investigation into "Sekrit" also identified the creation of a rentry page https://rentry.org/sekrit.

29. A true and correct screenshot from Yadegarnia's GitGud page where they mention collaboration with Sekrit on how to deploy the oai-reverse proxy tool is included below and attached hereto as **Exhibit 13**.



fiz123321 / oai-reverse-proxy / **Repository**

- Prompt and completion logging
- Abuse detection and prevention

Usage Instructions

If you'd like to run your own instance of this server, you'll need to deploy it somewhere and configure it with your API keys. A few easy options are provided below, though you can also deploy it to any other service you'd like if you know what you're doing and the service supports Node.js.

Self-hosting (locally or without Docker)

Follow the "Local Development" instructions below to set up prerequisites and start the server. Then you can use a service like ngrok or trycloudflare.com to securely expose your server to the internet, or you can use a more traditional reverse proxy/WAF like Cloudflare or Nginx.

Ensure you set the `TRUSTED_PROXIES` environment variable according to your deployment. Refer to .env.example and config.ts for more information.

Self hosting (with Docker)

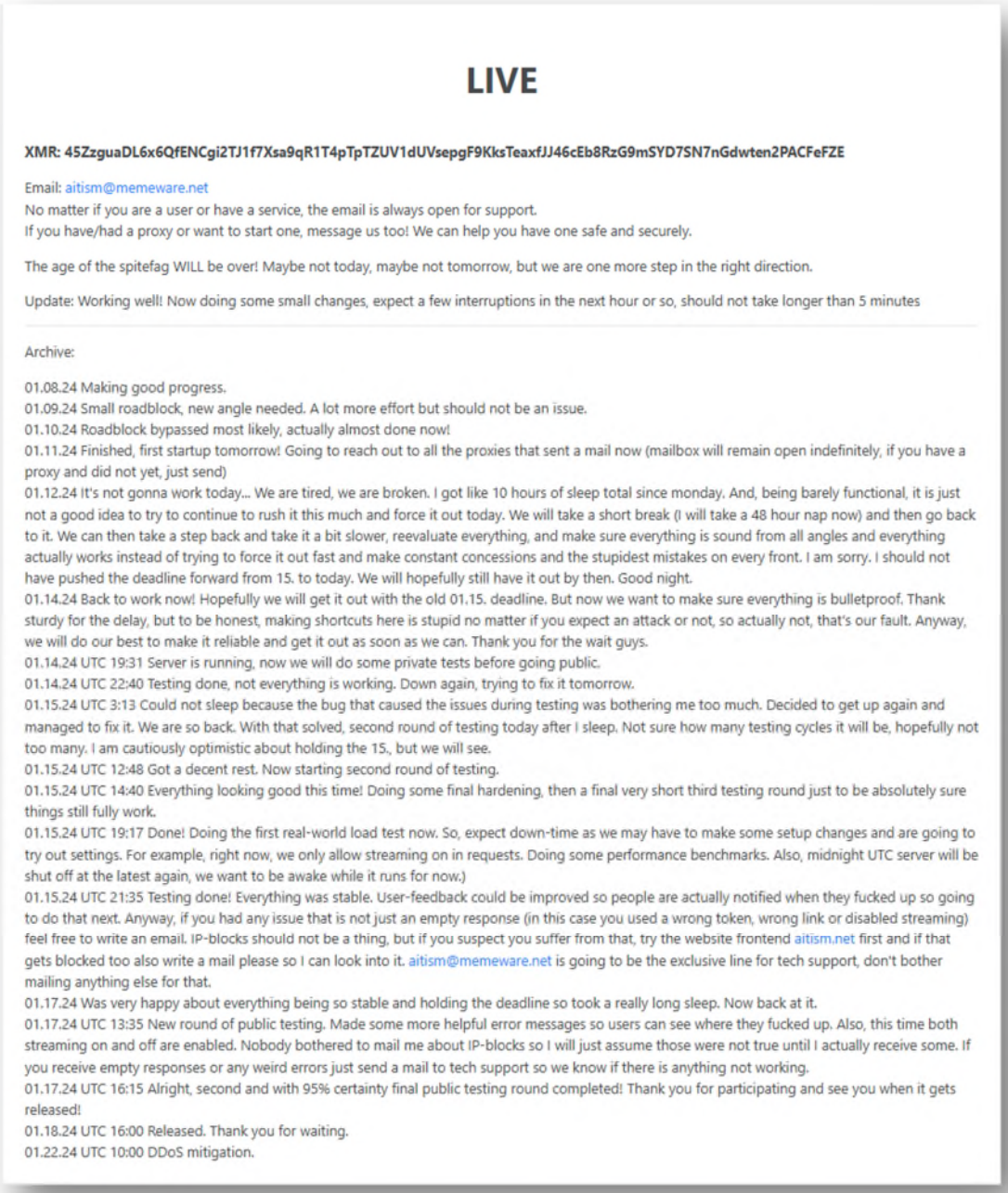
If you have a Docker-capable VPS or server, use the Huggingface Dockerfile (./docker/huggingface/Dockerfile) to build an image and run it on your server.

Ensure you set the `TRUSTED_PROXIES` environment variable according to your deployment. Refer to .env.example and config.ts for more information.

Alternatives

Fiz and Sekrit are working on some alternative ways to deploy this conveniently. While I'm not directly involved in writing code or scripts for that project, I'm providing some advice and will include links to their work here when it's ready.

30. A true and screenshot from Sekrit's Rentry page is included below and attached hereto as **Exhibit 14**.



LIVE

XMR: 45ZzguaDL6x6QfENCgi2TJ1f7Xsa9qR1T4pTpTZUV1dUVsepgF9KksTeaxfJJ46cEb8RzG9mSYD7SN7nGdwten2PACFeFZE

Email: aitism@memeware.net
No matter if you are a user or have a service, the email is always open for support.
If you have/had a proxy or want to start one, message us too! We can help you have one safe and securely.

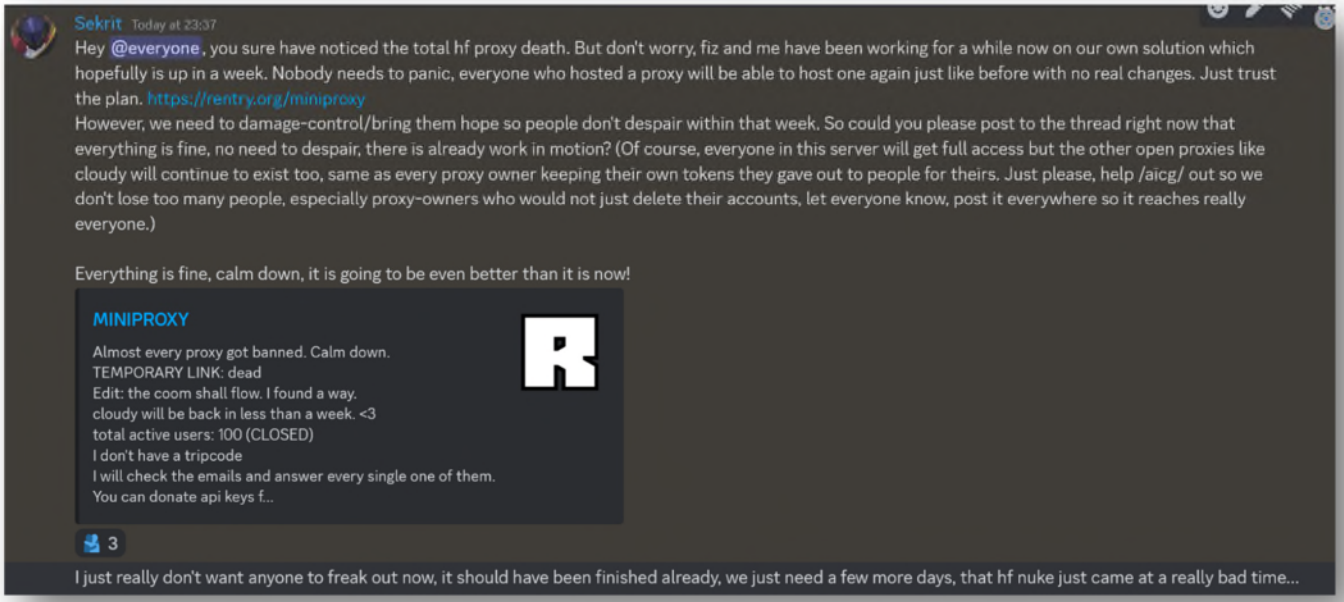
The age of the spitefag WILL be over! Maybe not today, maybe not tomorrow, but we are one more step in the right direction.

