Open Resolvers and why do they still exist?

Swapneel Patnekar
swapneel.patnekar@shreshtait.com

About me

- CEO at Shreshta, India - a DNS Security and cyber threat intelligence company
- FIRST Liaison & Co-chair of DNS Abuse SIG
- APNIC Community Trainer

Scope

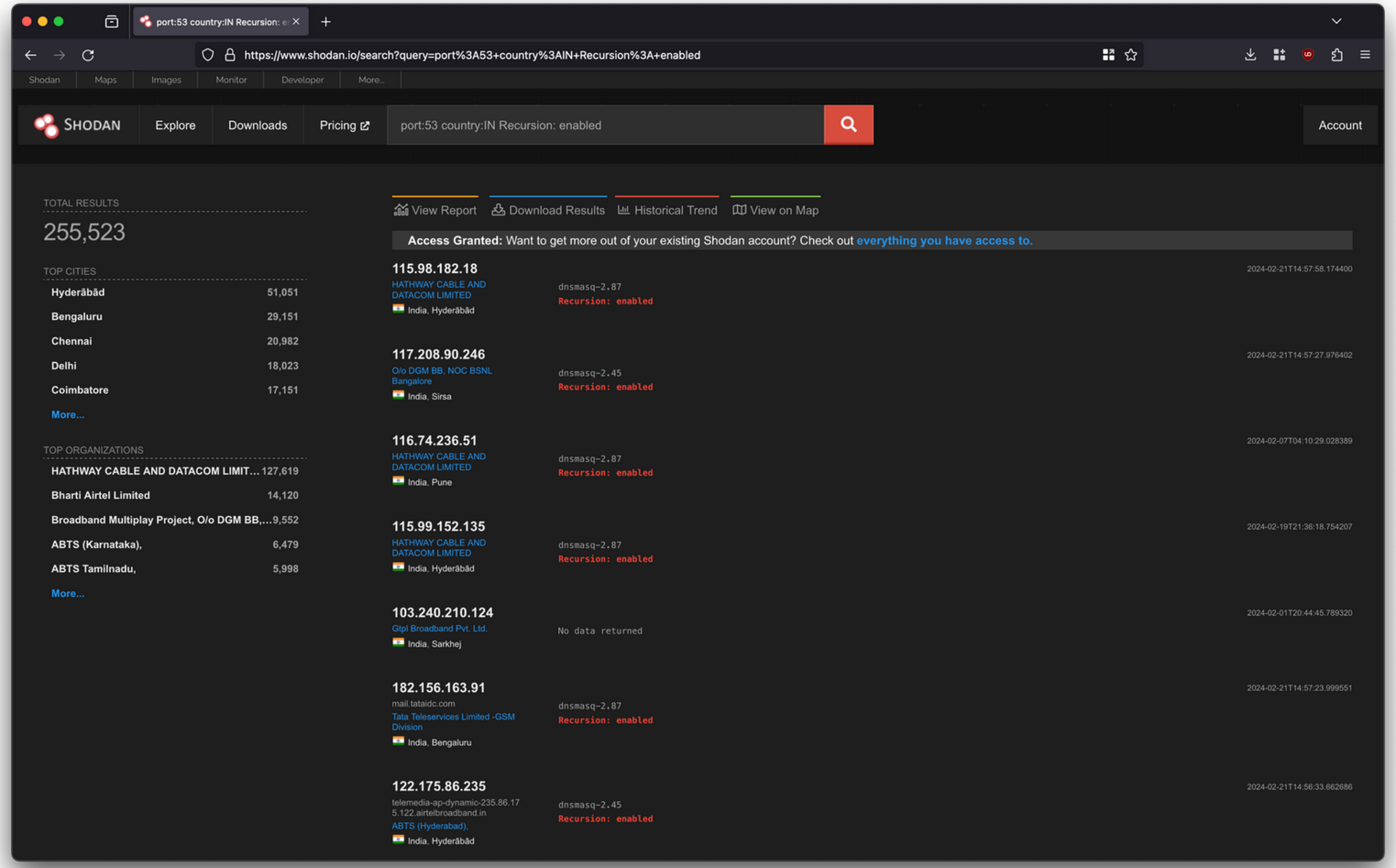
- Focus is on open resolvers excluding the ones operated by Quad resolver operators, threat intelligence company(honeypots) etc

