ICANN

ISPCP - OCTO

DNS RELATED THREATS

CAPACITY BUILDING

15:00 UTC | 10 APRIL 2025

What is DNS Abuse?

What is DNS Abuse?

Depends on who you ask:

ICANN's Contractual Definition: "malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS abuse)"
Registrar Accreditation Agreement, 2024 Global Amendment → SAC115

What is DNS Abuse?

Depends on who you ask:

A technical perspective though, from the incident response community - FIRST's DNS Abuse Techniques Matrix:

https://www.first.org/global/sigs/dns/DNS-Abuse-Techniques-Matrix_v1.1.pdf

DGAs	Dynamic DNS Resolution (Obfuscation)
Domain Name Compromise	Fast Flux (Obfuscation)
Lame Delegations	Infiltration/Exfiltration via DNS
DNS Cache Poisoning	Malicious Registration of 2nd Level Domains
DNS Server Compromise	Malicious Subdomains Under Dynamic DNS
Stub Resolver Hijacking	Domain Spoofing
On-path DNS Attack	DNS Tunneling
DoS Against the DNS	C2 Communication
DNS as a Vector for DoS	

What is DNS Abuse?

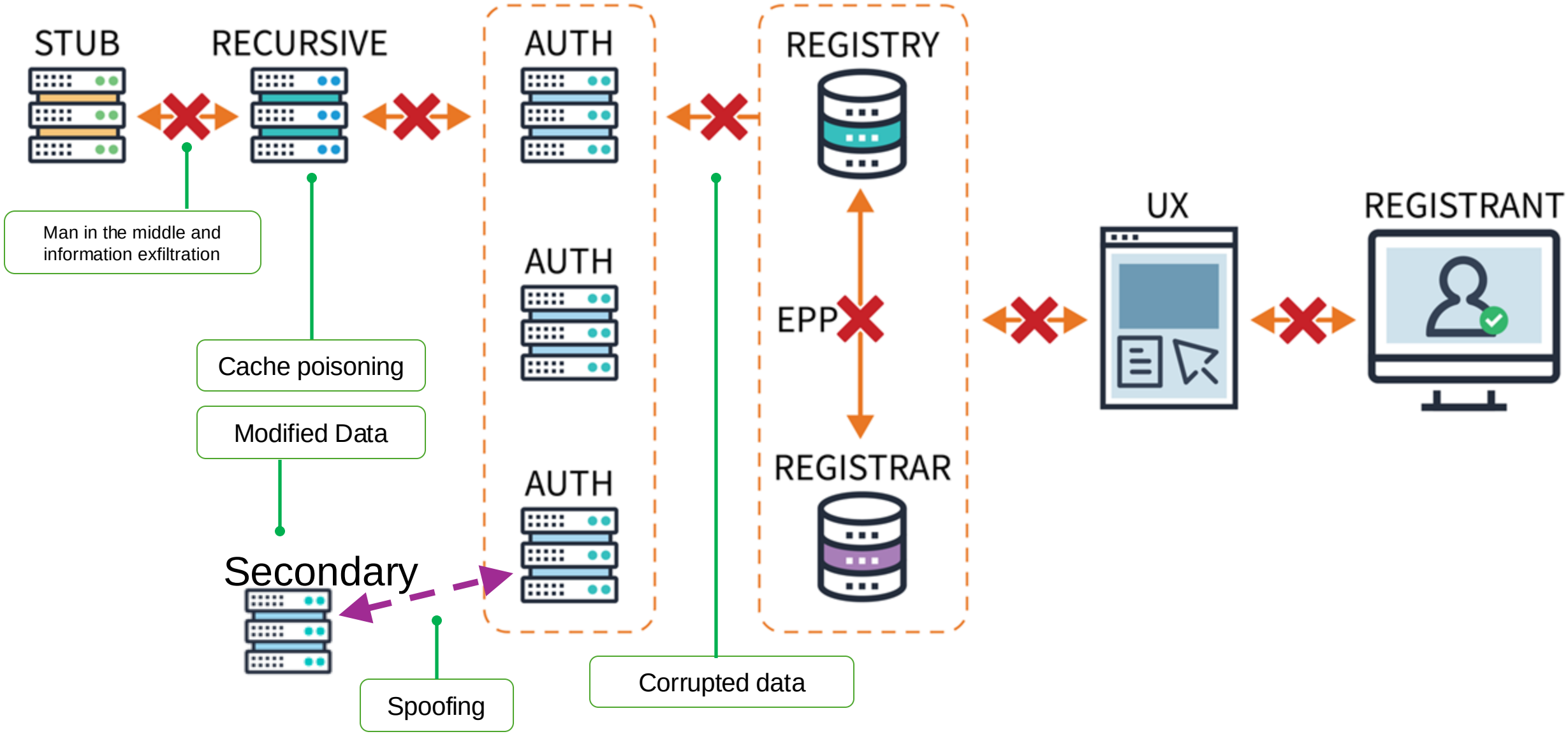
How are they different?

