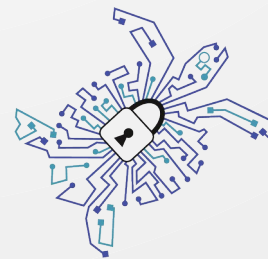# Tor Relays @ Foundation for Applied Privacy

Tor Relay Meetup

36C3, December 2019

Foundation for
Applied Privacy

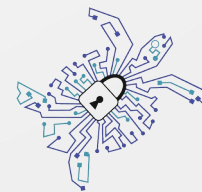# Foundation for Applied Privacy

- Non-profit Privacy Infrastructure Provider

- based in Vienna, Austria

- we run privacy enhancing services for the public
  - Tor Relays
  - DNS Privacy Services (DoH, DoT)

Foundation for
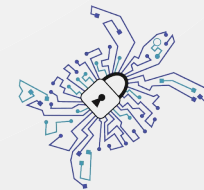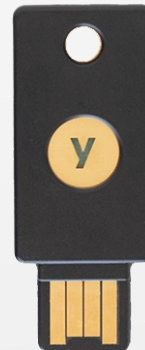Applied Privacy

34C3: tuwat!

Foundation for
Applied Privacy

Tor Exit Relay Infrastructure

- dedicated hardware

- exclusively used for Tor

- 10G uplinks via two transit provider

- SSH keys are stored on

Tor Exit Server Setup

- 16 Tor instances on single server
  (2 CPUs, 16 cores, 64GB RAM)

- configuration management using ansible-relayor

- per instance bw limit: 480 MBits

- OfflineMasterKey
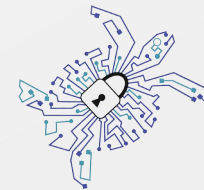
- OutboundBindAddressExit

ANSIBLE

Foundation for
Applied Privacy

DNS Resolver

unbound

- DNSSEC

- minimize data exposure:
  - QNAME minimization

  - prefetching

  - local root zone

  - 10 GByte cache
- 16 threads

Tor Exit Relay Preparations

- ticket system with auto responder
  - requirements: self-hosted, GPG and 2FA support

- WHOIS, abuse-c

- reverse DNS

- exit notice HTML page

DNS PTR Records

|	
109.70.100.18	tor-exit-anonymizer-01.appliedprivacy.net
109.70.100.19	tor-exit-anonymizer-02.appliedprivacy.net
109.70.100.20	tor-exit-anonymizer-03.appliedprivacy.net
109.70.100.21	tor-exit-anonymizer-04.appliedprivacy.net
109.70.100.22	tor-exit-anonymizer-05.appliedprivacy.net
109.70.100.23	tor-exit-anonymizer-06.appliedprivacy.net
109.70.100.24	tor-exit-anonymizer-07.appliedprivacy.net
109.70.100.25	tor-exit-anonymizer-08.appliedprivacy.net
109.70.100.26	tor-exit-anonymizer-09.appliedprivacy.net
109.70.100.27	tor-exit-anonymizer-10.appliedprivacy.net
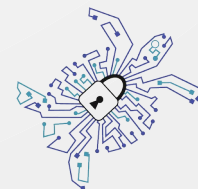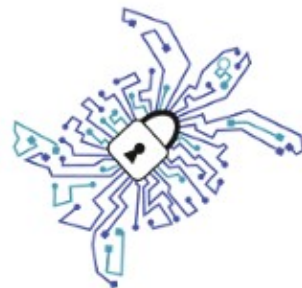
Foundation for
Applied Privacy