- DNS servers with recursion enabled accepting DNS queries from any IP address on the Internet


```
{
  "asn": "AS17488",
  "hash": -1360646303,
  "os": null,
  "timestamp": "2024-02-21T00:58:15.606312",
  "isp": "Hathway IP Over Cable Internet",
  "transport": "tcp",
  "_shodan": {
    "region": "na",
    "module": "dns-tcp",
    "ptr": true,
    "options": {},
    "id": "1d6cfbcc-90bf-4882-a341-cc34cec0da1b",
    "crawler": "308515b6113c0645034fb8122d0ff0d5194e7e72"
  },
  "hostnames": [],
  "location": {
    "city": "Kolkata",
    "region_code": "WB",
    "area_code": null,
    "longitude": 88.36304,
    "latitude": 22.56263,
    "country_code": "IN",
    "country_name": "India"
  },
  "dns": {
    "software": "dnsmasq-2.87",
    "recursive": true,
    "resolver_id": null,
    "resolver_hostname": null
  },
  "ip": 3419730570,
  "domains": [],
  "org": "HATHWAY CABLE AND DATACOM LIMITED",
  "data": "dnsmasq-2.87\nRecursion: enabled",
  "port": 53,
  "opts": {},
  "ip_str": "203.212.242.138"
}
```

