Who I am

- “ketominer”
  - electronics
  - (low level) code
  - networks
  - systems
  - putting weird things together and making them work
- Doing the **nodl box**, **nodl hosted services** and **host4coins**

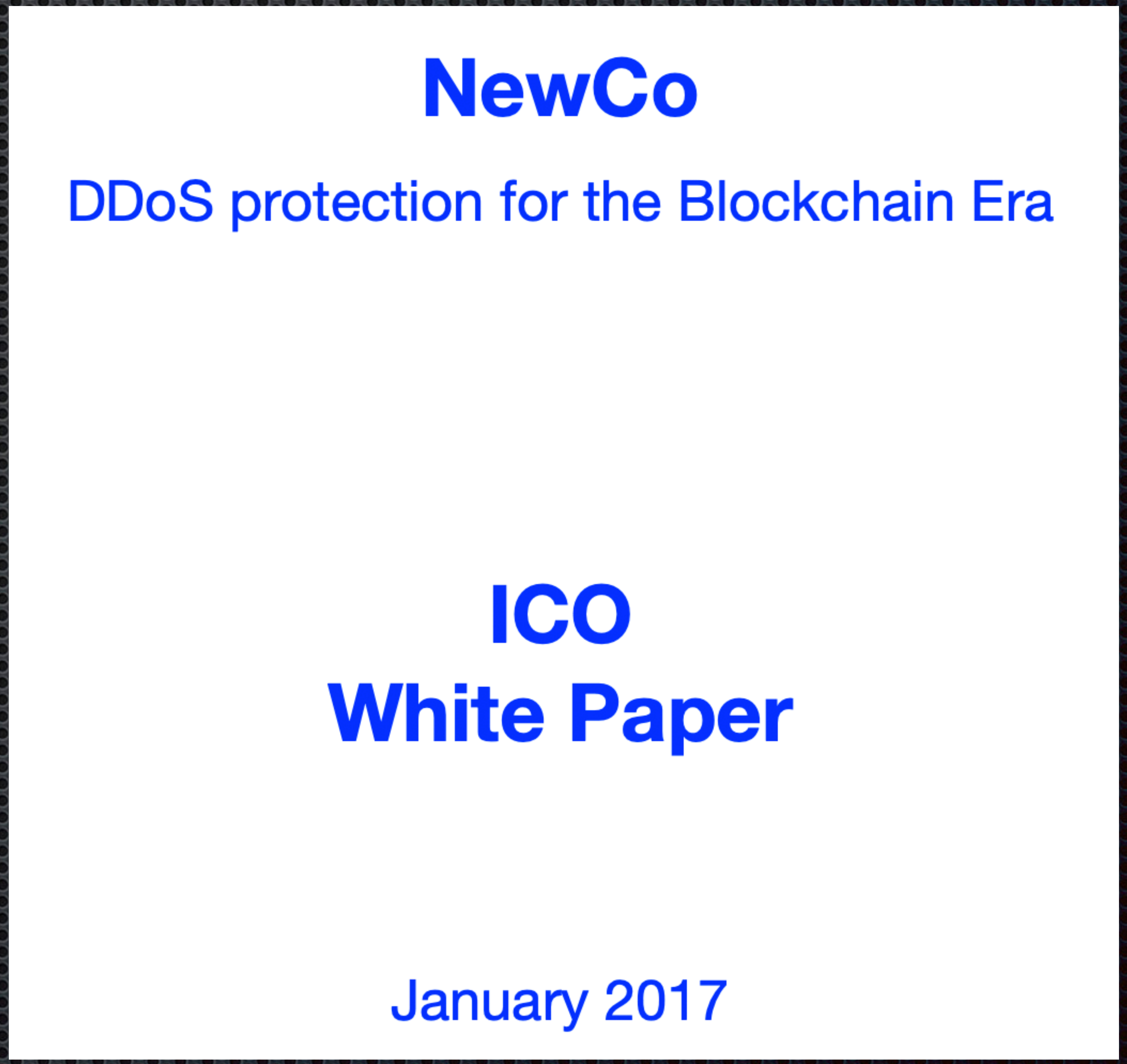
twitter/telegram/keybase: @ketominer

```
GPG: B5F6 FEBB 4D88 0398 7C60
     3E3F EAD1 75FA A6C4 B7DE
```