This is a Tor Exit Router

Most likely you are accessing this website because you had some issue with the traffic coming from this IP. This router is part of the Tor Anonymity Network, which is dedicated to providing privacy to people who need it most: average computer users.
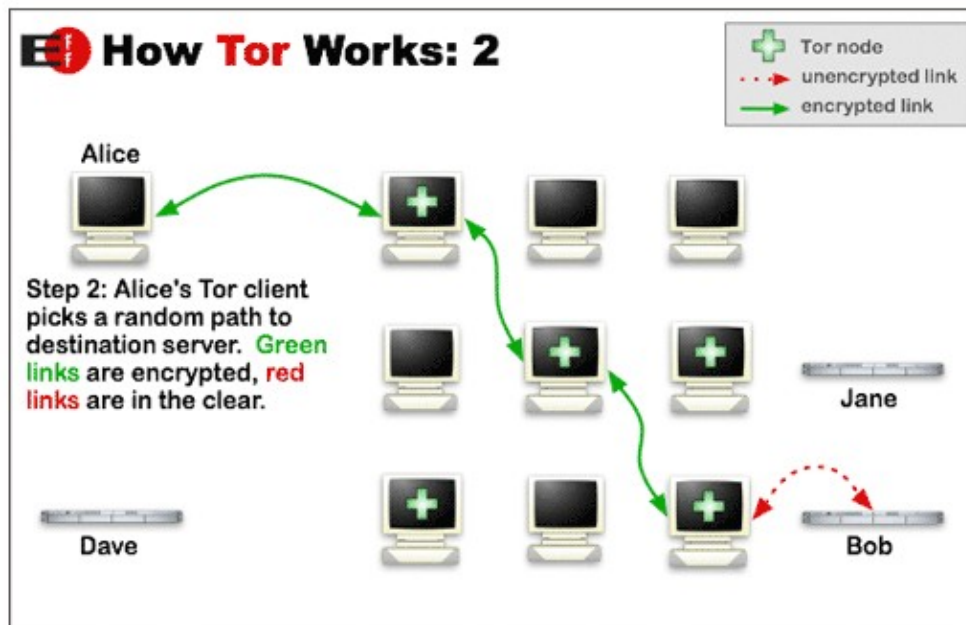
RIPE DB / WHOIS