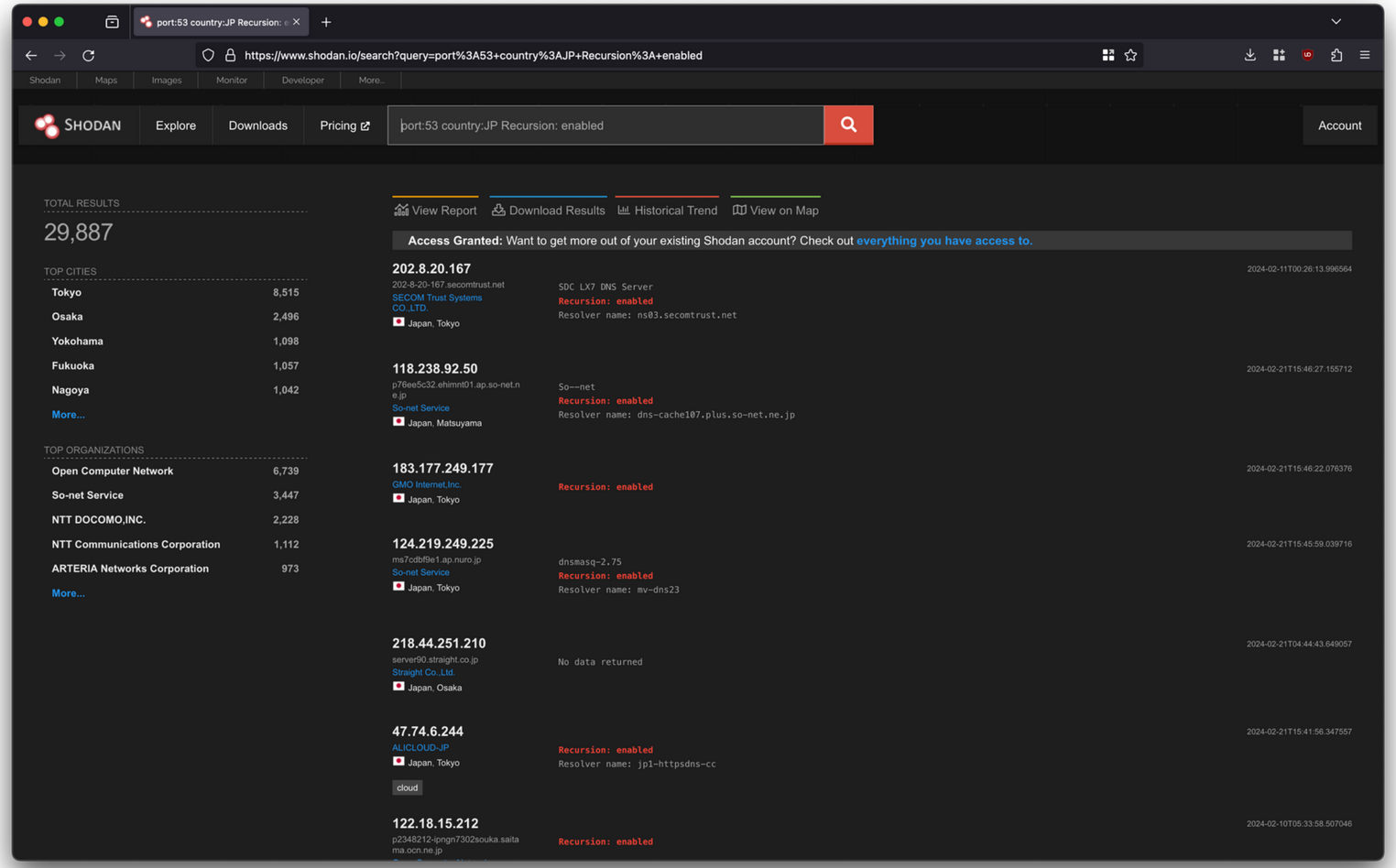
Open Resolvers in India

- Shodan reveals 200,000+ open resolvers in India alone (as on 21st Feb 2024 3:03 pm UTC)
- Count could be possibly higher considering large scale CGNAT deployment by network operators in the country



