Context

We suspect that the fediverse is being leveraged for a C&C style DDoS attack against arbitrary domains.
See the original thread (https://hachyderm.io/@dwarf@borg.social/109449246766819991)
Suspected malicious domains

```
*.activitypub-troll.cf
*.misskey-forkbomb.cf
*.repl.co
```

Resource on **blocking server domains**

(https://medium.com/@theghostoftomjoad/how-to-block-server-domains-in-mastodon-899b24f8fb6e)

Observations and Actions

1. Accounts created on **hachyderm.io** (http://hachyderm.io)

Bota
getchannels
Core
vinylteque

2. Sidekiq observed queue

```
To: https://2jb3chx5h.activitypub-troll.cf/inbox
{
    "@context":"https://www.w3.org/ns/activitystreams",
    "id":"https://hachyderm.io/users/vinylteque#delete",
    "type":"Delete",
    "actor":"https://hachyderm.io/users/vinylteque",
    "to":["https://www.w3.org/ns/activitystreams#Public"],
    "object":"https://hachyderm.io/users/vinylteque",
    "signature":{
        "type":"RsaSignature2017",
        "creator":"https://hachyderm.io/users/vinylteque#main-key",
        "created":"2022-12-03T18:28:09Z",
        "signatureValue":"redacted"
    }
}
109406507175403490
```

The URL above is random.

3. A user report came in

A user report came in from @Ghryphen at approximately 2:45 AM, indicating possible spam. I don't know where the user spotted the spam, it may make sense to reach out and ask.
Tani's guess is the message was seen in the federation stream.

4. Server defederated administratively

`activitypub-troll.cf` and all subdomains are defederated by hachyderm.
It appears that the pull queue still attempts to work through the pull queue.

5. New account creation administratevily disabled by hachyderm

6. Bot Accounts deleted

When the bots are deleted, they cause a significant quantity of traffic.

7. Main attack

Speculation:

1. A set of bot accounts were created on hachyderm.
2. An custom attack server was created on *.activitypub-troll.cf
3. Attack server placed behind cloudflare
4. Wildcard DNS was set to point to this attack server
5. Bot accounts would follow accounts on random *.activitypub-troll.cf servers
6. Messages pulled in are infinitely recursive, filling up database and queues
7. Attack server shut down
8. bot accounts deleted
9. queues fill up again with retries as cloudflare returns 521
10. failed messages end up on retry queue

Possible actions

Let it run its course for one week

The load isn't high on our servers, and the failure timeout increases exponentially.

Purge all records in the redis PULL queue matching the target URL

We would likely have to write some code to do this, also risky since it is a destructive action.

Blackhole DNS through dnsmaq or resolv.conf

Easy to implement, need to validate ruby is respecting the settings.
Since we split the queues from the web server, we might be able to just redirect all traffic to these addresses to 127.0.0.1

Source code from attacker

Attacker hosted the source of the attack.
Reach out if you want to review