ketominer@nodl.it

How I made an ICO

TCConf 2019



NewCo

DDoS protection for the Blockchain Era

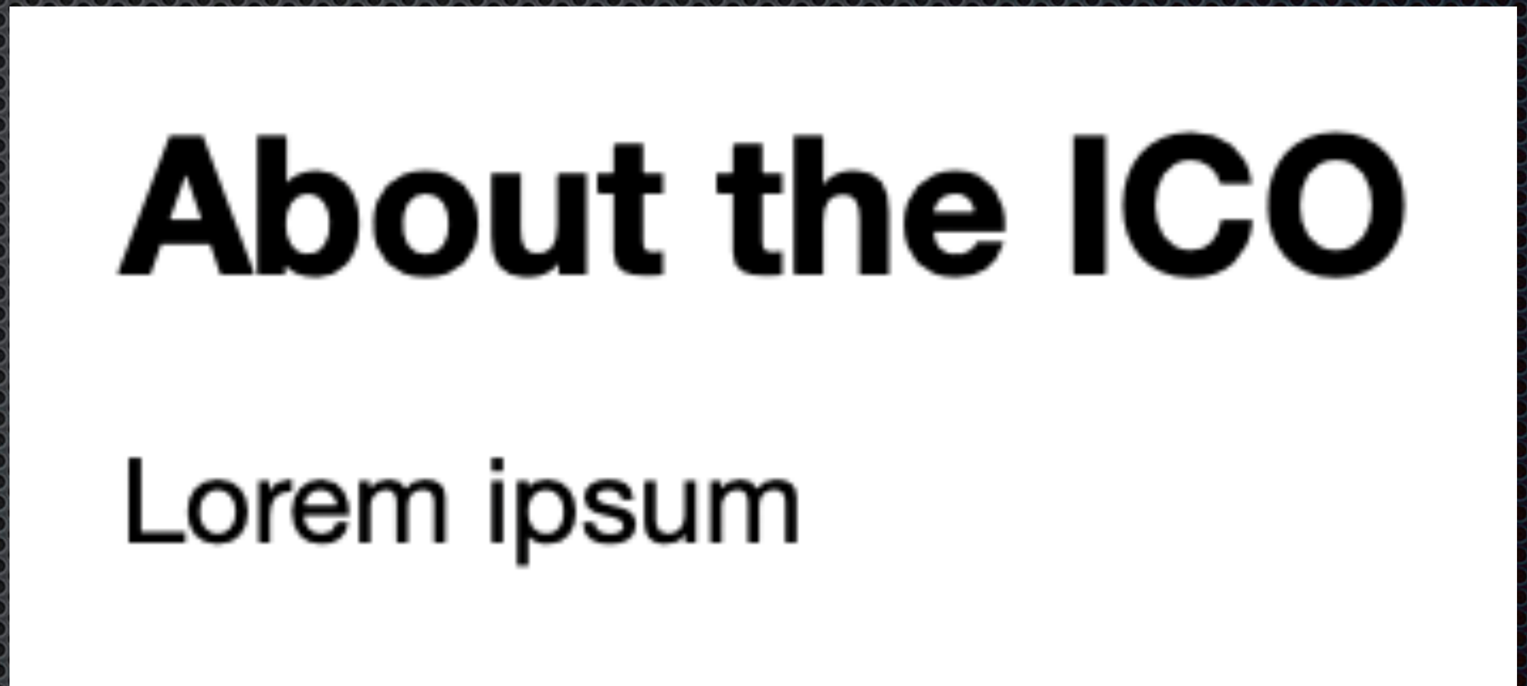
ICO
White Paper

January 2017

actual screenshot from the WP

How I almost made an ICO

TCConf 2019



About the ICO

Lorem ipsum

also actual screenshot from the WP

How I almost made an ICO

A technical talk about opportunism, money and large scale networking.