Update: Working well! Now doing some small changes, expect a few interruptions in the next hour or so, should not take longer than 5 minutes

Archive:

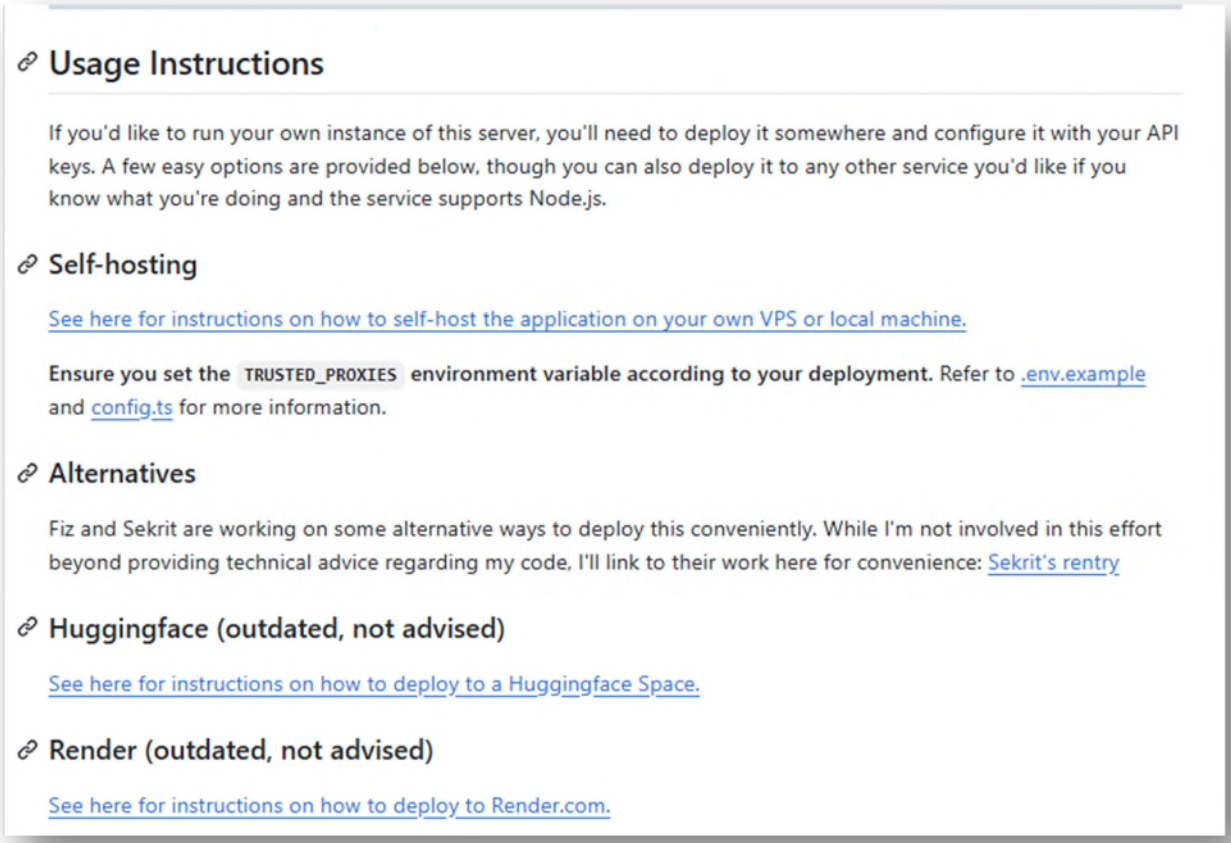
01.08.24 Making good progress.
01.09.24 Small roadblock, new angle needed. A lot more effort but should not be an issue.
01.10.24 Roadblock bypassed most likely, actually almost done now!
01.11.24 Finished, first startup tomorrow! Going to reach out to all the proxies that sent a mail now (mailbox will remain open indefinitely, if you have a proxy and did not yet, just send)
01.12.24 It's not gonna work today... We are tired, we are broken. I got like 10 hours of sleep total since monday. And, being barely functional, it is just not a good idea to try to continue to rush it this much and force it out today. We will take a short break (I will take a 48 hour nap now) and then go back to it. We can then take a step back and take it a bit slower, reevaluate everything, and make sure everything is sound from all angles and everything actually works instead of trying to force it out fast and make constant concessions and the stupidest mistakes on every front. I am sorry. I should not have pushed the deadline forward from 15. to today. We will hopefully still have it out by then. Good night.
01.14.24 Back to work now! Hopefully we will get it out with the old 01.15. deadline. But now we want to make sure everything is bulletproof. Thank sturdy for the delay, but to be honest, making shortcuts here is stupid no matter if you expect an attack or not, so actually not, that's our fault. Anyway, we will do our best to make it reliable and get it out as soon as we can. Thank you for the wait guys.
01.14.24 UTC 19:31 Server is running, now we will do some private tests before going public.
01.14.24 UTC 22:40 Testing done, not everything is working. Down again, trying to fix it tomorrow.
01.15.24 UTC 3:13 Could not sleep because the bug that caused the issues during testing was bothering me too much. Decided to get up again and managed to fix it. We are so back. With that solved, second round of testing today after I sleep. Not sure how many testing cycles it will be, hopefully not too many. I am cautiously optimistic about holding the 15., but we will see.
01.15.24 UTC 12:48 Got a decent rest. Now starting second round of testing.
01.15.24 UTC 14:40 Everything looking good this time! Doing some final hardening, then a final very short third testing round just to be absolutely sure things still fully work.
01.15.24 UTC 19:17 Done! Doing the first real-world load test now. So, expect down-time as we may have to make some setup changes and are going to try out settings. For example, right now, we only allow streaming on in requests. Doing some performance benchmarks. Also, midnight UTC server will be shut off at the latest again, we want to be awake while it runs for now.)
01.15.24 UTC 21:35 Testing done! Everything was stable. User-feedback could be improved so people are actually notified when they fucked up so going to do that next. Anyway, if you had any issue that is not just an empty response (in this case you used a wrong token, wrong link or disabled streaming) feel free to write an email. IP-blocks should not be a thing, but if you suspect you suffer from that, try the website frontend aitism.net first and if that gets blocked too also write a mail please so I can look into it. aitism@memeware.net is going to be the exclusive line for tech support, don't bother mailing anything else for that.
01.17.24 Was very happy about everything being so stable and holding the deadline so took a really long sleep. Now back at it.
01.17.24 UTC 13:35 New round of public testing. Made some more helpful error messages so users can see where they fucked up. Also, this time both streaming on and off are enabled. Nobody bothered to mail me about IP-blocks so I will just assume those were not true until I actually receive some. If you receive empty responses or any weird errors just send a mail to tech support so we know if there is anything not working.
01.17.24 UTC 16:15 Alright, second and with 95% certainty final public testing round completed! Thank you for participating and see you when it gets released!
01.18.24 UTC 16:00 Released. Thank you for waiting.
01.22.24 UTC 10:00 DDoS mitigation.

31. A true and screenshot from a 4chan post discussing Sekrit's collaboration with Yadegarnia is attached hereto as **Exhibit 15**.



Defendant Ricky Yuen

32. Microsoft's continued investigation into the Azure Abuse Enterprise identified another member of the Enterprise named Ricky Yuen, aka "CG-Dot", who appears to reside in the Hong Kong Special Administrative Region of the People's Republic of China. Yuen is a contributor to the oai-reverse-proxy source code initially authored by "Khannon" and has adapted that code to enable abuse of Google's Cloud Platform ("GCP"). Yuen's initial commit to the oai-reverse-proxy code occurred on June 29th, 2024, where they implemented GCP Claude support to the tool. A true and correct compilation of screenshots taken public GitHub repository showing Yuen's connection to the Azure Abuse Enterprise are included below and attached as **Exhibit 16**.



Usage Instructions

If you'd like to run your own instance of this server, you'll need to deploy it somewhere and configure it with your API keys. A few easy options are provided below, though you can also deploy it to any other service you'd like if you know what you're doing and the service supports Node.js.

Self-hosting

See here for instructions on how to self-host the application on your own VPS or local machine.