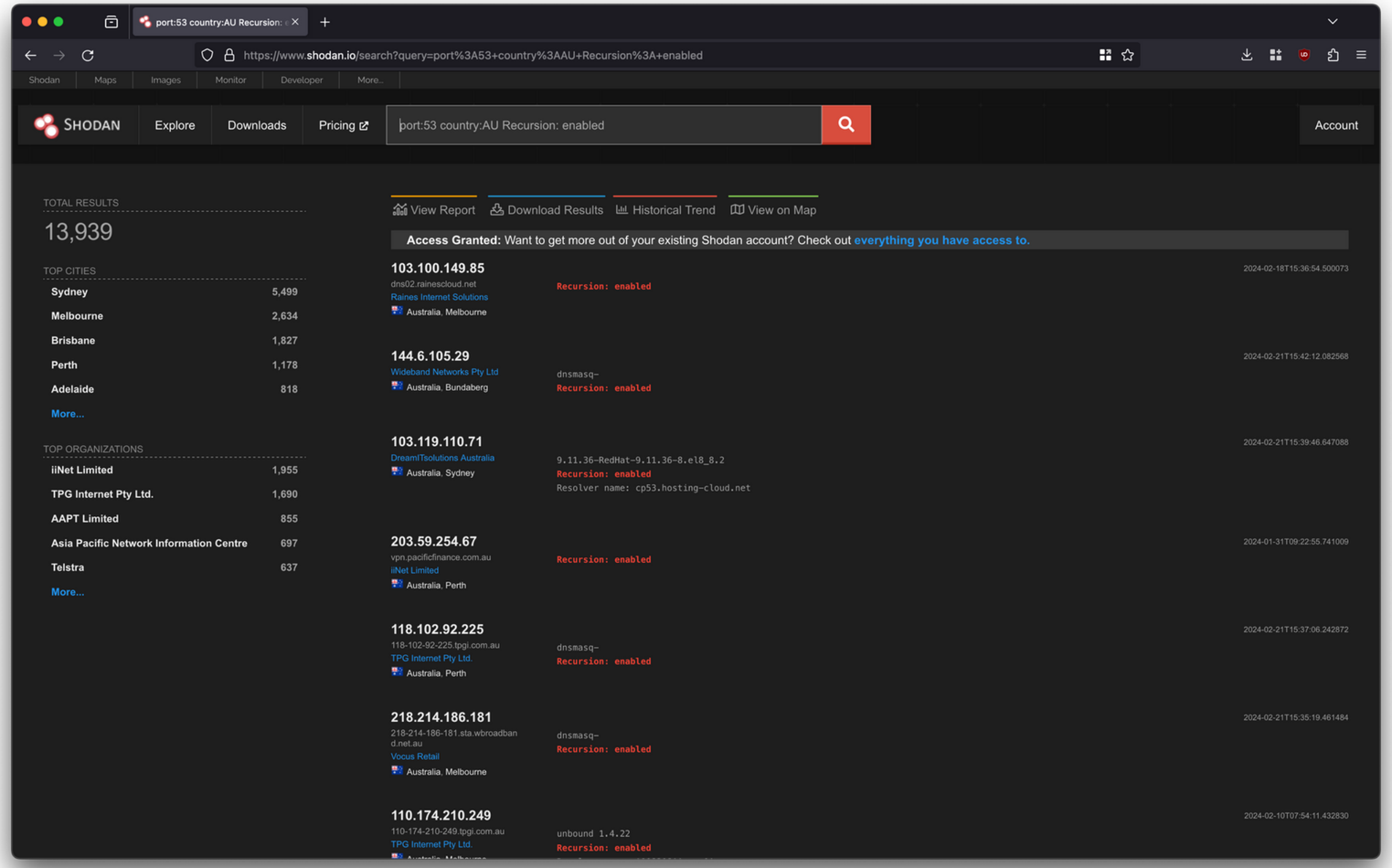
Open Resolvers in Japan

- Shodan reveals 29,000+ open resolvers in Japan alone (as on 21st Feb 2024 3:03 pm UTC)
- Result of “Japan’s IoT scanning project looks for vulnerable IoT devices” ?



Open Resolvers in Singapore

- Shodan reveals 13,000+ open resolvers in Japan alone (as on 21st Feb 2024 3:03 pm UTC)



Why are Open resolvers a problem?

Between 15 January 2023, 15:01:17 and 10 April 2023, 01:28:31, a single instance of our honeypot received 135,972,316 DNS queries from Brazil for the domain higi.com.

What is a DNS amplification attack?

This DDoS attack is a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible.