TCConf 2019

Fasten your seatbelts

What is a DoS attack

- Preventing legitimate users from using a service by overloading it

- Usually using “elaborate” techniques to overload the CPU/RAM
  - not just lots of requests but specially crafted requests
  - examples: slowloris, UDP flood, SYN flood, ping of death, …

- Usually doesn’t require many requests, hence not Distributed

What is a DDoS attack

- Preventing legitimate users from using a service by overloading it

- Usually using dumb techniques to overload the incoming pipes of the network
  - using a botnet
  - using a reflection and amplification attack
  - or both

- Can optionally use the “elaborate” techniques from a regular DoS attack (but why bother)

What are we trying to protect

- Nowadays, many (most ?) things are done over HTTP(S)
- (Un)fortunately
- Even DNS (DoH) - but not quite yet
- Let’s focus on DNS and HTTPS

How to protect against DoS (1/2)

- Buy a next-gen ™ firewall (lol) - please don’t
- Deny by default
- Use simple firewall rules (ex. pass in proto tcp flags S/SA synproxy state*)
- Use smart rate limiting rules (ex. pass in on egress proto tcp to $web_server port 443 flags S/SA keep state max-src-conn 100, max-src-conn-rate 15/5, overload <abusive_hosts> flush**)

*PF will generate strong Initial Sequence Numbers (ISNs) for packets matching this rule - bonus it obfuscates client OS

**Limits the maximum number of connections per source to 100. Rate limits the number of connections to 15 in a 5 second span. Puts the IP address of any host that breaks these limits into the <abusive_hosts> table. For any offending IP addresses, flush any states created by this rule.

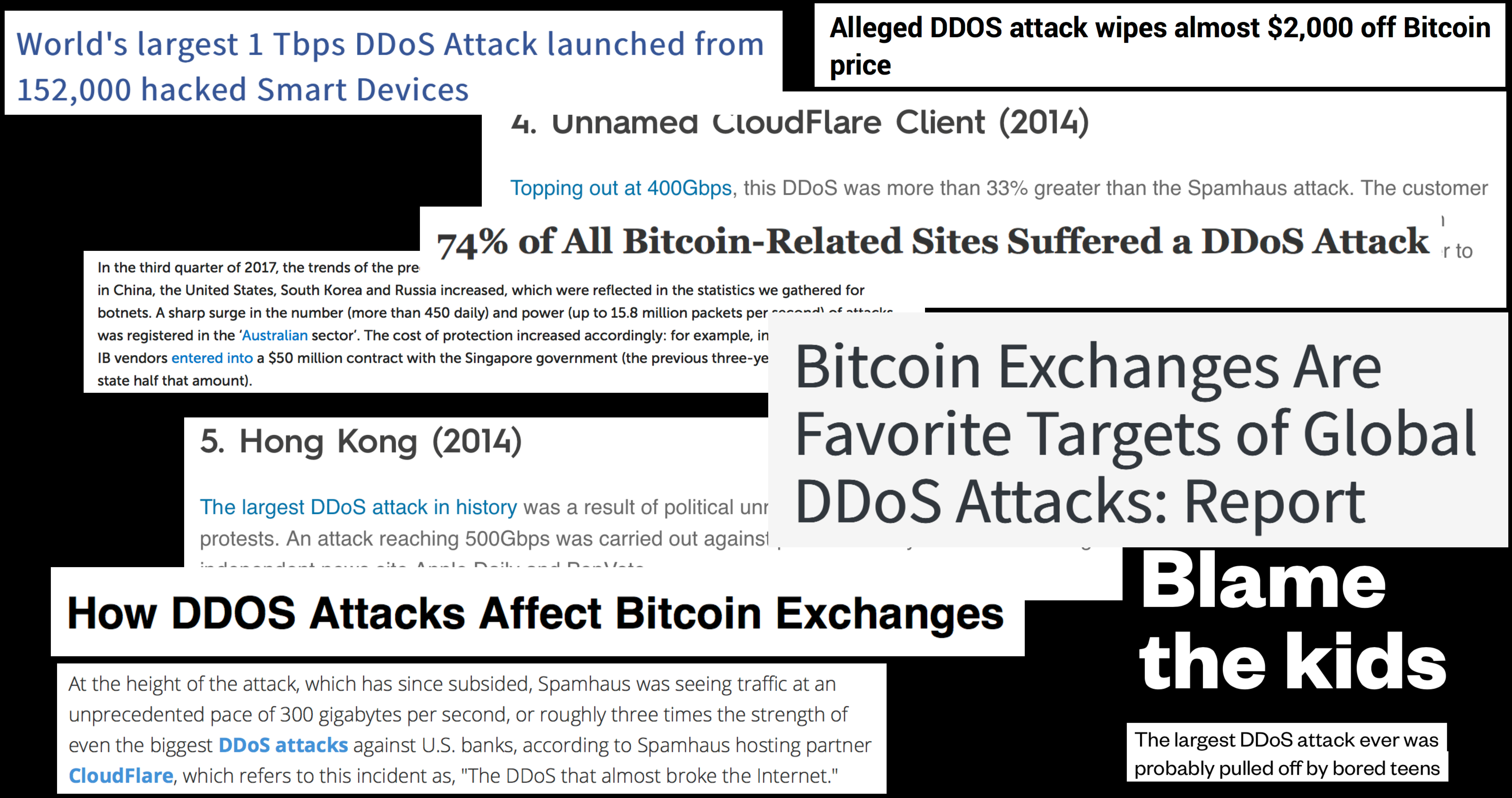
How to protect against DoS (2/2)