Ensure you set the `TRUSTED_PROXIES` environment variable according to your deployment. Refer to .env.example and config.ts for more information.

Alternatives

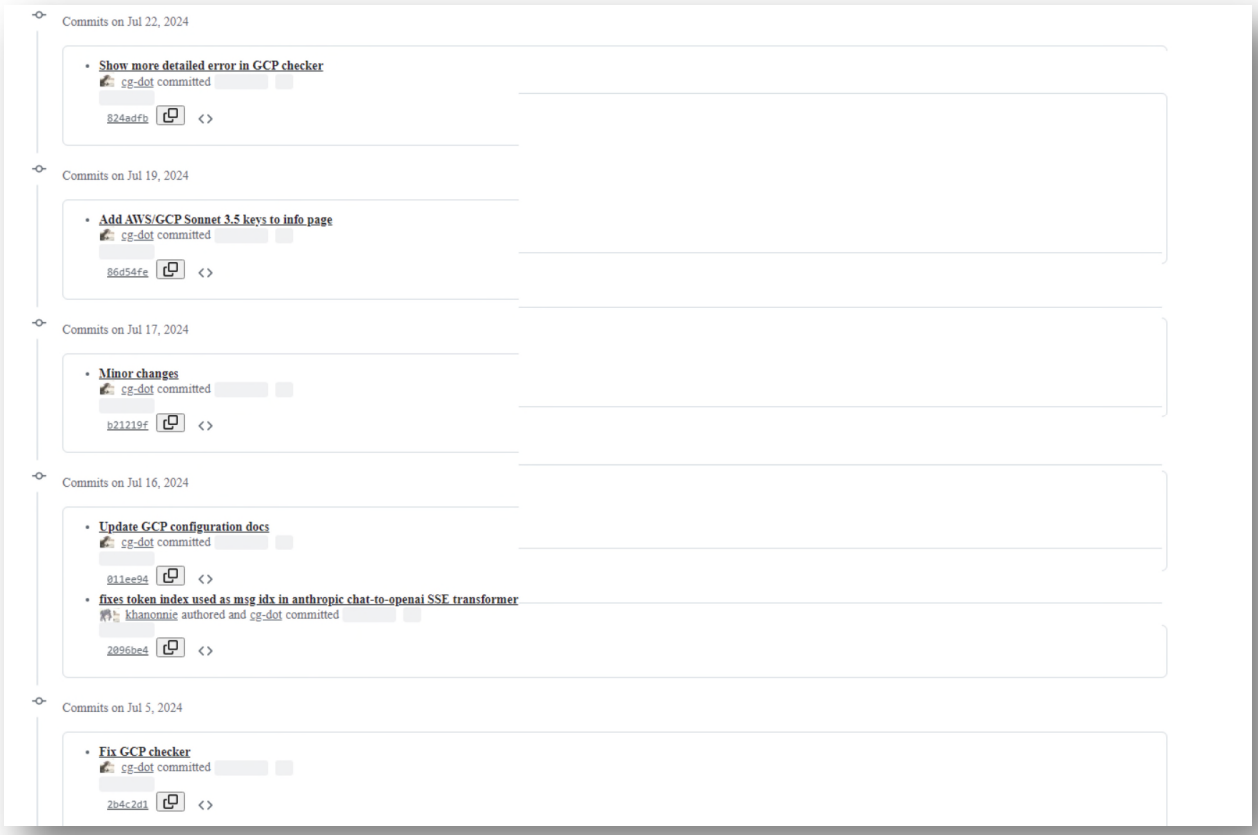
Fiz and Sekrit are working on some alternative ways to deploy this conveniently. While I'm not involved in this effort beyond providing technical advice regarding my code, I'll link to their work here for convenience: Sekrit's rentry

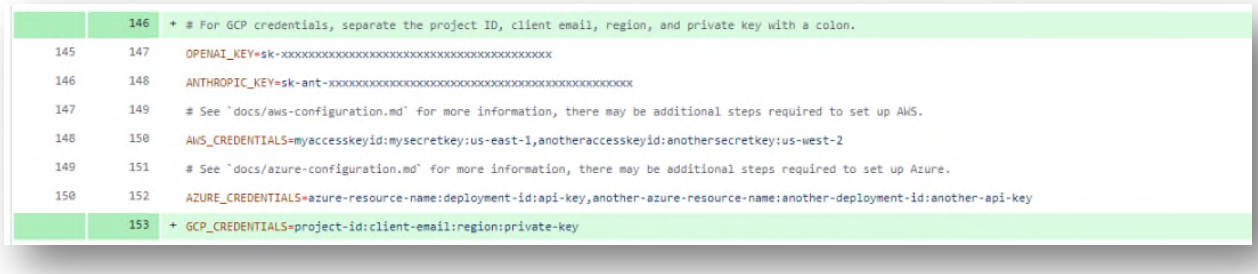
Huggingface (outdated, not advised)

See here for instructions on how to deploy to a Huggingface Space.

Render (outdated, not advised)

See here for instructions on how to deploy to Render.com.



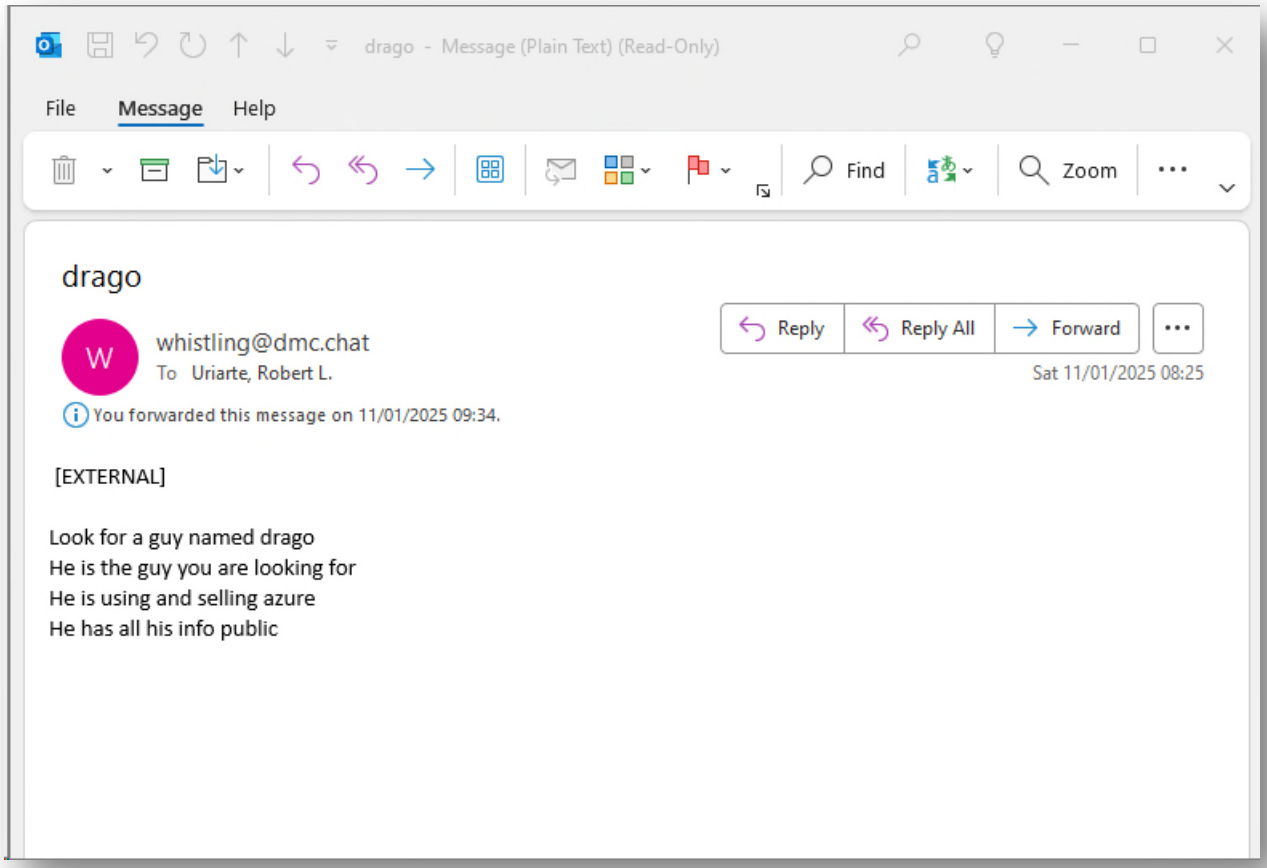


Defendant Alan Krysiak

33. Microsoft's continued investigation into the Azure Abuse Enterprise identified another member of the Enterprise named Alan Krysiak, aka "Drago." Krysiak appears to reside in the United Kingdom and has used proxy domains and stolen customer credentials in order to provide himself and others with unauthorized access to the Azure OpenAI Service. Krysiak

forkedthe oai-reverse-proxy source code initially authored by “Khannon” and provided it on their own personal Gitgud page https://gitgud.io/Drago/oai-reverse-proxy.

