Protect Kamailio Against DoS Attacks With APIBan

September 2020
@fredposner

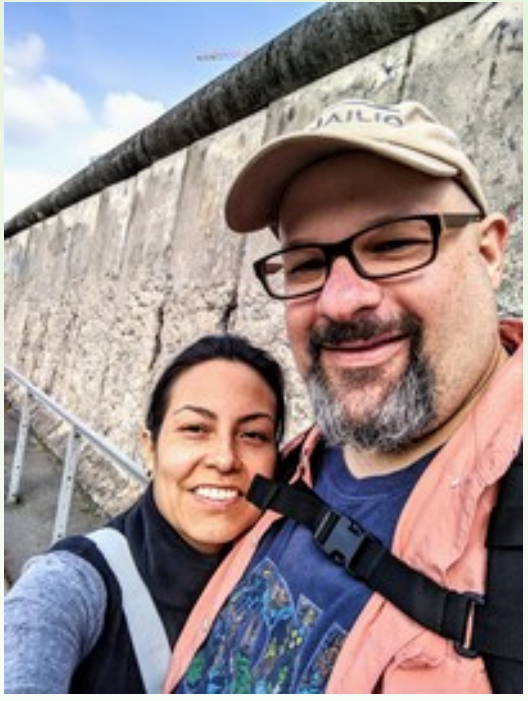
Kamailio World

What is APIBAN

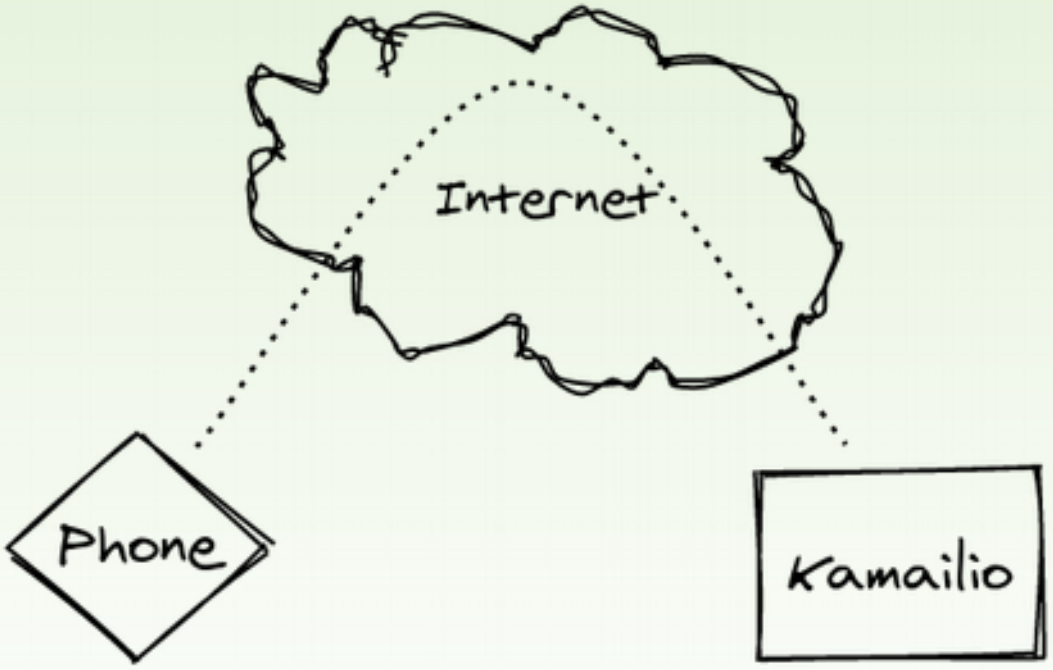
- “Community Sharing of **Bad Actors**”
- Free
- Hosted/Provided by LOD.com