Responsible organisation: Foundation for Applied Privacy
Abuse contact info: abuse@appliedprivacy.net

```
inetnum:      109.70.100.0 - 109.70.100.64
netname:      TOR-EXIT--FOUNDATION-FOR-APPLIED-PRIVACY
remarks:      Send abuse emails to: abuse@appliedprivacy.net
country:      AT
org:          ORG-PRIV3-RIPE
admin-c:      OPER1-RIPE
tech-c:       OPER1-RIPE
abuse-c:      ATF13-RIPE
status:       ASSIGNED PA
```
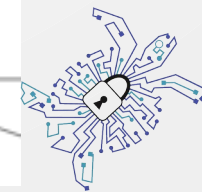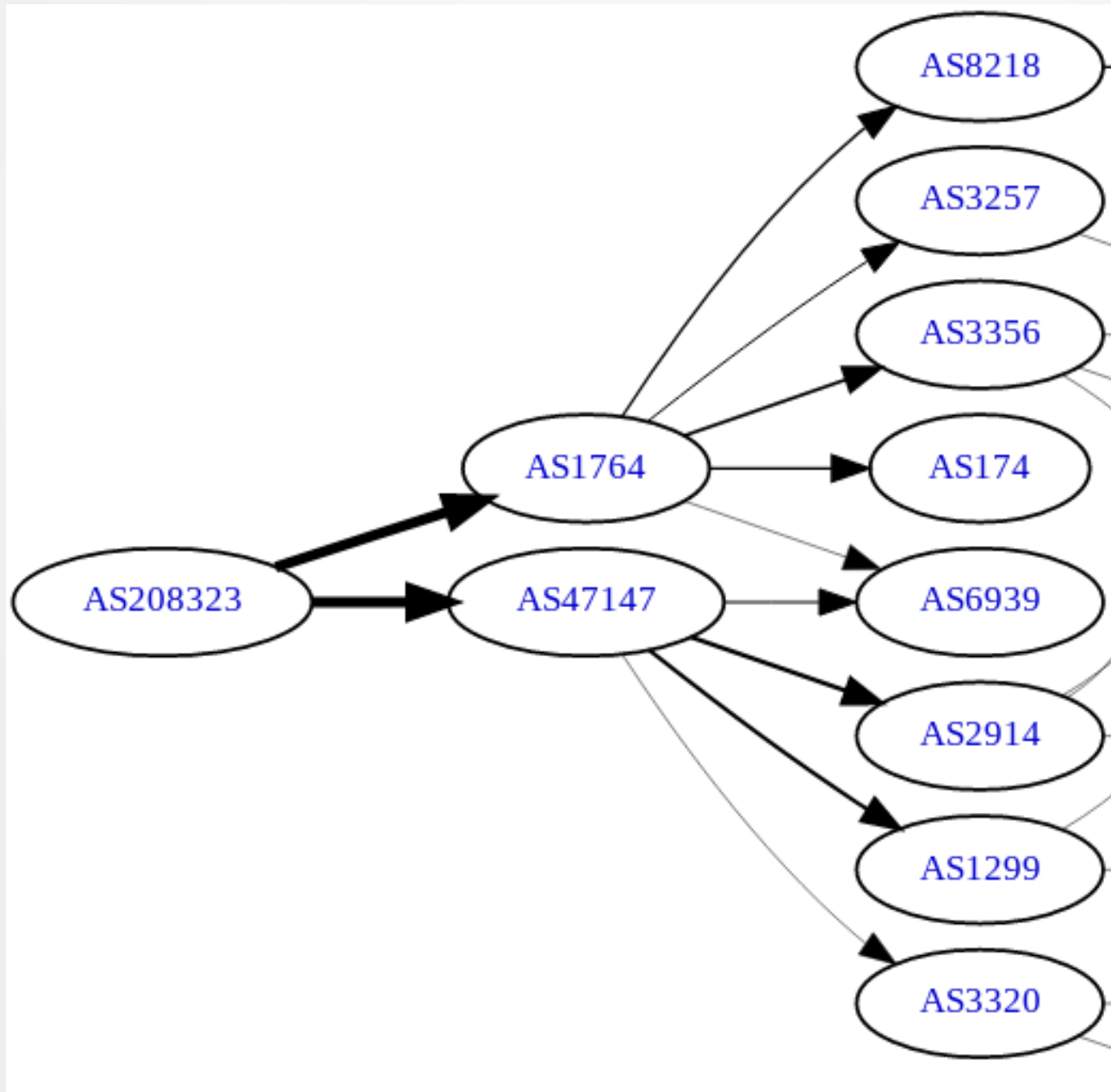
Foundation for
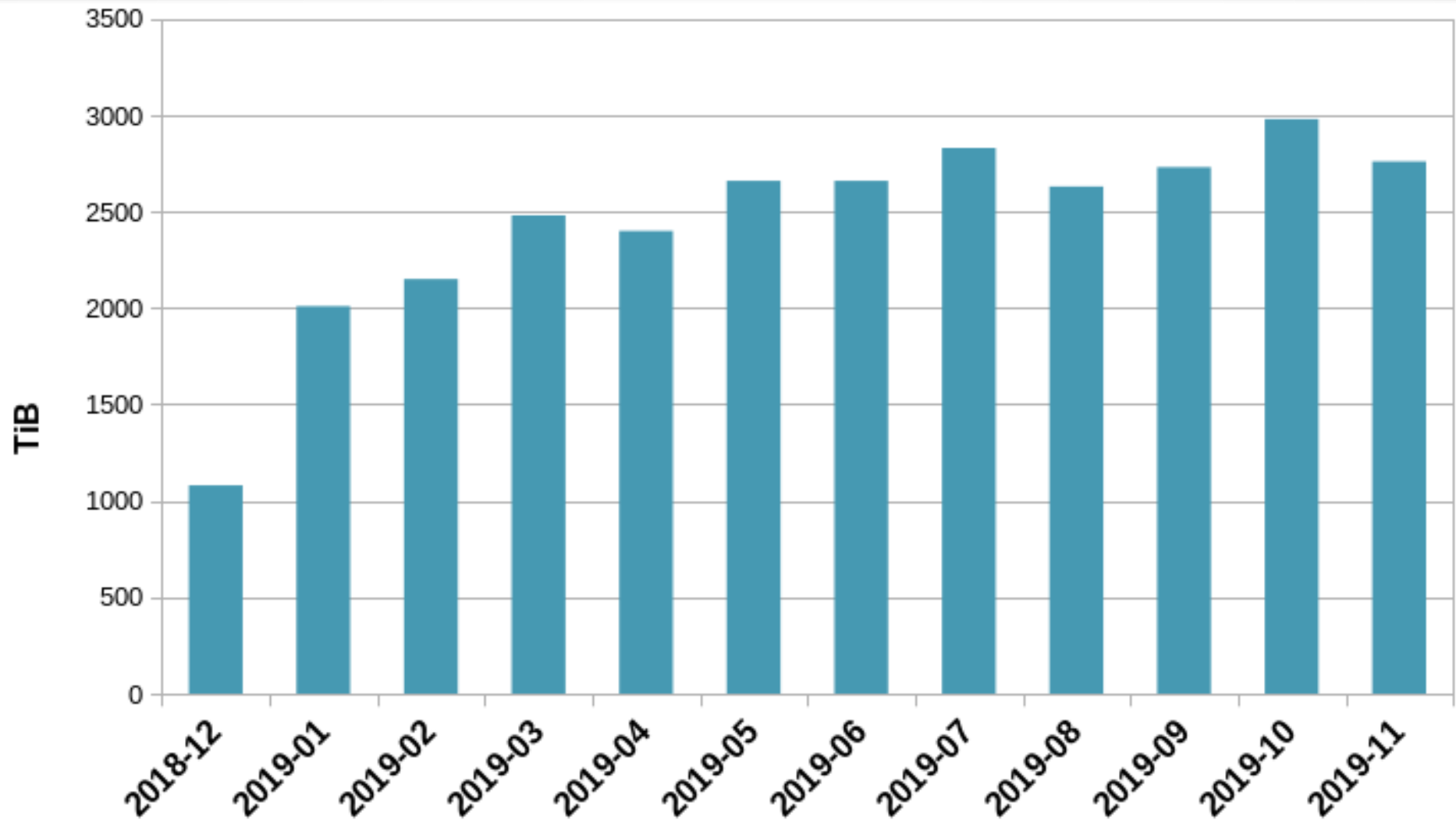Applied Privacy