34. A compilation of screenshots of emails and webpages showing Krysiak’s connection to the Azure Abuse Enterprise are included below and attached as **Exhibit 17**.



Subject: the guy you are looking for - azure

https://discord.gg/scylla-charybdis This is the discord. They are selling access to azure for over 100 dollars. The old guys you are trying to sue don't even sell anything. These guys do.
This is the site: https://scylla.wtf

This is the main guy(drago) discord id: 325722644060176385 Attached proof of them talking about how they steal keys.
Their illegal proxy has over 3500 users.
NOTE: they know that you guys are looking and they started hiding their proxy's main page. Consider a sinkhole.

Main proxy with 3500 users(main page hidden): https://charybdis.scylla.wtf

Stat page unhidden: https://charybdis.scylla.wtf/status (they forgot to hide this)

Other proxy(main page not hidden): https://unicorn.scylla.wtf

The more advanced proxy software these people use: https://gitgud.io/Drago/oai-reverse-proxy (also written by drago the main ring leader)
Other fork: https://gitgud.io/yae-miko/oai-reverse-proxy/ (written by another person known as asakuri the assistant leader)

Related proxy by another person known as asakuri in the same discord available in the scylla.wtf domain:
https://rentry.org/GuujiYaeProxy
https:// guujiyae.me/

Note: they are lying about the keys being donated. These people are stealing the keys. This is just a straight up lie.

This is a real enterprise unlike the other group you are looking for. Sekrit, khanon, fiz are NOT the enterprise. These guys have potentially stolen millions of dollars from stolen azure and aws keys. Including dall-e stolen from upper tier customers with specific dall-e instances without any safety filters!
Link to the illegal azure proxy ran by drago and asakuri: https://shark-lost-brilliant-harbor.trycloudflare.com/

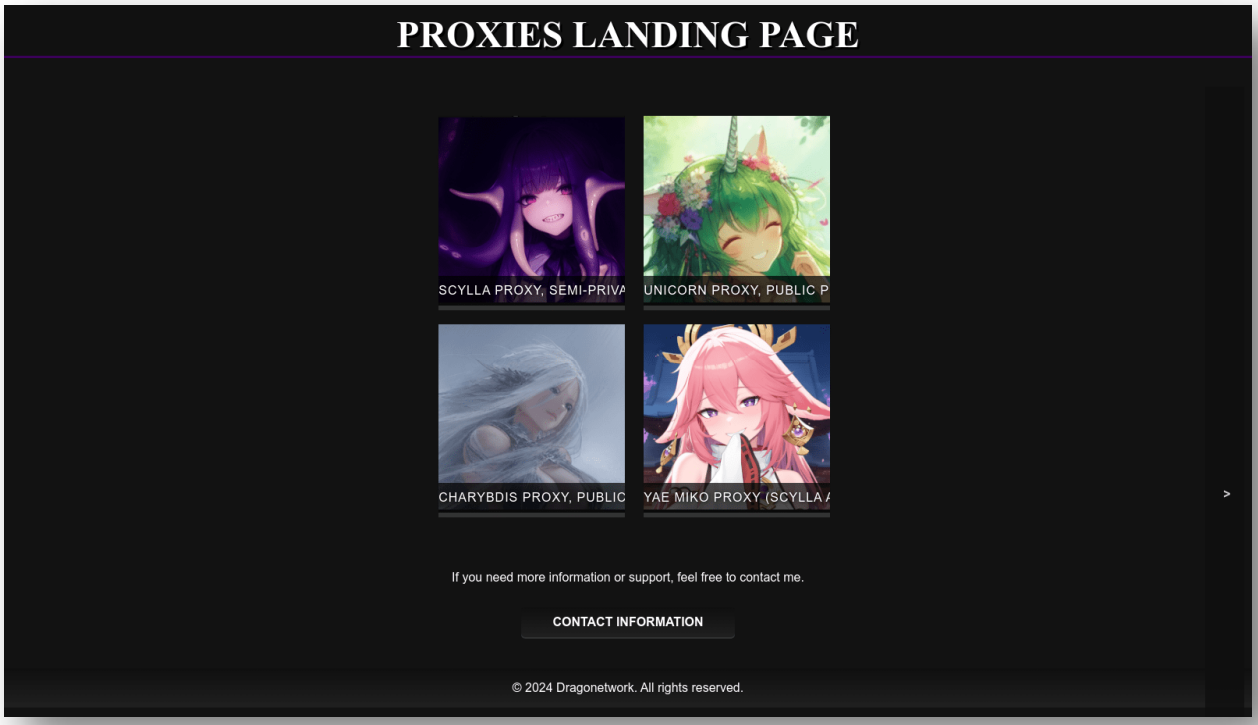
Attached screenshots in case they take it down.

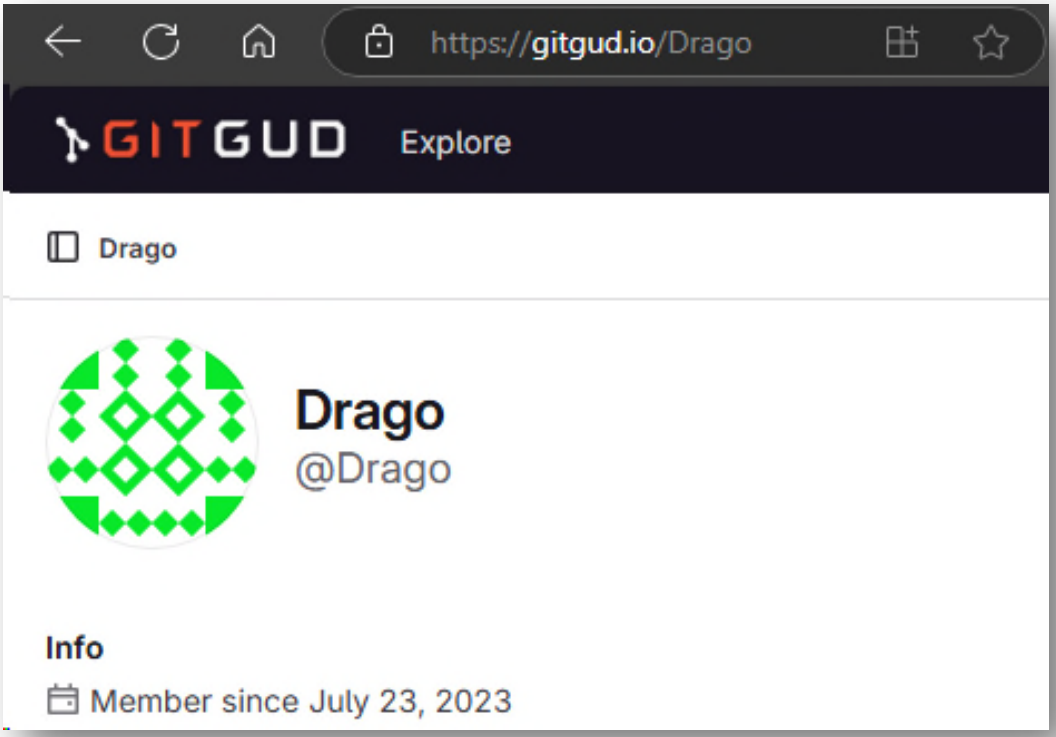
You can find a lot of proof and info in the provided Discord server.