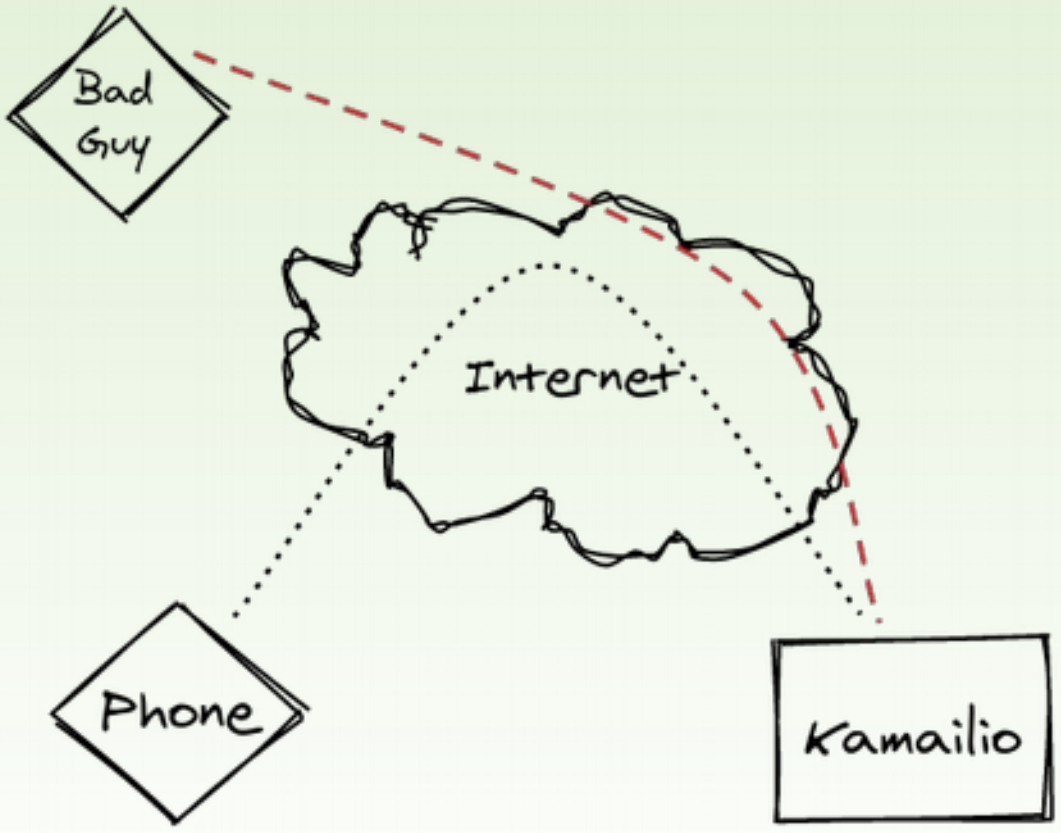
Who am I?