Autonomous System

- AS208323
- Community IX requirement
- motivation: **free bandwidth**
- BGP Routing Security (RPKI)
- Redundancy
- Abuse Management
- Anycast (not related to Tor)

Foundation for
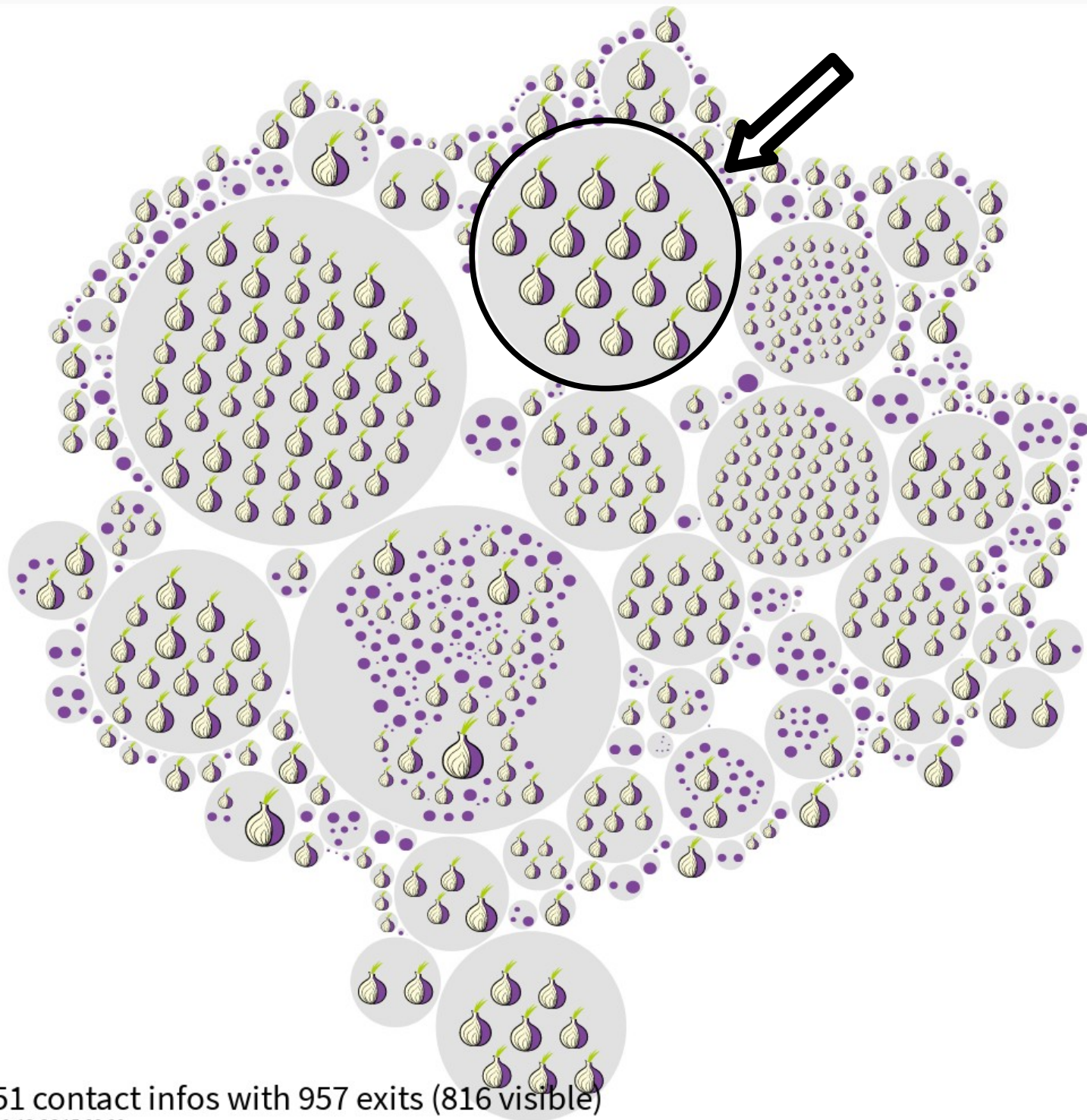Applied Privacy

Autonomous System

Our Traffic Stats

Foundation for
Applied Privacy

>35 Petabibytes Traffic
(2018-06 - 2019-11)

Foundation for
Applied Privacy

351 contact infos with 957 exits (816 visible)
2019-12-26 15:00:00

Abuse Stats

- most abuse emails are automated

- 9 LEA requests (2018-08 - 2019-12)
  - Austria (4)
    - from USA (1) – invalid, not our IP address
    - from Belarus (1)
  - Russia (2)
  - Norway (1)
  - Germany (1)
  - India (1)

Foundation for
Applied Privacy

What's next?

Foundation for
Applied Privacy

Yearly Transparency Reports

Foundation for
Applied Privacy

Infrastructure Security Bug Bounty

Foundation for
Applied Privacy

applied-privacy.net

DoT
dot1.applied-privacy.net

DoH
https://doh.applied-privacy.net/query

Tor Exit Relays
109.70.100.0/26
2a03:e600:100::/112

STICKERS!!!!!11
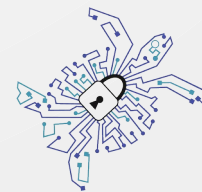
Foundation for
Applied Privacy

Hoodies

Foundation for
Applied Privacy

Questions?

✉ contact@appliedprivacy.net

🐦 @applied_privacy

🐘 https://mastodon.social/@applied_privacy

https://applied-privacy.net
PGP: 45F1C720EDCD34E1D584609768E9077A0D81577A

Foundation for
Applied Privacy