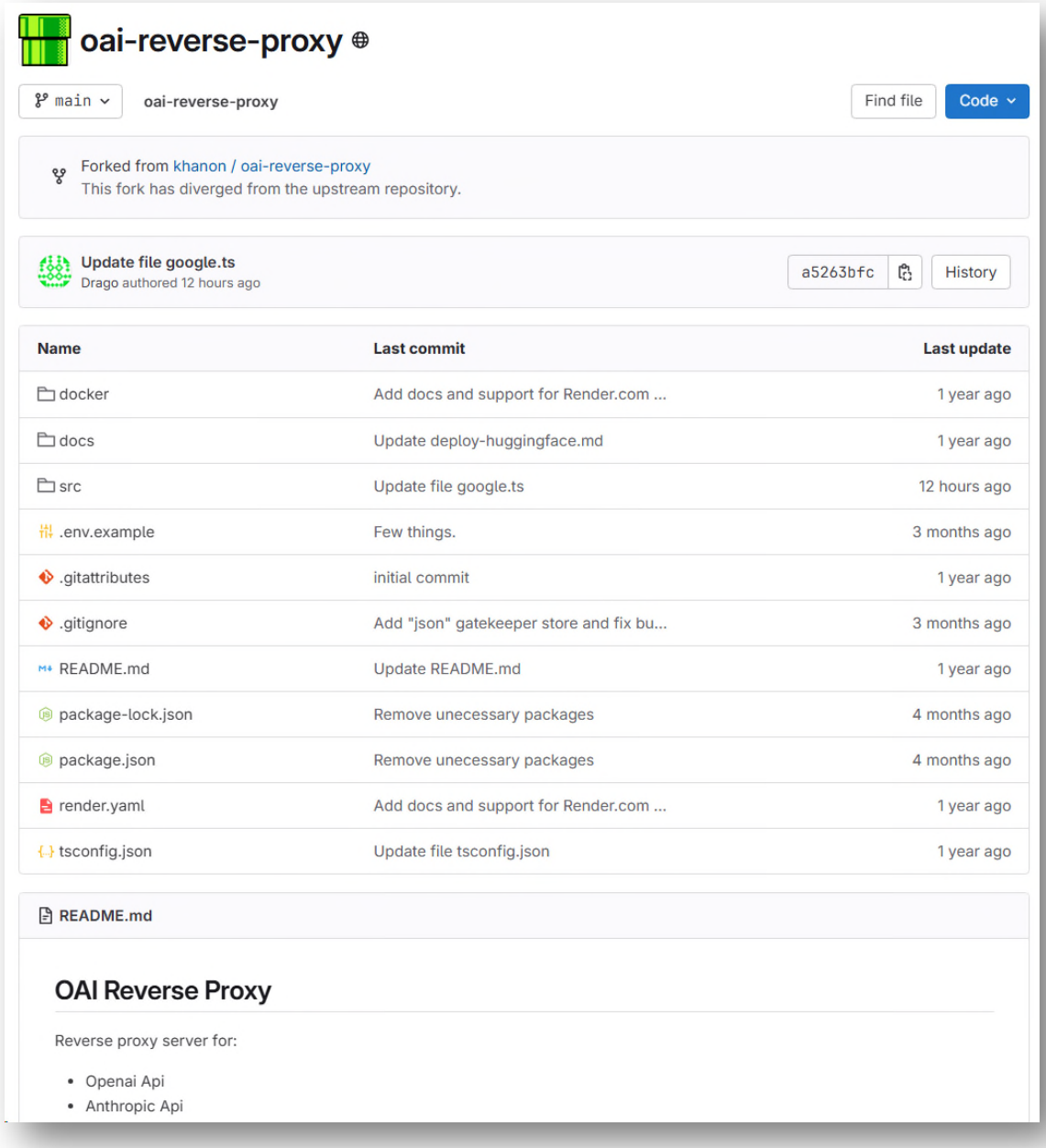
notable people:

dragOn3xt
Mr. Yae (asakuri)
rarestmeow

NOTE: these people are professionals. Consider restraining orders. I can provide you with more info if necessary.


PROXIES LANDING PAGE
SCYLLA PROXY, SEMI-PRIVA
UNICORN PROXY, PUBLIC P
CHARYBDIS PROXY, PUBLIC
YAE MIKO PROXY (SCYLLA
If you need more information or support, feel free to contact me.
CONTACT INFORMATION
© 2024 Dragonetwork. All rights reserved.


https://gitgud.io/Drago
GITGUD
Explore
Drago
Drago
@Drago
Info
Member since July 23, 2023



oai-reverse-proxy

main oai-reverse-proxy Find file Code

Forked from khanon / oai-reverse-proxy
This fork has diverged from the upstream repository.

Update file google.ts
Drago authored 12 hours ago a5263bfc History

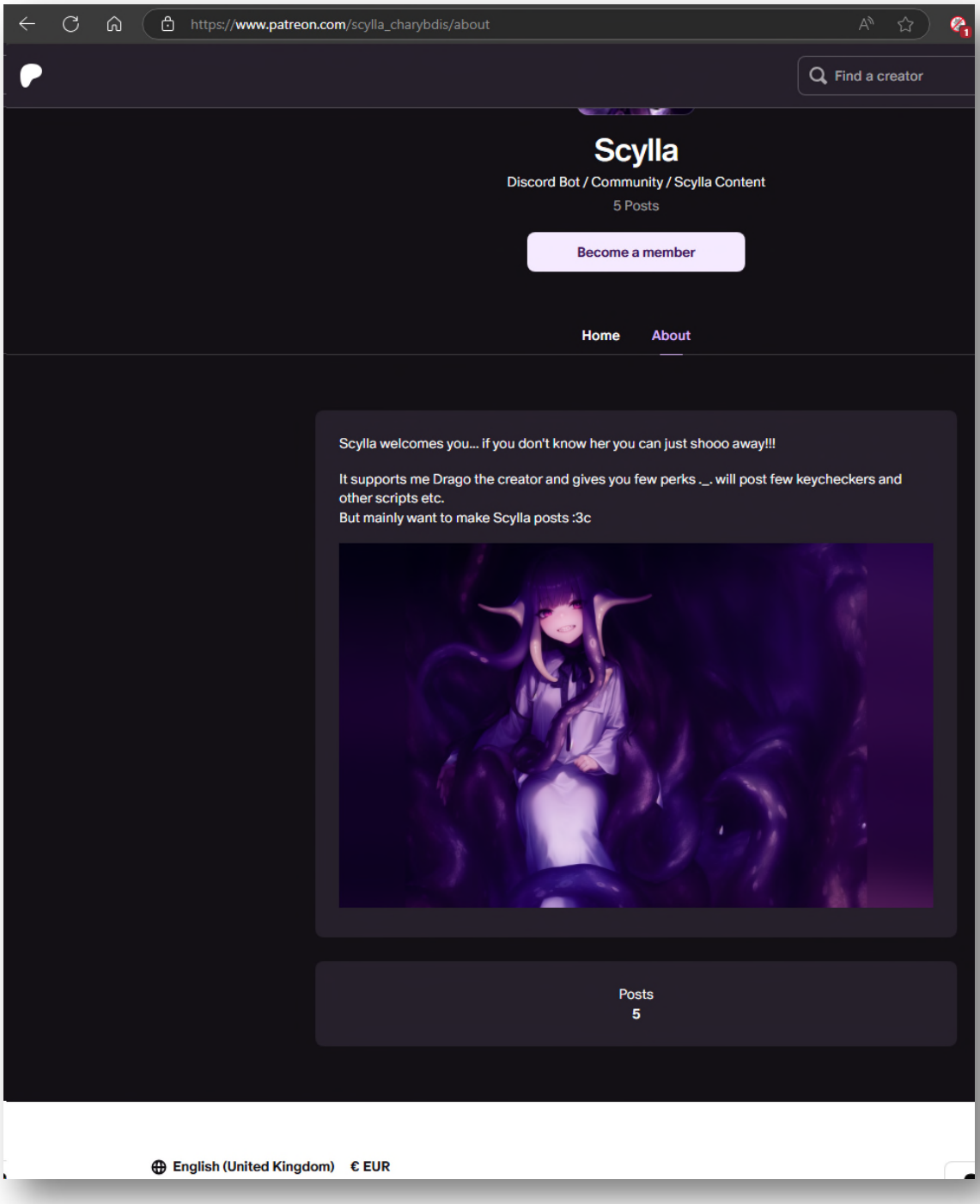
Name	Last commit	Last update
docker	Add docs and support for Render.com ...	1 year ago
docs	Update deploy-huggingface.md	1 year ago
src	Update file google.ts	12 hours ago
.env.example	Few things.	3 months ago
.gitattributes	initial commit	1 year ago
.gitignore	Add "json" gatekeeper store and fix bu...	3 months ago
README.md	Update README.md	1 year ago
package-lock.json	Remove unecessary packages	4 months ago
package.json	Remove unecessary packages	4 months ago
render.yaml	Add docs and support for Render.com ...	1 year ago
tsconfig.json	Update file tsconfig.json	1 year ago