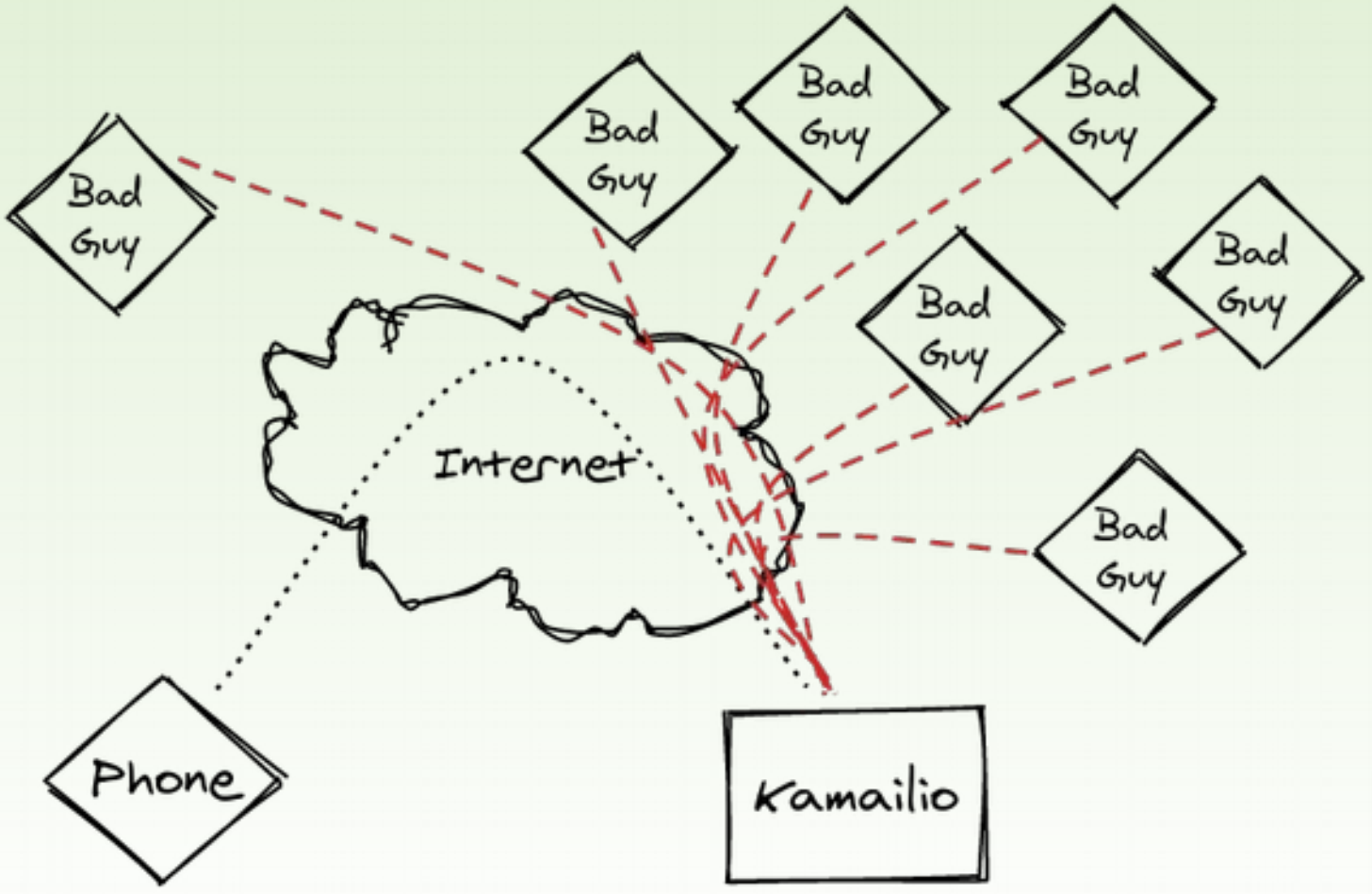
- Fred Posner
- qxork.com
- Loves Kamailio