https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

Under the hood

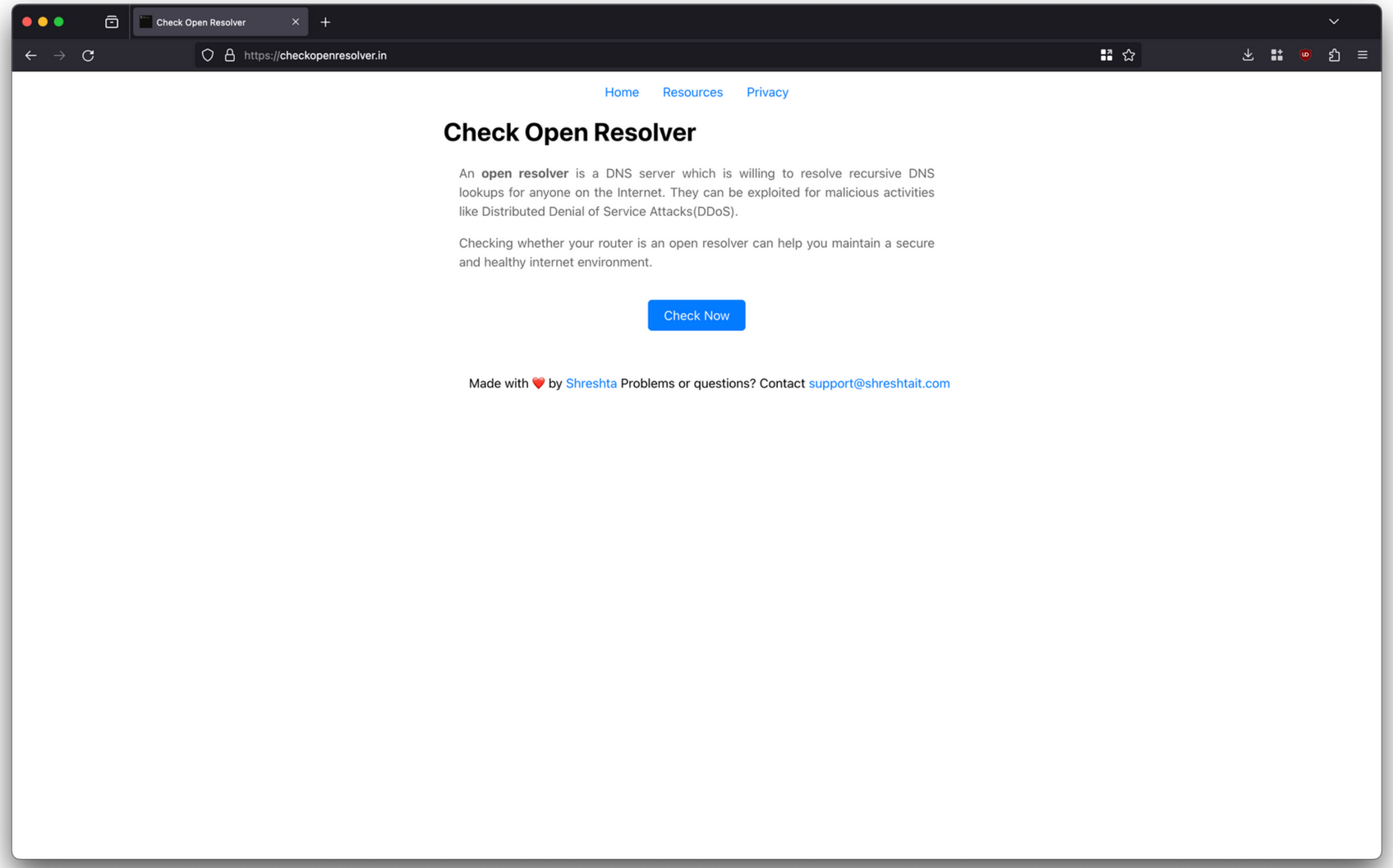
- Broken CPE devices running busybox etc which are EOL, no firmware updates from manufacturer

- Cases of misconfigurations -
  1. Authoritative name servers misconfigured with recursion enabled to the Internet
  2. Enterprise recursive resolvers misconfigured and exposed to the Internet accepting DNS queries from any IP address