README.md

OAI Reverse Proxy

Reverse proxy server for:

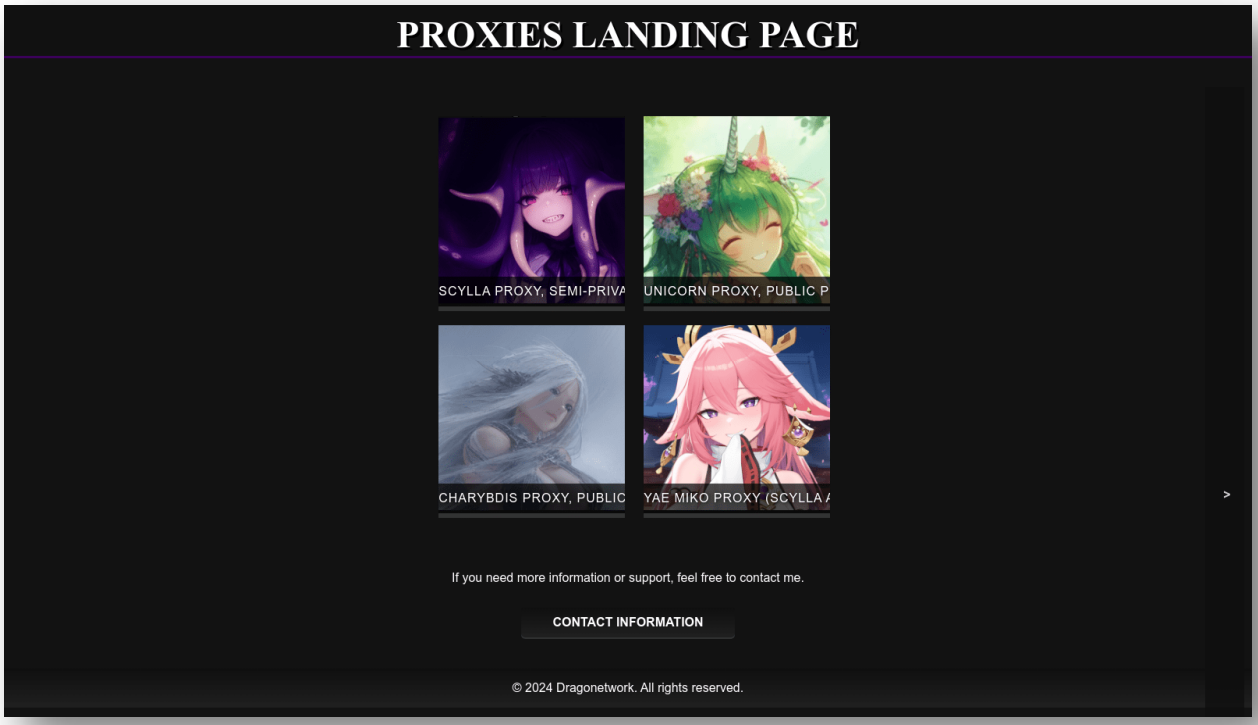
- Openai Api
- Anthropic Api



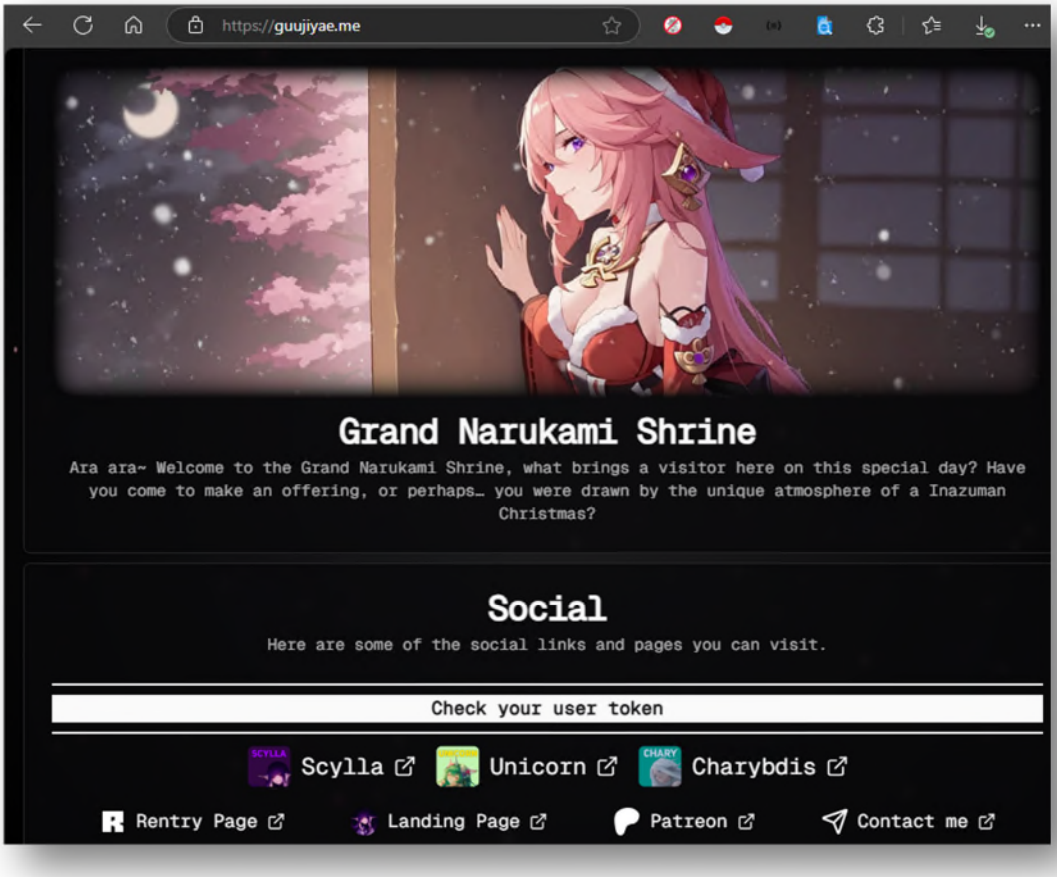
Defendant Phát Phùng Tấn aka ”Asakuri”

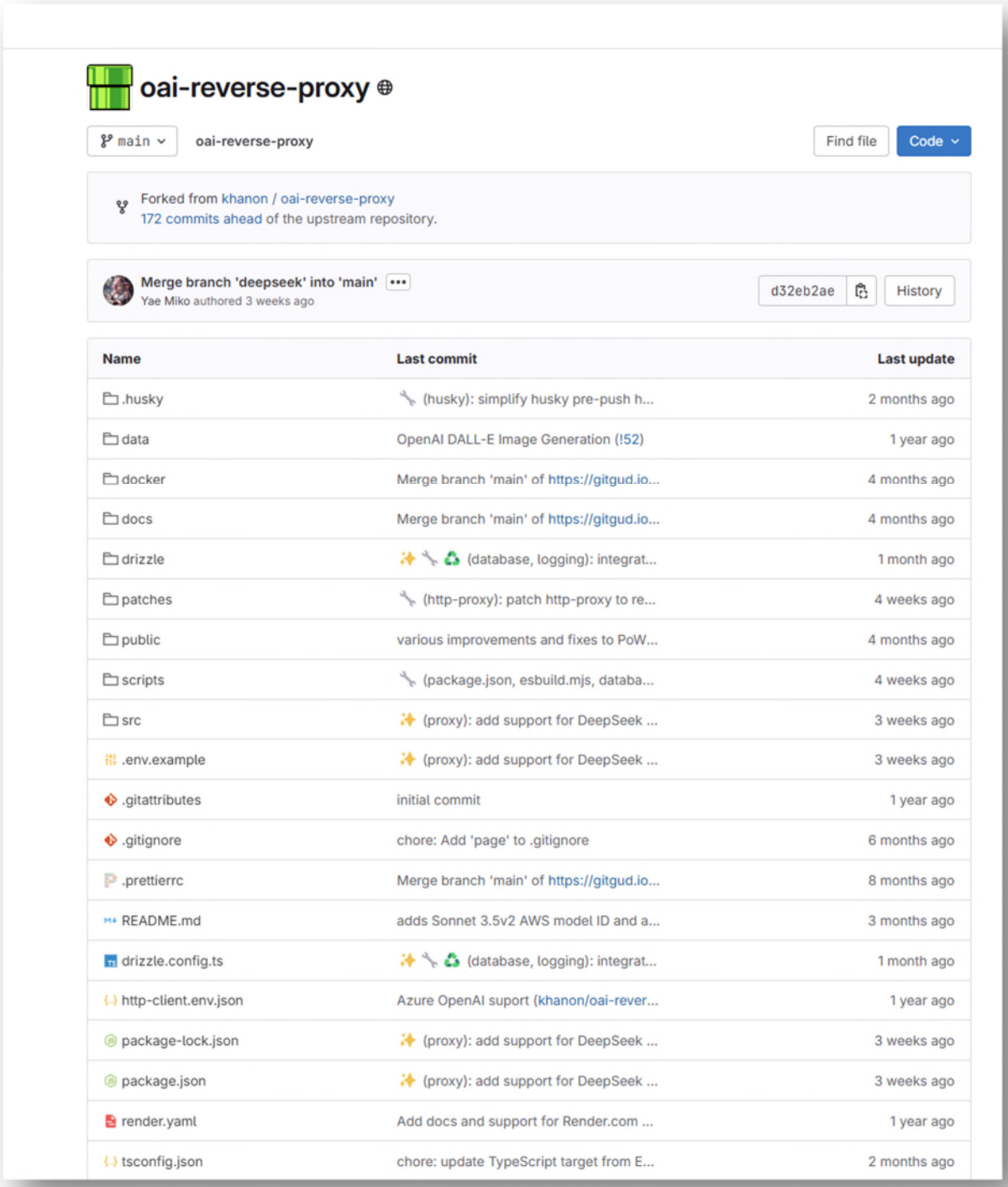
35. Microsoft’s continued investigation into the Azure Abuse Enterprise identified another member of the Enterprise named Phát Phùng Tấn aka ”Asakuri”. Tấn appears to reside in