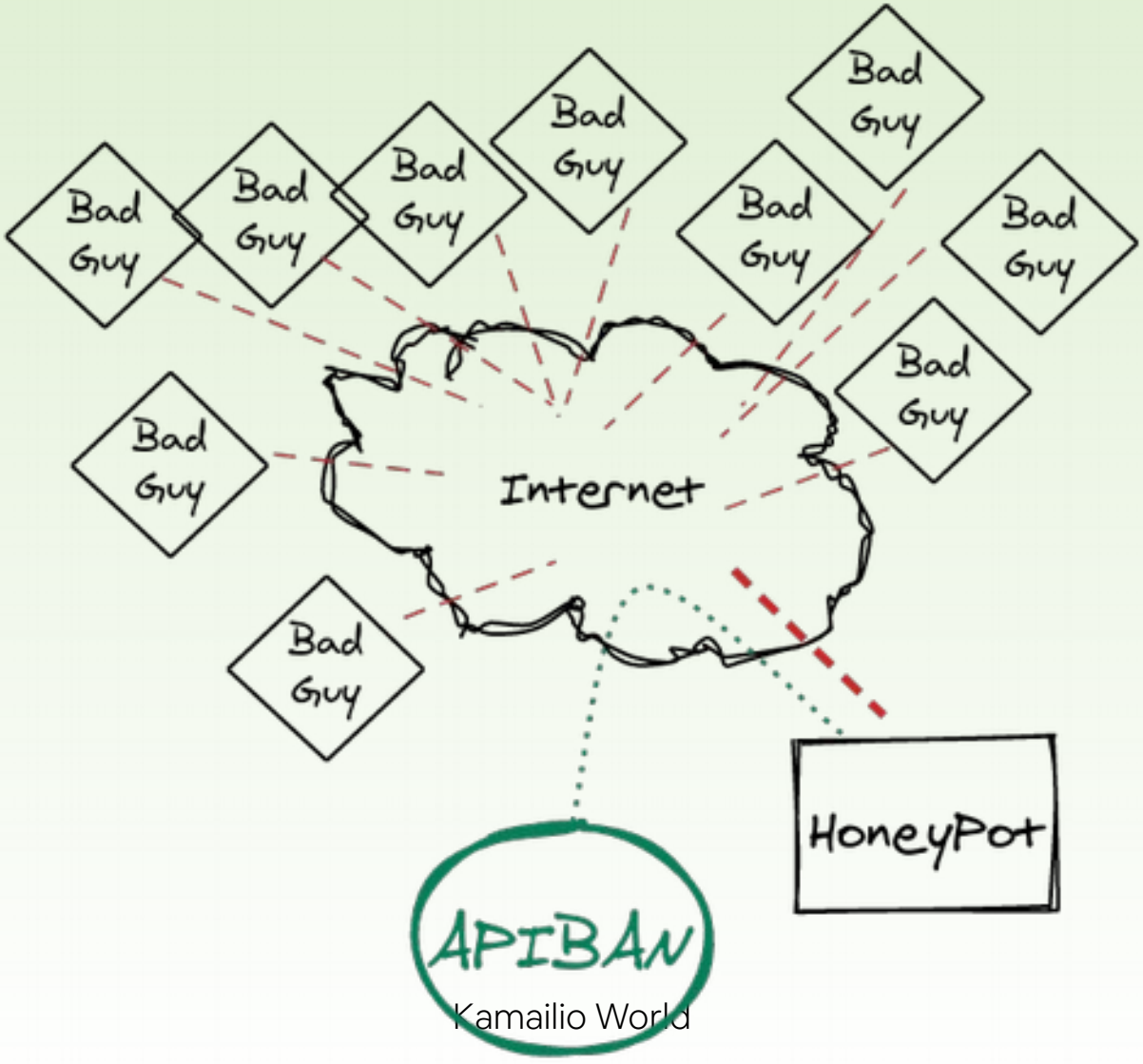


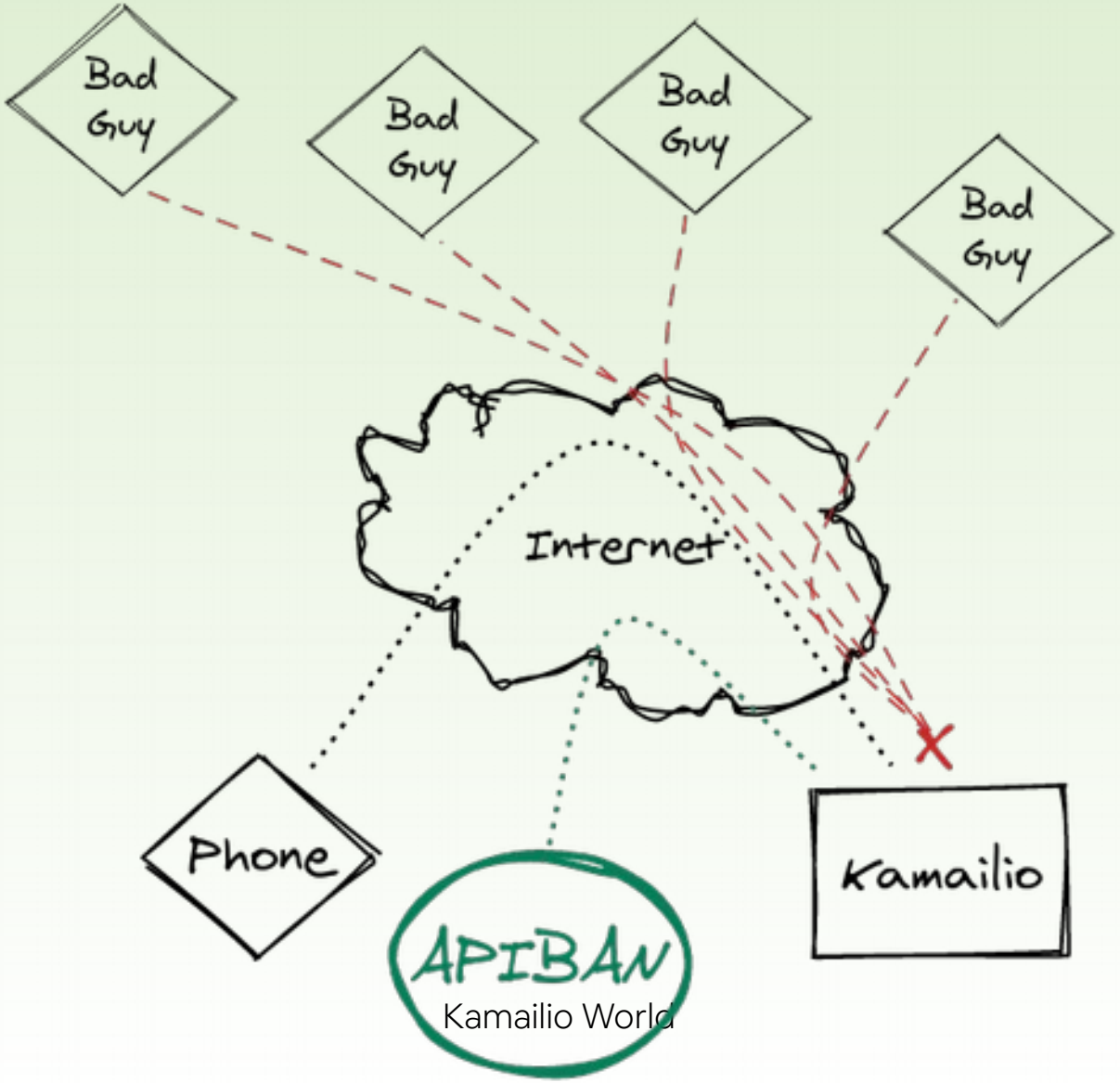
APIBAN Overview

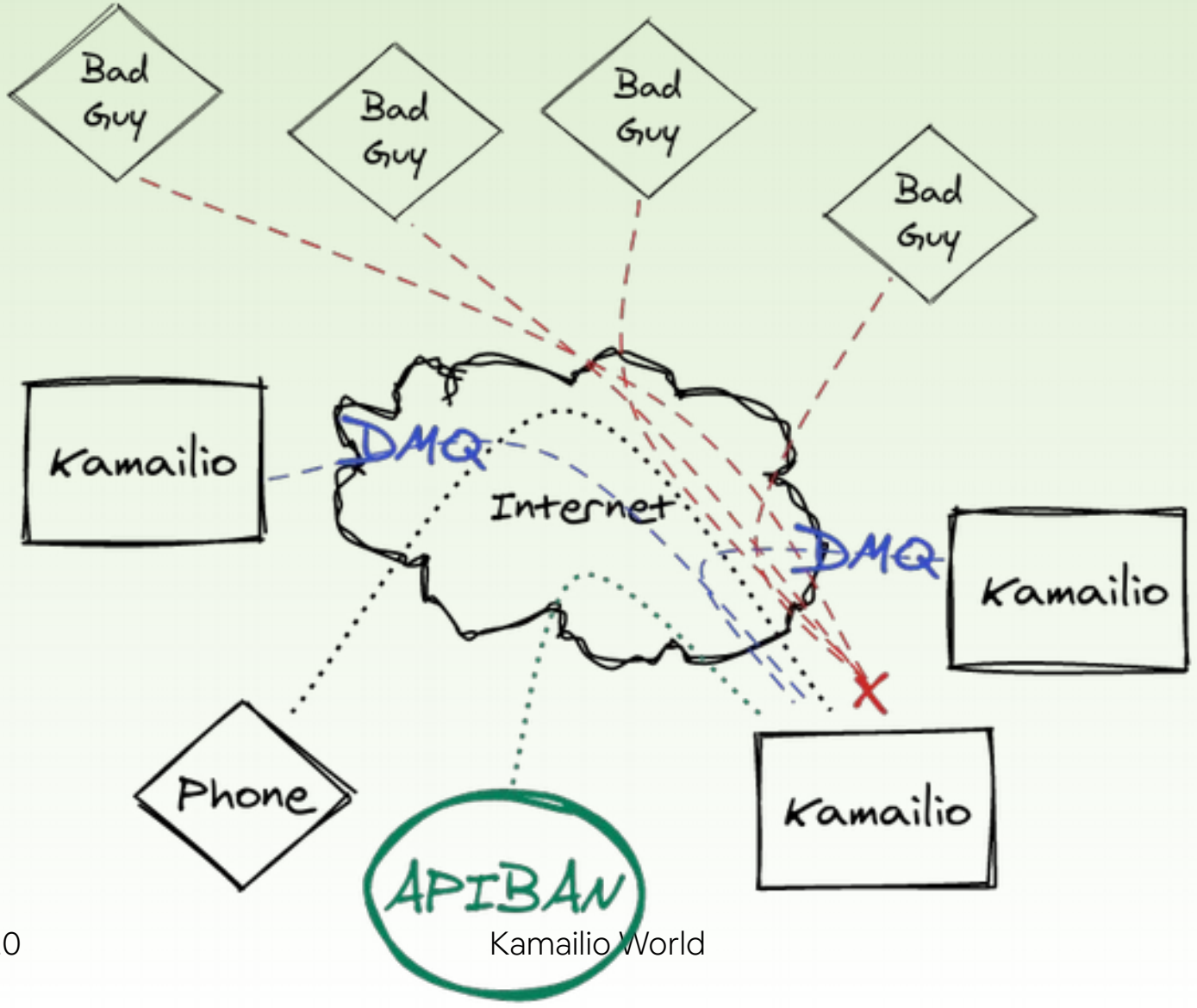



Bad Guy
Internet
Phone
Kamailio


Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Internet
Phone
Kamailio


Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Bad Guy
Internet
HoneyPot
APIBAN


Bad Guy
Bad Guy
Bad Guy
Bad Guy
Internet
Phone
APIBAN
Kamailio


Bad Guy
Bad Guy
Bad Guy
Bad Guy
Kamailio
DMQ
Internet
DMQ
Kamailio
Phone
APIBAN
Kamailio

Why?

- Benefits of conferences and side conversations...
- We all get scanned
- Always talked about getting a centralized data source
- Found myself some time

How Does it Work?

- **Trusted** Honeypots
- Globally Deployed
- Special thanks to Ivan Nyarko
- Record SIP traffic

- USA (many locations)
- UK
- Berlin
- Mumbai
- Sao Paulo
- Paris
- Cape Town
- Canada
- Plus others

How Does it Work?

- IP Addresses are “active” for 7 days
- Can be reactivated immediately
- API based retrieval of lists (full, incremental, individual)
- 5 requests / 2 min

How Does it Work?