- Buy an expensive load balancer (lol) - please don’t
- Use haproxy
- Apply the same kind of rules as for L4 to L7, rinse, repeat
- https://www.haproxy.com/fr/blog/four-examples-of-haproxy-rate-limiting/ - Sliding Window Rate Limiting, Rate Limit by Fixed Time Window, Rate Limit by URL, Rate Limit by URL Parameter
- My favorite, playing dead: very slowly reply with an error to abusive requests - attacker thinks they won, legitimate users don’t notice anything
- Many, many other examples on haproxy blog

DDoS

actual slide
from the
ICO PPT

The problem (1/2)



World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices

Alleged DDOS attack wipes almost $2,000 off Bitcoin price

4. Unnamed CloudFlare Client (2014)

Topping out at 400Gbps, this DDoS was more than 33% greater than the Spamhaus attack. The customer

74% of All Bitcoin-Related Sites Suffered a DDoS Attack

r to

In the third quarter of 2017, the trends of the pre
in China, the United States, South Korea and Russia increased, which were reflected in the statistics we gathered for botnets. A sharp surge in the number (more than 450 daily) and power (up to 15.8 million packets per second) of attacks was registered in the 'Australian sector'. The cost of protection increased accordingly: for example, in
IB vendors entered into a $50 million contract with the Singapore government (the previous three-ye
state half that amount).

Bitcoin Exchanges Are Favorite Targets of Global DDoS Attacks: Report

5. Hong Kong (2014)

The largest DDoS attack in history was a result of political unr
protests. An attack reaching 500Gbps was carried out against
independent news site Apple Daily and PopVote

How DDOS Attacks Affect Bitcoin Exchanges

At the height of the attack, which has since subsided, Spamhaus was seeing traffic at an unprecedented pace of 300 gigabytes per second, or roughly three times the strength of even the biggest **DDoS attacks** against U.S. banks, according to Spamhaus hosting partner **CloudFlare**, which refers to this incident as, "The DDoS that almost broke the Internet."