ICANN's Contractual definition is about contract enforcement in the context of certain abuse types

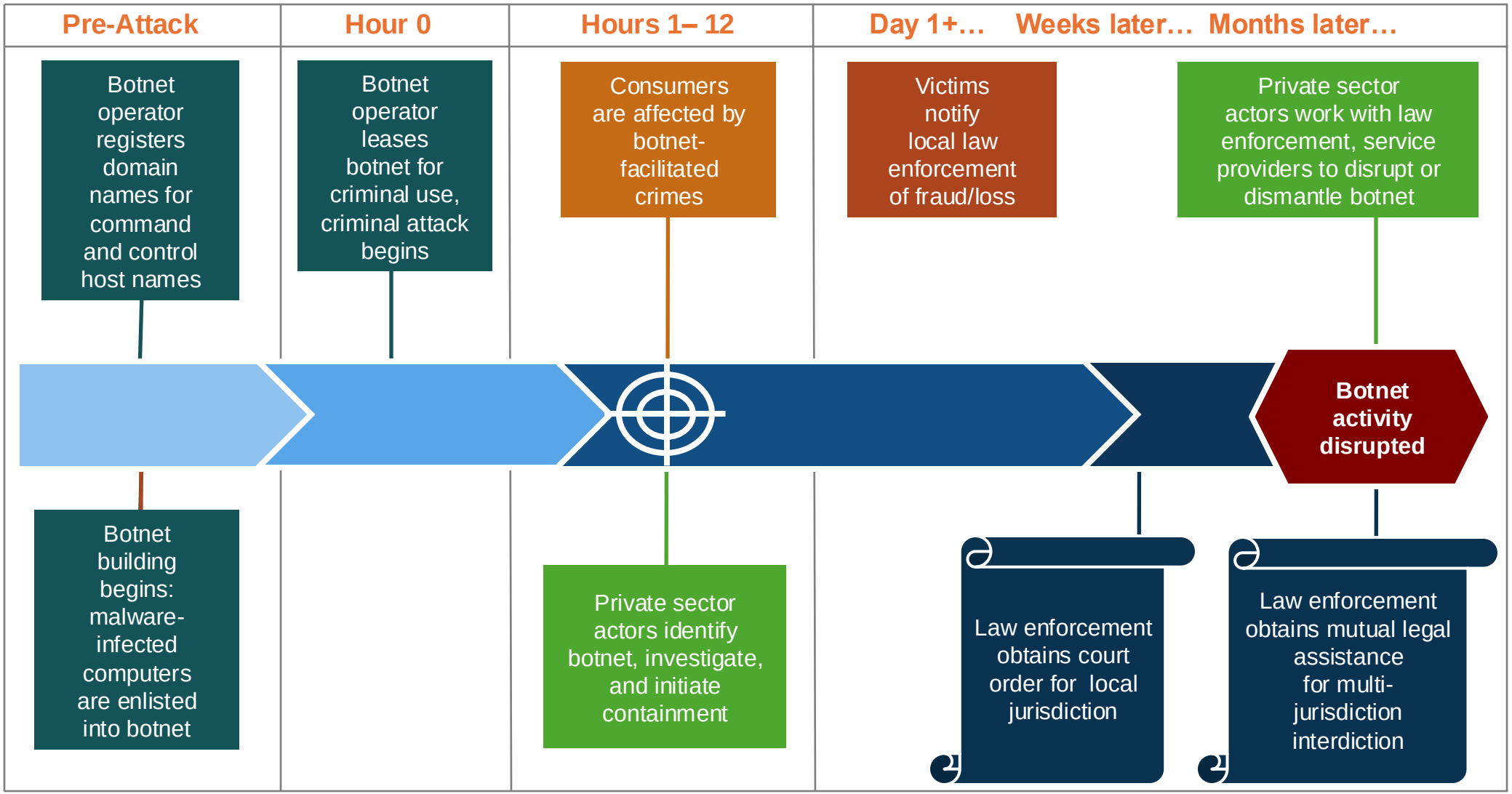
To a cyber security professional, many kinds of malicious activity target the DNS, or leverage it