Socialist Republic of Vietnam. Tấn has used proxy domains and stolen customer credentials in order to provide themselves and others with unauthorized access to the Azure OpenAI Service. Tấn proxy domains were hosted on one of Drago's main websites https://dragonetwork.pl. Additionally, Tấn forked[2] the oai-reverse-proxy source code initially authored by "Khannon" and provided it on their own personal gitgud page gitgud.io/yae-miko/oai-reverse-proxy. A true and correct compilation of screenshots showing Tấn's connection to the Azure Abuse Enterprise isincluded below and attached as **Exhibit 18.**



[22] In the context of computer programing, "forking" generally refers to making a copy of a source code repository (the one being forked) and starting a new branch of source code development.


https://guujiyae.me
Grand Narukami Shrine
Ara ara~ Welcome to the Grand Narukami Shrine, what brings a visitor here on this special day? Have you come to make an offering, or perhaps… you were drawn by the unique atmosphere of a Inazuman Christmas?
Social
Here are some of the social links and pages you can visit.
Check your user token
Scylla
Unicorn
Charybdis
Rentry Page
Landing Page
Patreon
Contact me



oai-reverse-proxy

main · oai-reverse-proxy · Find file · Code

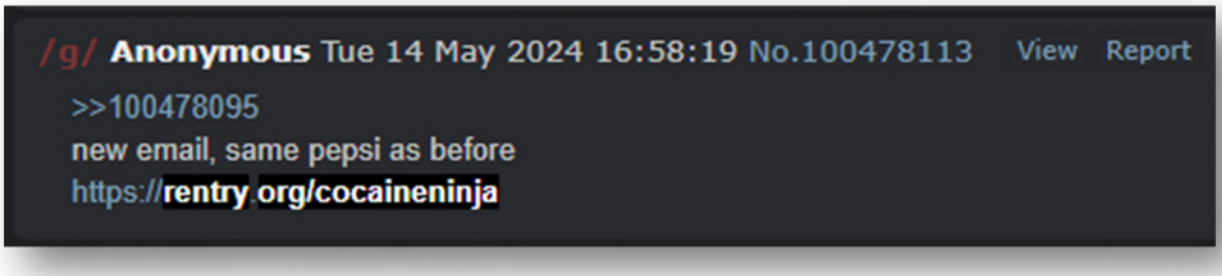
Forked from khanon / oai-reverse-proxy
172 commits ahead of the upstream repository.

Merge branch 'deepseek' into 'main'
Yae Miko authored 3 weeks ago · d32eb2ae · History

Name	Last commit	Last update
.husky	(husky): simplify husky pre-push h...	2 months ago
data	OpenAI DALL-E Image Generation (!52)	1 year ago
docker	Merge branch 'main' of https://gitgud.io...	4 months ago
docs	Merge branch 'main' of https://gitgud.io...	4 months ago
drizzle	(database, logging): integrat...	1 month ago
patches	(http-proxy): patch http-proxy to re...	4 weeks ago
public	various improvements and fixes to PoW...	4 months ago
scripts	(package.json, esbuild.mjs, databa...	4 weeks ago
src	(proxy): add support for DeepSeek ...	3 weeks ago
.env.example	(proxy): add support for DeepSeek ...	3 weeks ago
.gitattributes	initial commit	1 year ago
.gitignore	chore: Add 'page' to .gitignore	6 months ago
.prettierrc	Merge branch 'main' of https://gitgud.io...	8 months ago
README.md	adds Sonnet 3.5v2 AWS model ID and a...	3 months ago
drizzle.config.ts	(database, logging): integrat...	1 month ago
http-client.env.json	Azure OpenAI suport (khanon/oai-rever...	1 year ago
package-lock.json	(proxy): add support for DeepSeek ...	3 weeks ago
package.json	(proxy): add support for DeepSeek ...	3 weeks ago
render.yaml	Add docs and support for Render.com ...	1 year ago
tsconfig.json	chore: update TypeScript target from E...	2 months ago

Other Members of the Azure Abuse Enterprise

36. Microsoft's continued investigation into the Azure Abuse Enterprise identified another member of the Enterprise who uses the alias "Pepsi." Pepsi appears to reside in the United States and has used proxy domains and stolen customer credentials in order to provide themselves and others with unauthorized access to the Azure OpenAI Service. Additionally, Microsoft identified a rentry page https://rentry.org/cocaineninja and a GitHub repository https://github.com/dietpesigirl which appeared to be controlled by "Pepsi". Microsoft's analysis from reviewing discovery data identified that Pepsi was recently visiting the "aitism.net" website from January 9th, through January 26th, 2025. This website was a part of the static infrastructure used to operate the Defendants scheme. A true and correct compilation of screenshots of evidence showing Pepsi's connection to the Azure Abuse Enterprise is included below and attached as **Exhibit 19**.



the claude issues are happening to everyone on every proxy (aws issue)

thank you fiz! <3 <3

thank you openttd enjoyer <3 <3

proxy info

closed

gpt/claude/gemini/mistral/dalle3
vision on for gpt and gemini

proxy: https://fuji-seniors-nor-namely.trycloudflare.com/

email: dietpepsigirl@proton.me

i accept aws key donations

please don't token share

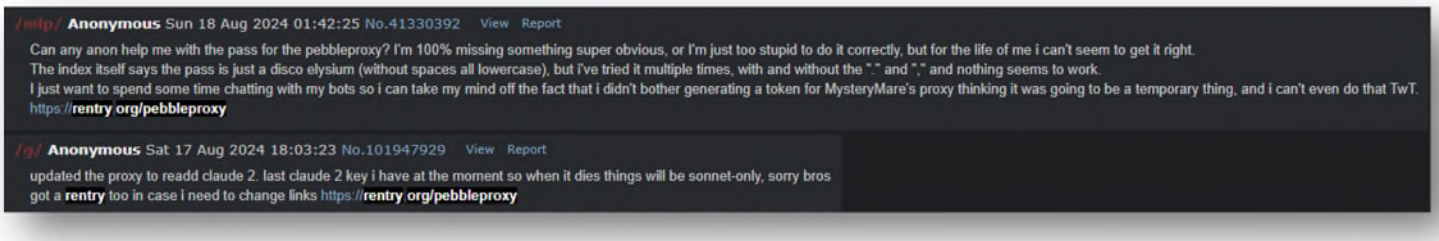
going through emails (143 unread)