Blame the kids

The largest DDoS attack ever was probably pulled off by bored teens

actual slide
from the
ICO PPT

The problem (2/2)

- DDoS is easy (you can buy one on publicly accessible websites and it’s nearly impossible to track back the perpetrator) and relatively cheap

- DDoS is harmful (few companies can endure a few 100s Gbps attack, let alone a few Tbps attack)

- Protection is hard (magic appliances and firewalls only work if your incoming pipe is bigger than the size of the attack)

- Gbps are not everything, Mpps are worse and Msps (sessions per second) are a nightmare

- Attackers get smart (we start seing adaptative attacks detecting the kind of protection used) and attacks evolve fast

The (only) solution

- Have bigger pipes than the sum of all the attackers
- Currently it’s at least a few Tbps (yes, Tera bits per second)
- As good as your filter (we call it scrubbing center) is, if the incoming pipe can’t handle the attack, the filters are worthless
- Filtering hundreds of Gbps is _hard_

The (good) ideas

- Filter as early as possible, as much as possible
- BCP38, RPKI, IRR… - make sure the traffic coming to you is actually for you and is actually coming from the network pretending to be sending it to you
- Flowspec - basically, describe expected traffic (ip:port …) and propagate that to BGP peers
- Use 100Gbps network interface cards with integrated FPGAs for in-nic first stage filtering (Intel, Mellanox,…)
- Then we go into usual firewalling / rate-limiting / L4-L7 filtering

The (less good) ideas

- JS proof of work (for web browsers)
- TCP “hashcash” (for API clients)
- IP reputation database (in a (side)chain, of course) for pre-approval or pre-ban of users based on previous behavior

More (good) ideas

- Direct connect to “clouds” - clean traffic doesn’t go through Internet
- VPN for “premium” users
- 100+Gbps backbone across the world
- Ultimately, an independant “Internet” for Bitcoin users and services

- It’s like the SWIFT network for Bitcoin?
- Or just a cypherpunk dream of having an independent network

What about DNS

- Hard to protect
- Just build it big enough to absorb any (legitimate or not) load
- 2x25G Mellanox NICs with embedded ARM CPUs, OS and own intelligence