DNS Perspective

Some of the Potential Target Points of the DNS Ecosystem



Attackers Operate at Internet Pace



Representative Timeline for a Botnet-Enabled Criminal Attack

Time for Some Hard Truth

This is never going to stop

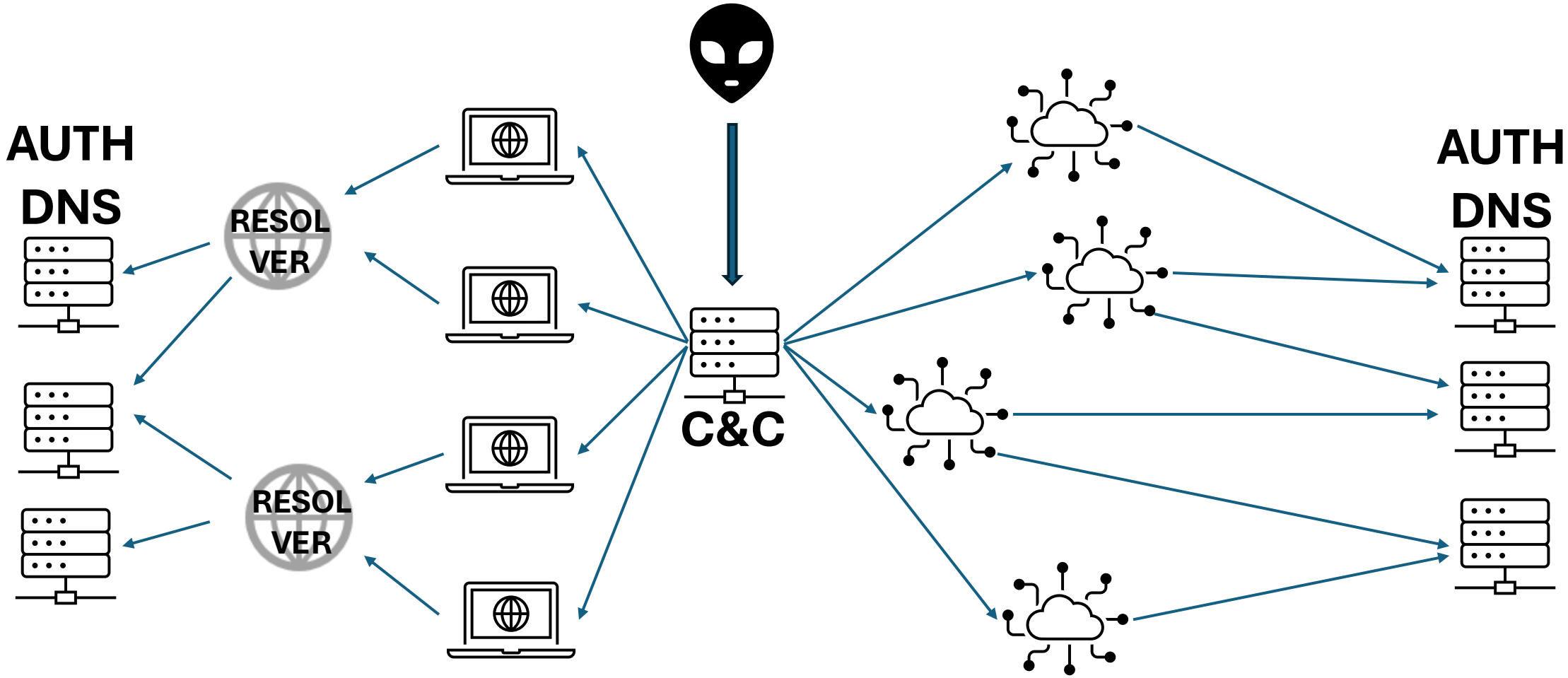
- Attackers are motivated to find new vulnerabilities
- Attackers can be creative and sometimes sophisticated
- Attackers are almost always ahead of ”the good guys”
- Something new is just around the corner . . .

Technical Details

Authoritative DNS

DDoS

DDoS – Distributed Denial of Service



DDoS – Distributed Denial of Service

Prevention

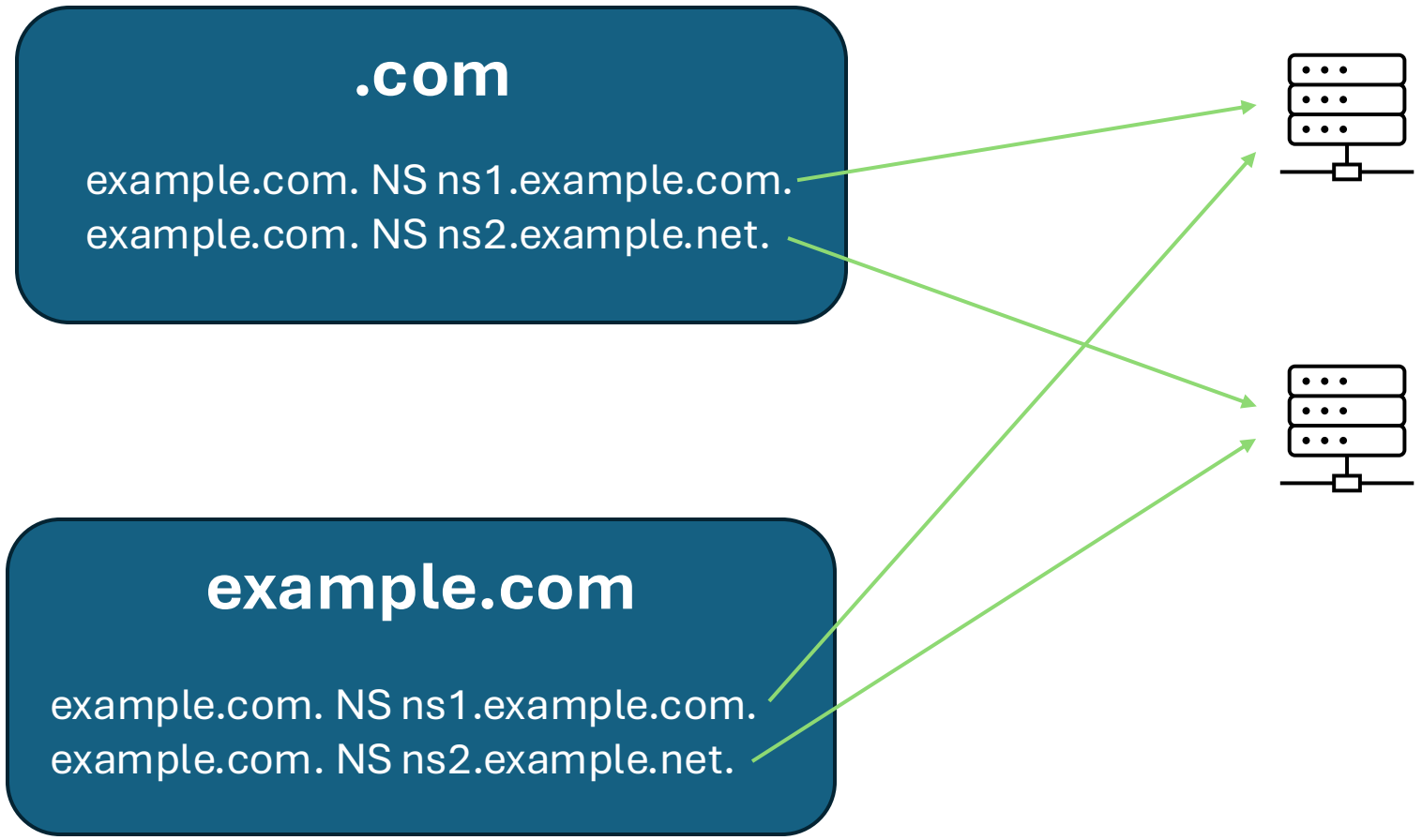
- Do not allow ANY (RFC 8482)
- Rate Limit
- Support DNS Cookies
- DNSSEC – Aggressive NSEC
- Use at least one Anycast DNS Provider, preferably two