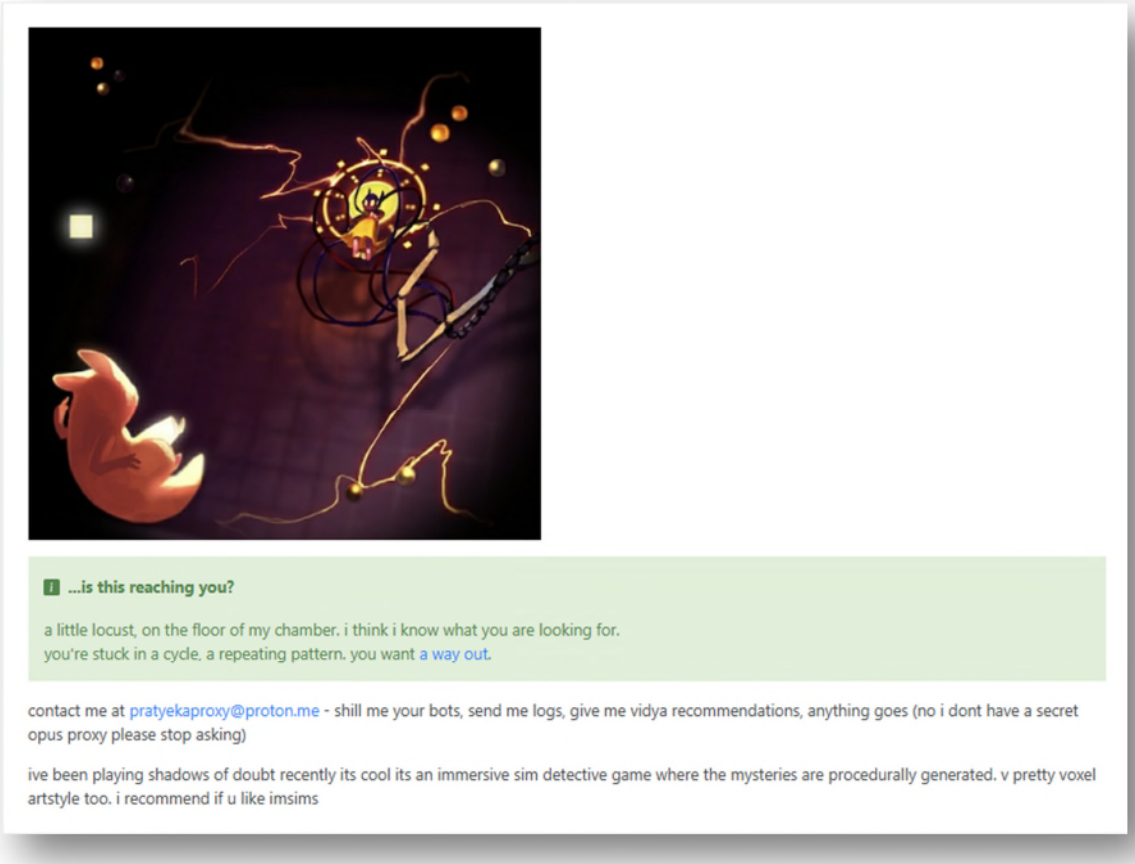
email: proxy1@cocaine.ninja
https://huggingface.co/spaces/cocaine-ninja/1
gpt-4 / gpt-4-turbo / gpt-4-omni / aws claude-3-sonnet
key donated / sources accepted

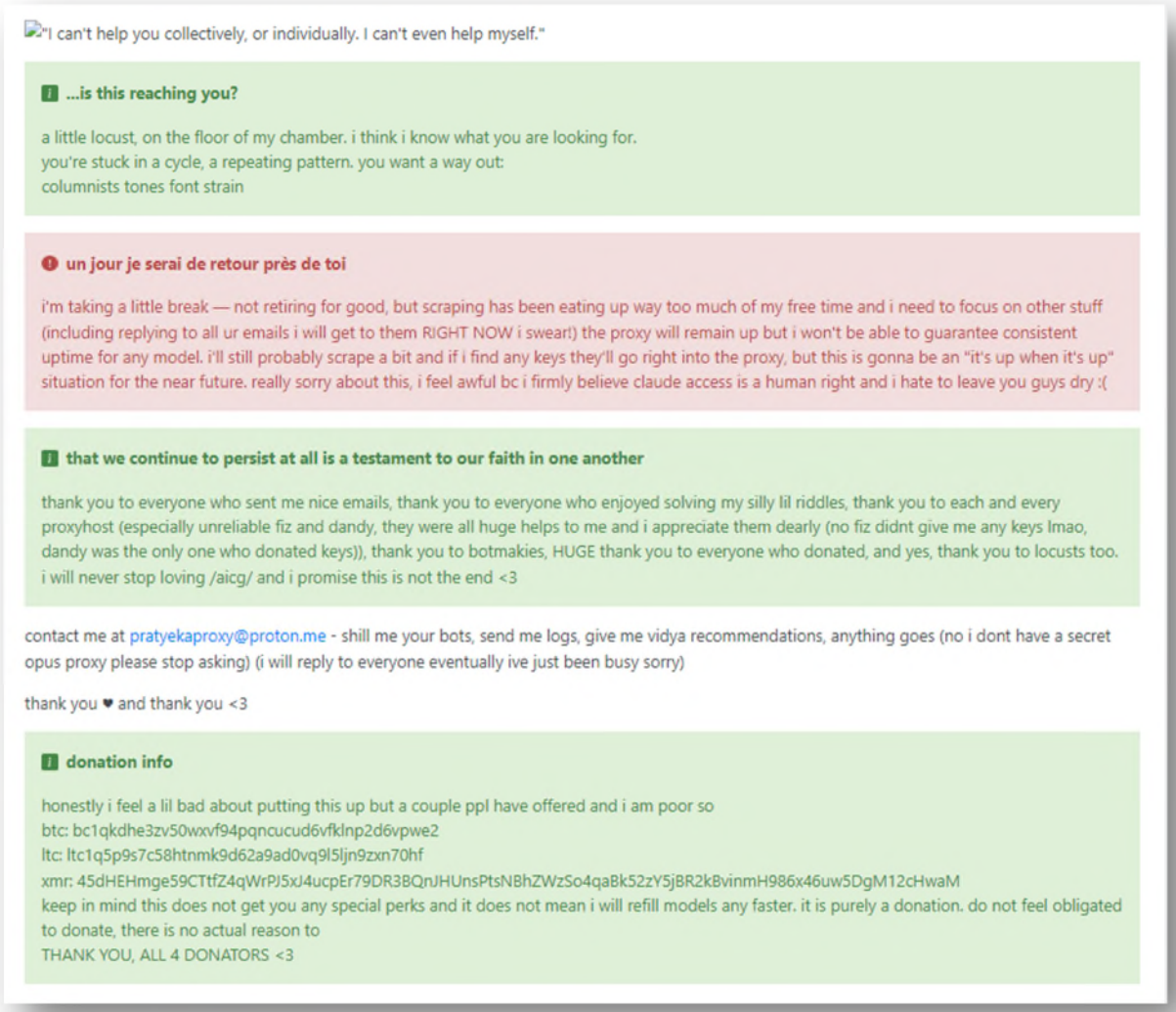
pls DO NOT send anything to https://rentry.org/dietproxy.

i am the original (see bio): https://github.com/dietpepsigirl

37. Microsoft's continued investigation into the Azure Abuse Enterprise identified another member of the Enterprise who uses the alias "Pebble." Pebble appears to reside in the United States and has used proxy domains and stolen customer credentials in order to provide themselves and others with unauthorized access to the Azure OpenAI Service. A true and correct compliation of screenshots of evidence showing Pebble's connection to the Azure Abuse Enterprise is included below and attached as **Exhibit 20**.







DOES 4-7 are "Dazz," "Jorge," "Jawajawaable," and "1pghlgm"

38. Microsoft's continued investigation into the Azure Abuse Enterprise identified other members of the Enterprise as end users who use the aliases "dazz", "Jorge", "jawajawaable", "1phlgm" (Does 4-7). These individuals except for "Jorge" appear to reside outside the United States and have used infrastructure and stolen credentials provided by the Azure Abuse Enterprise to gain unauthorized access to the Azure OpenAI Service. Based off my investigation of the end users "dazz", Jorge", "jawajawaable", and "1phlgm" they appear to utilize the infrastructure provided by DOEs 1-3 to create images that targeted celebrities that were in violation of our terms of use.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 26th day of February 2025.

Maurice Mason