- Step 1: Get a key
  - apiban.org
  - sent via email
- Step 2: Deploy
  - Kamailio
  - Stand alone client

Kamailio Integration

- **HTABLE**
- **HTTP_CLIENT**
- **JANSSON**
- **RTIMER**
- **DMQ?**

Config Highlights

- max_while_loops=250
- apiban=>size=11;
- apibanctl=>size=1;initval=0;
- RTIMER to sync new addresses

Config Highlights

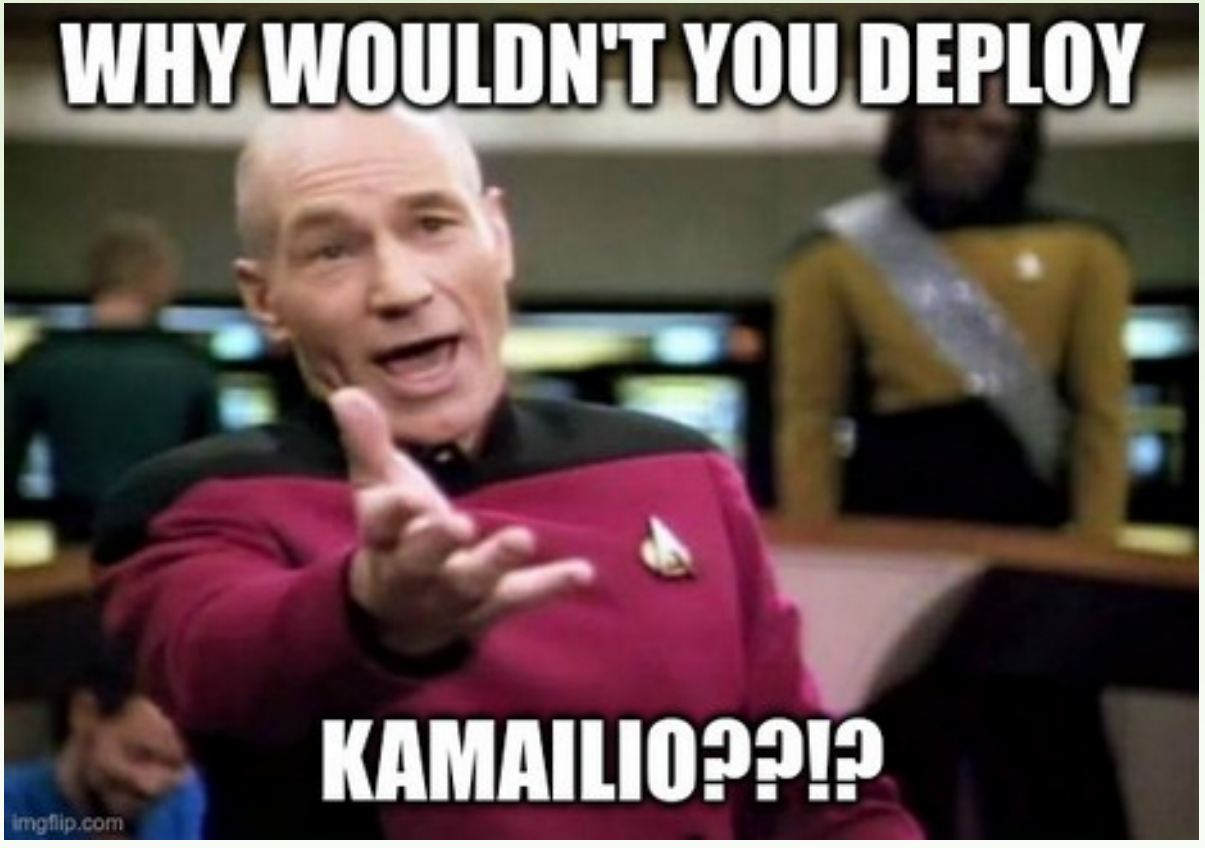
```
if($sht(apiban=>$si)!=$null) {
    // ip is blocked from apiban.org
    xdbg("apiban blocked IP - $rm from $fu (IP:$si:$sp)\n");
    exit;
}
```

Get the config example

- https://apiban.org/doc.html
- https://github.com/palner/apiban

What if no Kamailio?


NO KAMAILIO?
imgflip.com


WHY WOULDN'T YOU DEPLOY
KAMAILIO??!?
imgflip.com

APIBAN Clients

- Bash
  - IPTABLES
  - NFT
- Go(lang)
  (Huge thank you to Seán C McCord)
  - IPTABLES

Questions?

Thank you for flying Kamailio!