The Flood is incoming

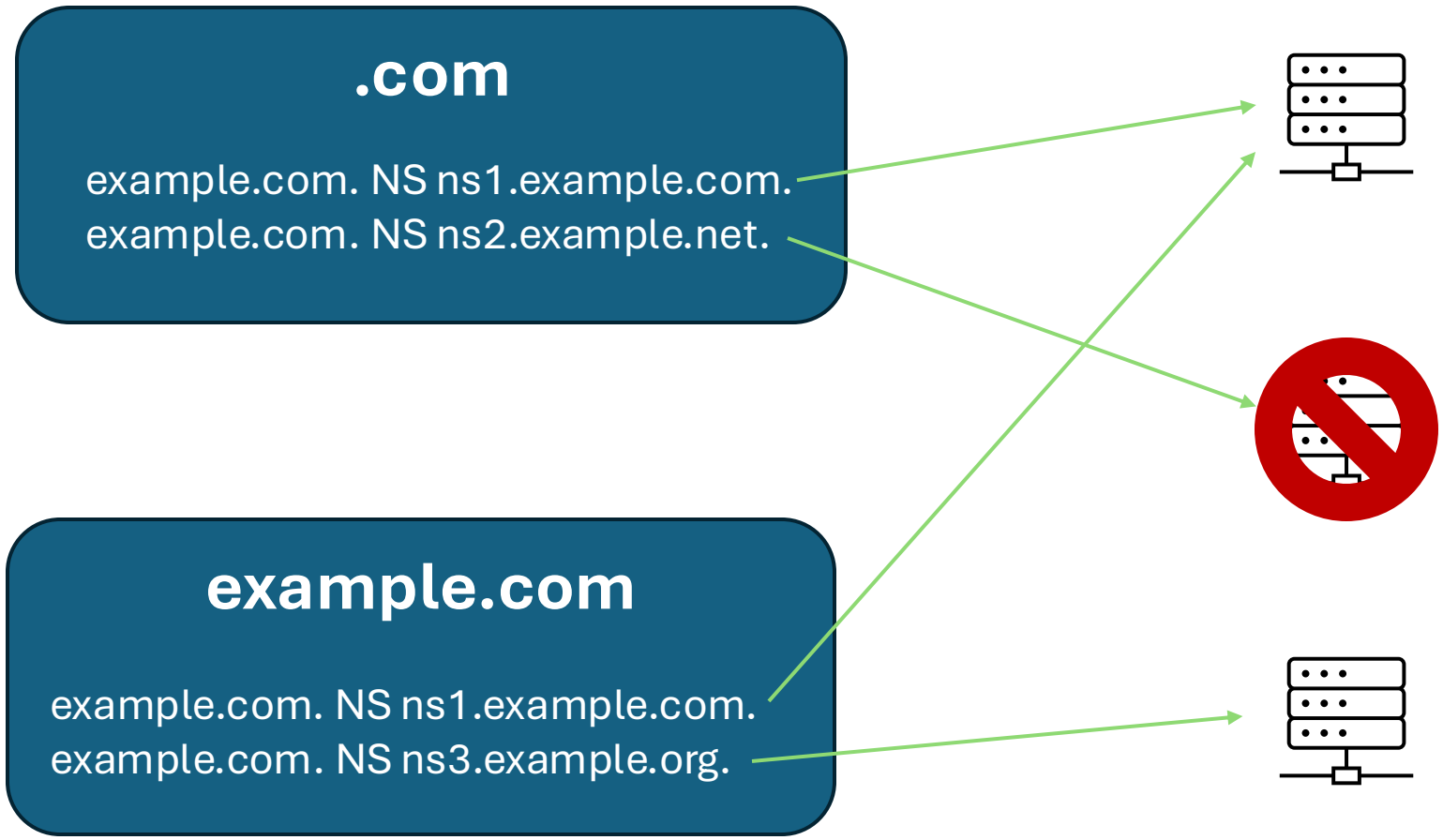
- Plan to retain communications capabilities
- Have contact details and documentation for upstream ready