Best practices

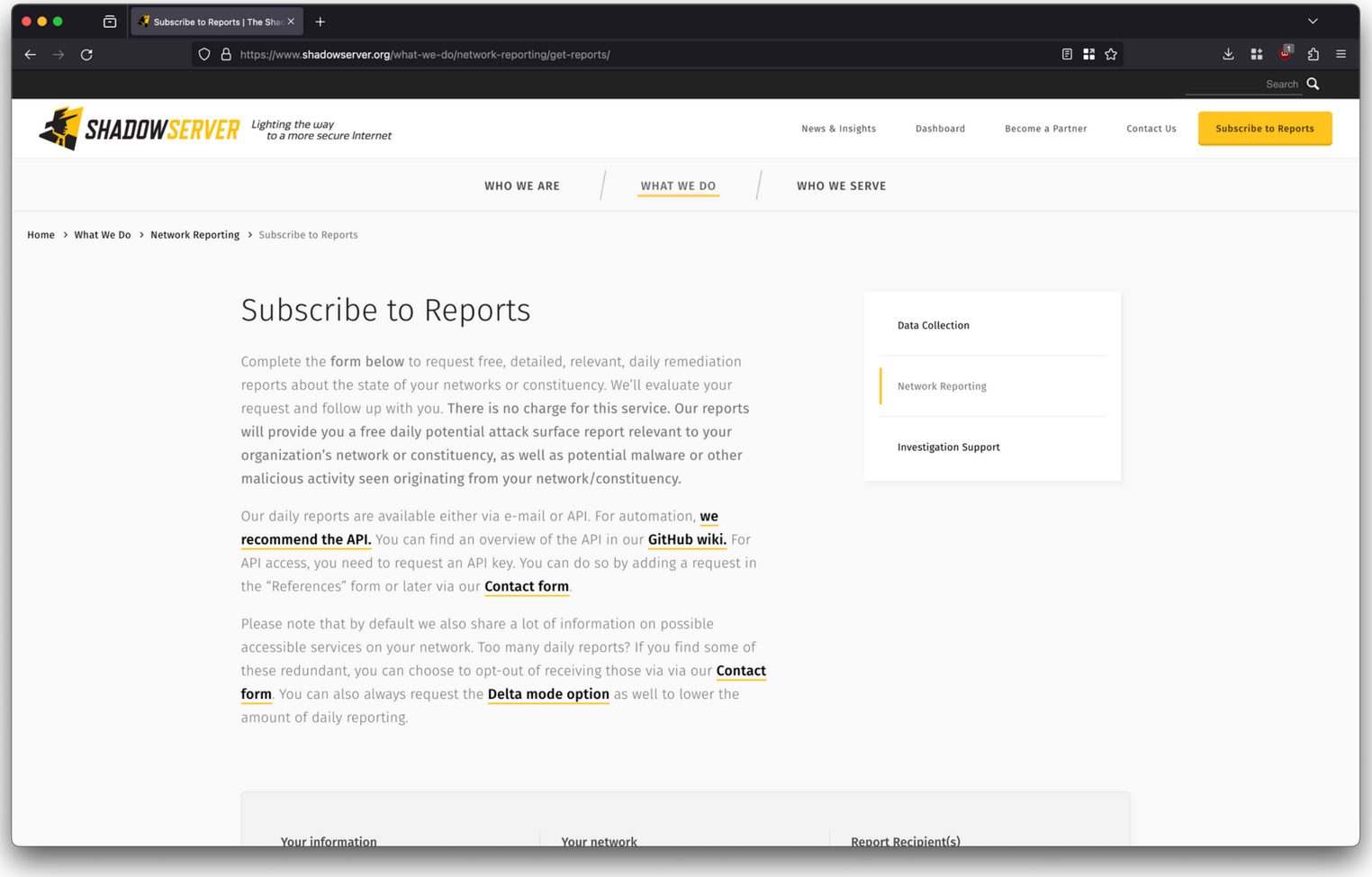
- Allow access to the recursive resolver only to the authorized IP addresses/netblock.
- Response rate limiting.
- On an authoritative-only nameserver, disable recursion.
- For network operators — implement BCP 38 (Network Ingress Filtering).
- ICANN Knowledge-Sharing and Instantiating Norms for DNS and Naming Security(KINDNS)

Checkopenresolver.in



Shadowserver Network Reports

- Free reports for network operators
- Reports are not just limited to port 53



References

- Open Resolvers: Understanding security risks and best practices
  https://blog.apnic.net/2023/05/17/open-resolvers-understanding-security-risks-and-best-practices/

- Check Open Resolver
  https://checkopenresolver.in/

- ICANN Knowledge-Sharing and Instantiating Norms for DNS and Naming Security(KINDNS)
  https://kindns.org/

- Japan’s IoT scanning project looks for vulnerable IoT devices
  https://resources.infosecinstitute.com/topics/iot-security/japans-iot-scanning-project-looks-for-vulnerable-iot-devices/

Thoughts/Questions?