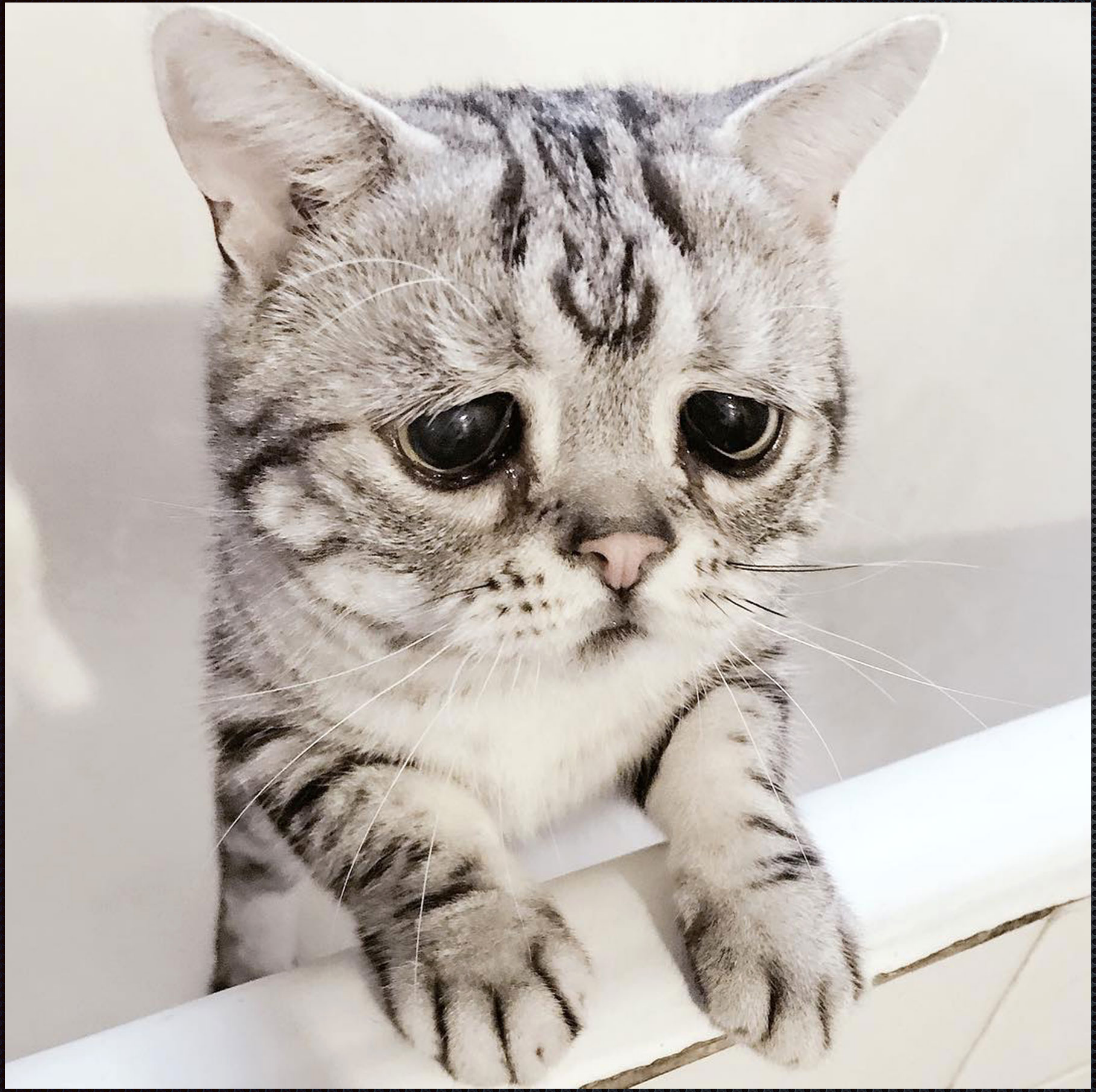
$$$

- Attackers won’t wait for us to scale up before attacking
- We need to be ready from day 1

How do we achieve that

- Minimum 1 Tbps capacity per Point Of Presence
- Minimum 10 POPs in the world
- 30-60 100 Gbps ports routers for each location
- Private 100 Gbps links between POPs
- Servers with 100 Gbps FPGA NICs for filtering
- Servers with 25 Gbps “Smart” NICs for DNS
- Direct Connect to AWS, Azure, GCP, Private infrastructures

btw, how big do you think a 60*100Gbps router is?



But we came for the ICO

How to finance this project

- Project born during the big ICO crazyness - opportunism
- Estimated cost of the project (CAPEX + OPEX): $10M to $100M depending on the coverage for 1 to 3 years of operation
- “DoS Token” (BTC sidechain) used as a mean to pre-sell the service to potential users (exchanges, mining pools, corporate / whale users)
- RGB, Liquid, … didn’t exist yet

Why we didn’t do it

- Project born during the big ICO crazyness - opportunism
- Estimated cost of the project (CAPEX + OPEX): $10M to $100M depending on the coverage for 1 to 3 years of operation
- “DoS Token” (BTC sidechain) used as a mean to pre-sell the service to potential users (exchanges, mining pools, corporate / whale users)
- RGB, Liquid, … didn’t exist yet

Could we still do it?

- The cost of the project would probably be between 2 to 4 times lower than 2 years ago
- We could probably start with $5M and build up from that
- IPv4 are gone and expensive to get on the secondary market
- Notwithstanding the anti-DDoS part, we are still building it, self-funded, on a small scale (GVA, PAR, FRA, NYC, MSK, …)
- This is the “nodl cloud”

Q ?