Lame Delegation

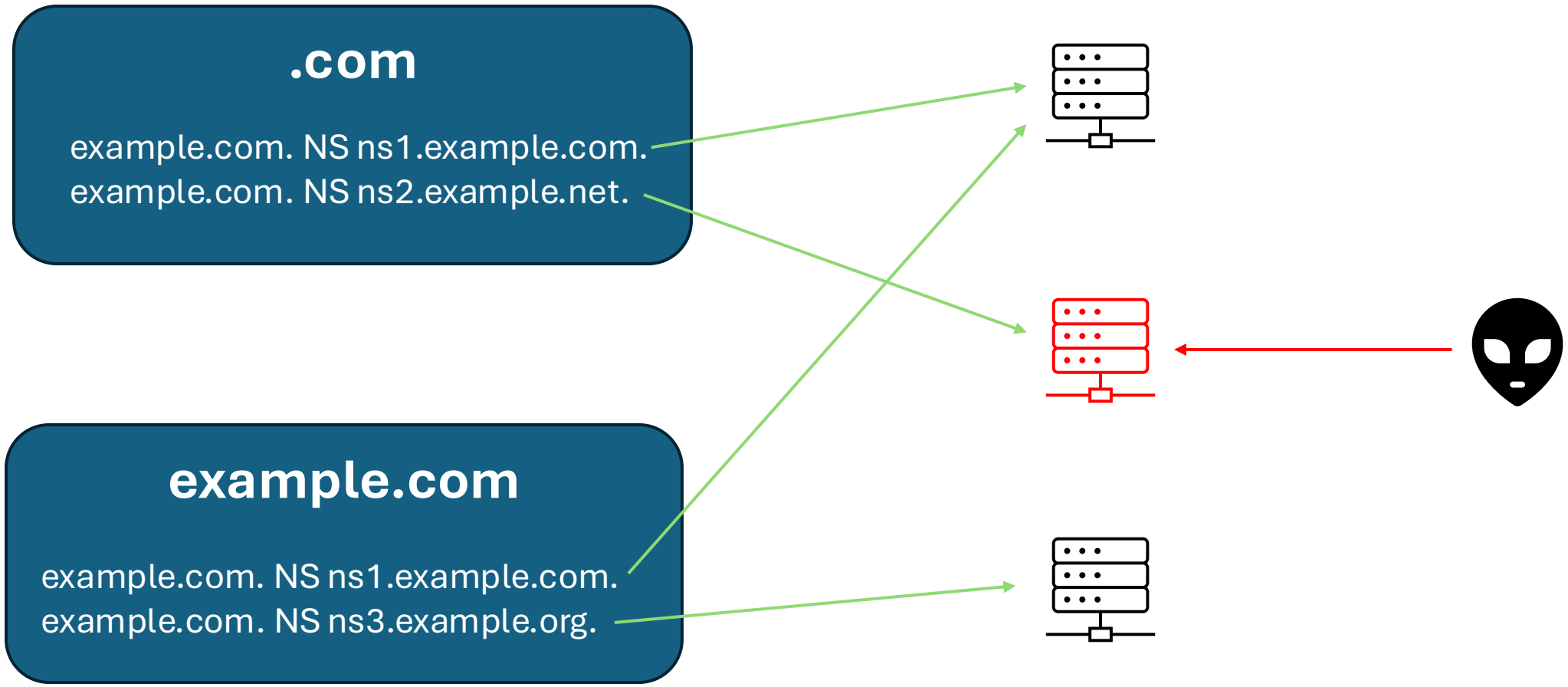
Lame Delegation



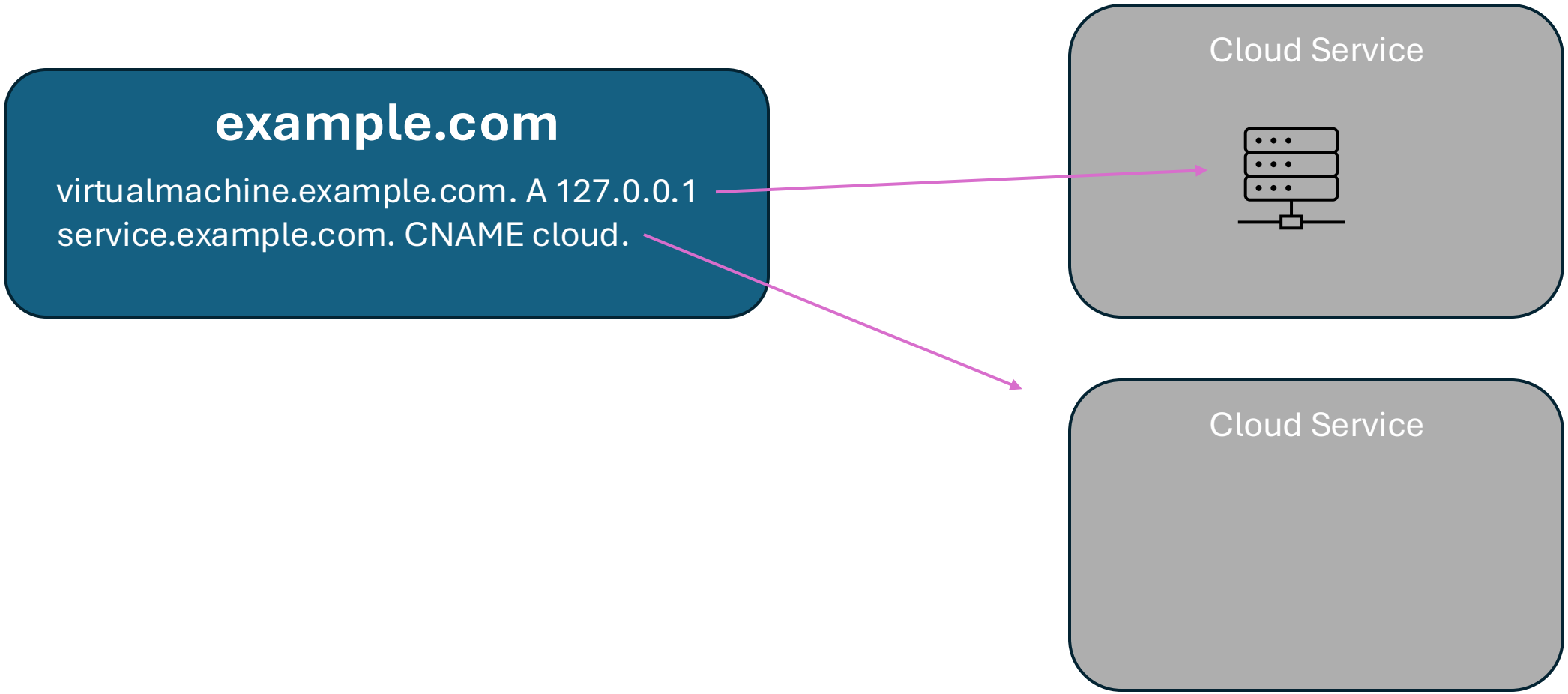
Lame Delegation



Lame Delegation



Dangling records



Subdomain Registration

Subdomain Registration

example.com

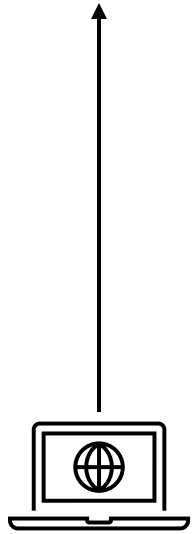
example.com. NS ns1.provider.example.

Provider.example

example.com

ns1.provider.example

example.com



Subdomain Registration

example.com

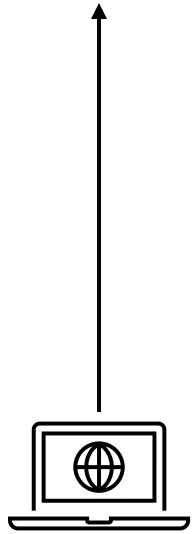
example.com. NS ns1.provider.example.

Provider.example

example.com

ns1.provider.example

example.com



malicious.example.com

Subdomain Registration

example.com

example.com. NS ns1.provider.example.

malicious.example.com

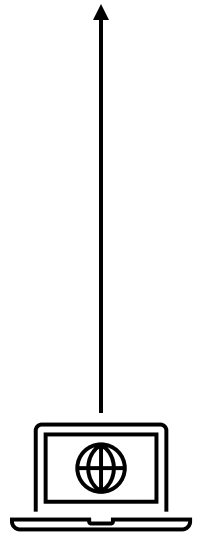
Provider.example

example.com

malicious.example.com

ns1.provider.example

example.com



Subdomain Registration

example.com

example.com. NS ns1.provider.example.

malicious.example.com

Provider.example

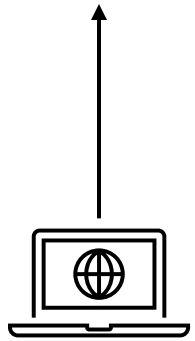
example.com

malicious.example.com

ns1.provider.example

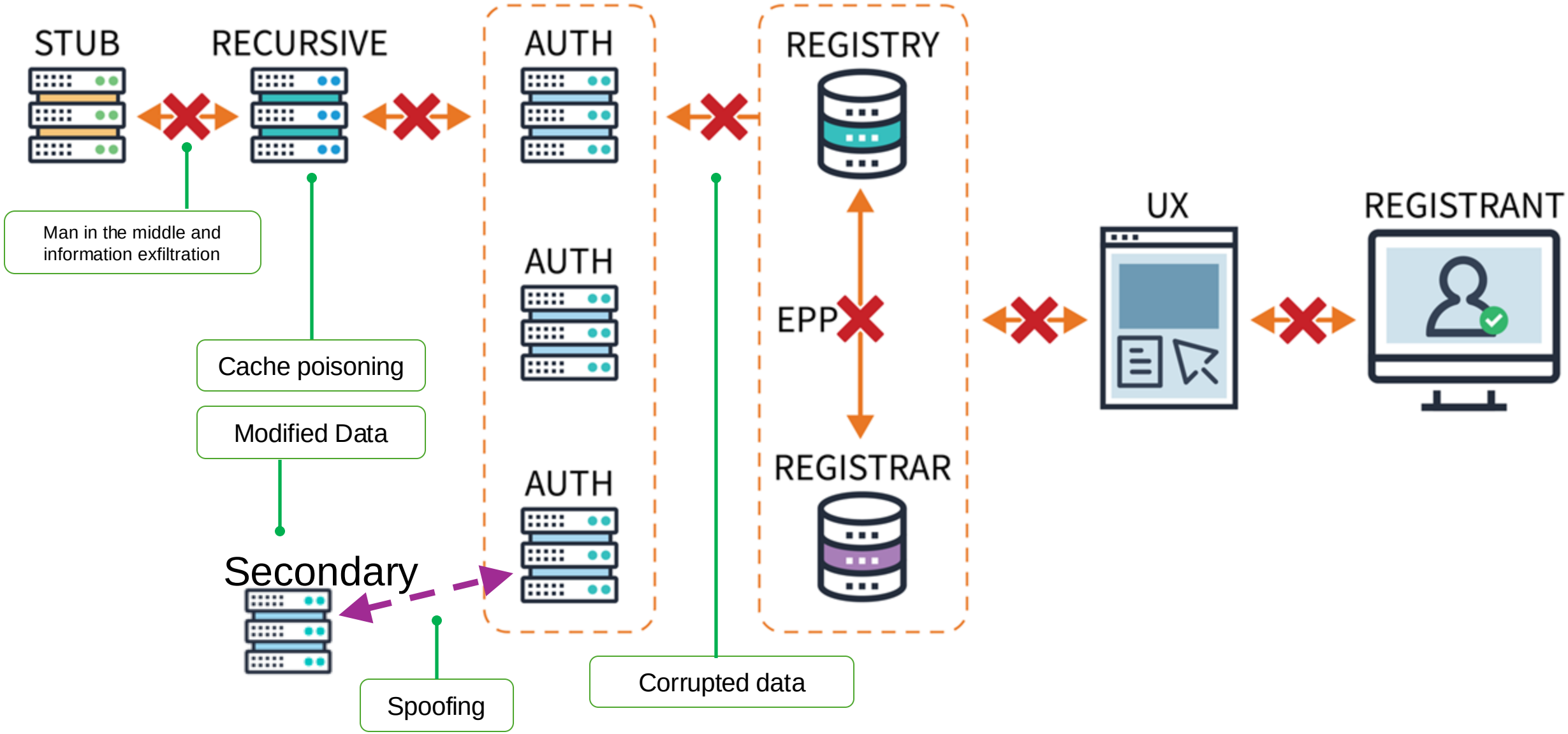
example.com

malicious.example.com



DNS Take-Over

Some of the Potential Target Points of the DNS Ecosystem



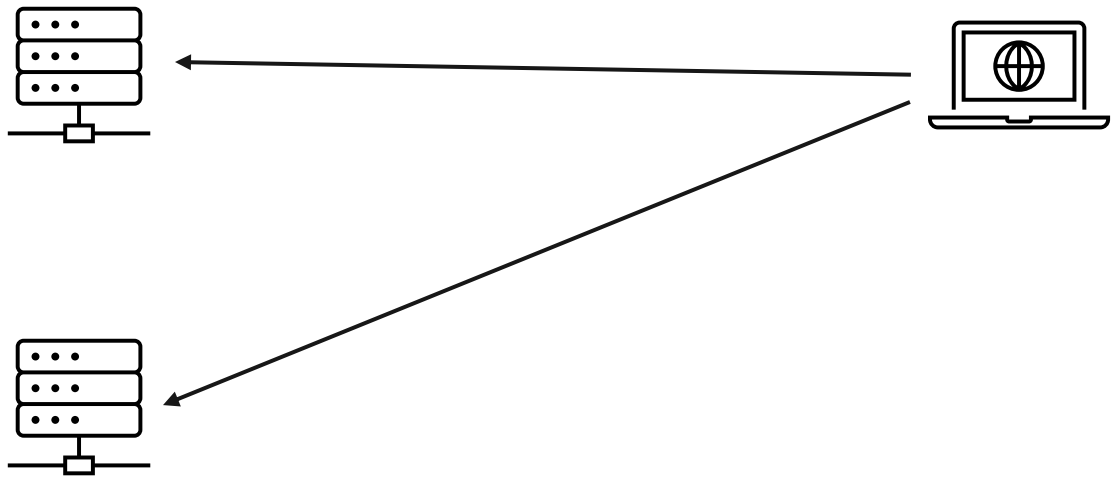
DNS Take-Over

.com

example.com. NS ns1.example.com.
example.com. NS ns2.example.net.

example.com

example.com. NS ns1.example.com.
example.com. NS ns2.example.net.



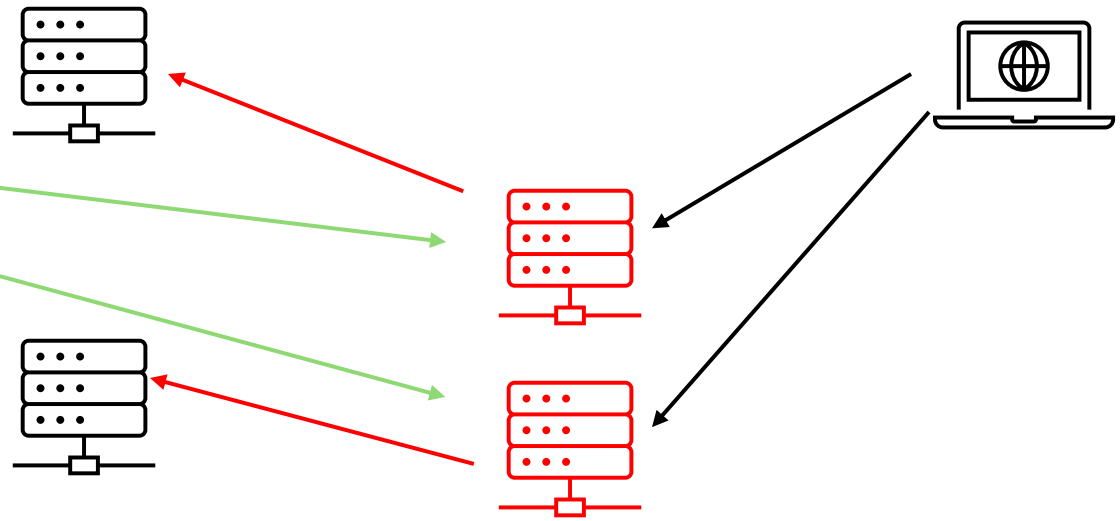
DNS Take-Over

.com

example.com. NS ns1.malicious.example.
example.com. NS ns2.malicious.example.

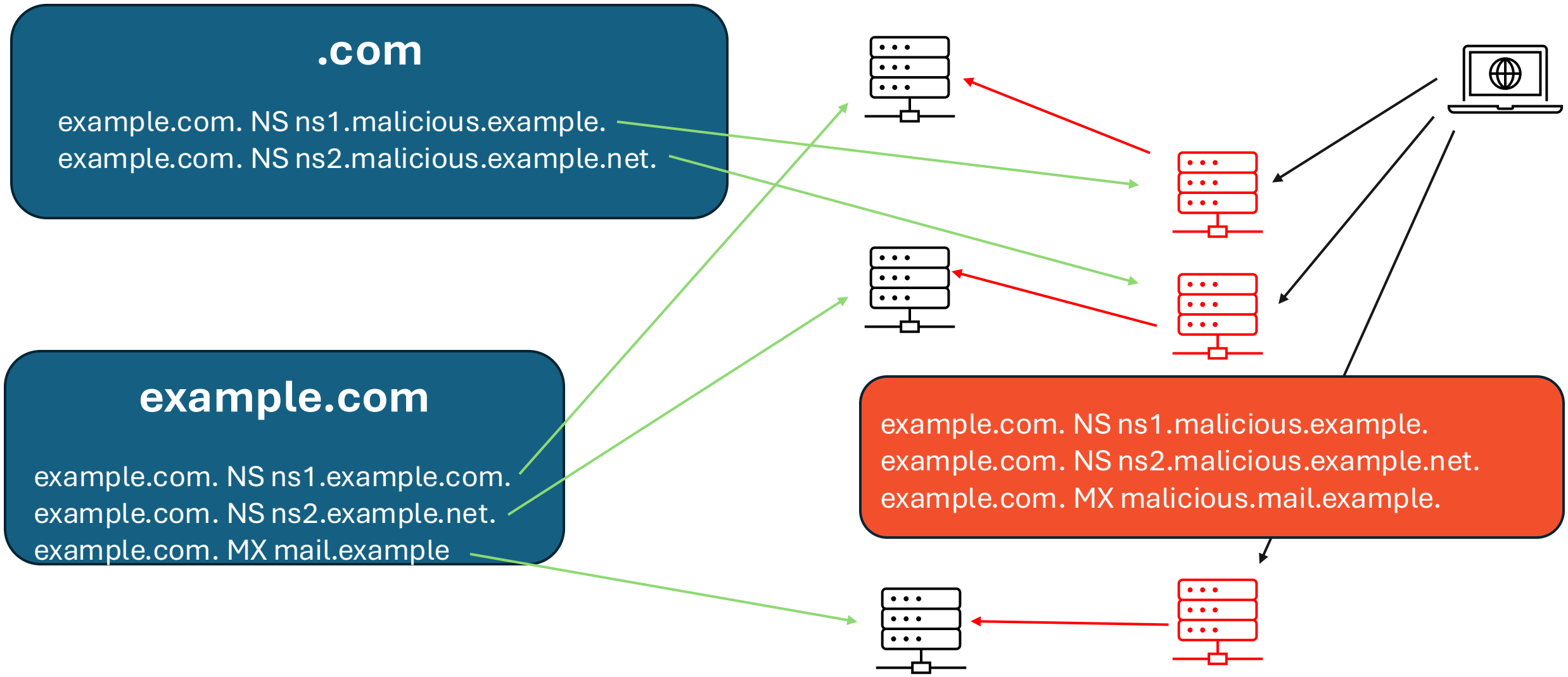
example.com

example.com. NS ns1.example.com.
example.com. NS ns2.example.net.



example.com. NS ns1.malicious.example.
example.com. NS ns2.malicious.example.

DNS Take-Over



Fast-Flux

Fast-Flux

malicious.example

malicious.example. NS ns1.malicious.example.
malicious.example. NS ns2.malicious.example.

www.malicious.example. 5 A 127.0.0.1
www.malicious.example. 5 A 127.0.0.2
www.malicious.example. 5 A 127.0.0.3

ns1.malicious.example. 5 A 127.1.0.1
ns1.malicious.example. 5 A 127.1.0.2
ns1.malicious.example. 5 A 127.1.0.3

ns2.malicious.example. 5 A 127.2.0.1
ns2.malicious.example. 5 A 127.2.0.2
ns2.malicious.example. 5 A 127.2.0.3

Defences

Defences

MONITORING

Defences

DNSSEC

Resolvers

DO

NOT

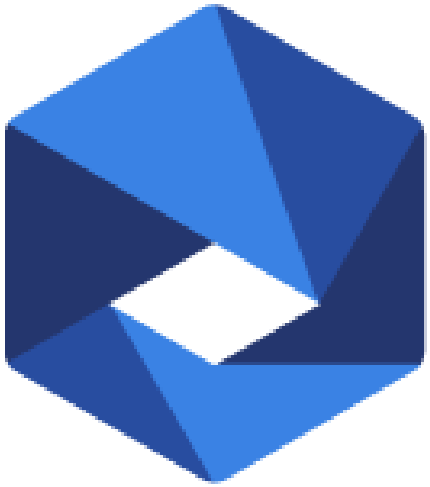
RUN AN

OPEN RESOLVER

PROTECT YOUR RESOLVERS

- Protect all your resolvers from queries from outside
  - This includes resolvers on CPE's which should just resolve the queries from the one customer, not all your customers
- Protect against rebinding
- Protect against Spoofing, do DNSSEC Validation
- Protect against Spoofing, do not disable port or id randomization
- Limit NSEC3 iterations (use updated name server software)
- Offer DNS over HTTPS, DNS over TLS and soon DNS over QUIC
- Consider DNS filtering (could be an extra service)

Best Current Practices



MANRS


KINDNS
KINDNS
KINDNS
ICANN
Follow us on Twitter:
@4KINDNS

KINDNS

An Initiative to Promote DNS Operational Best Practices

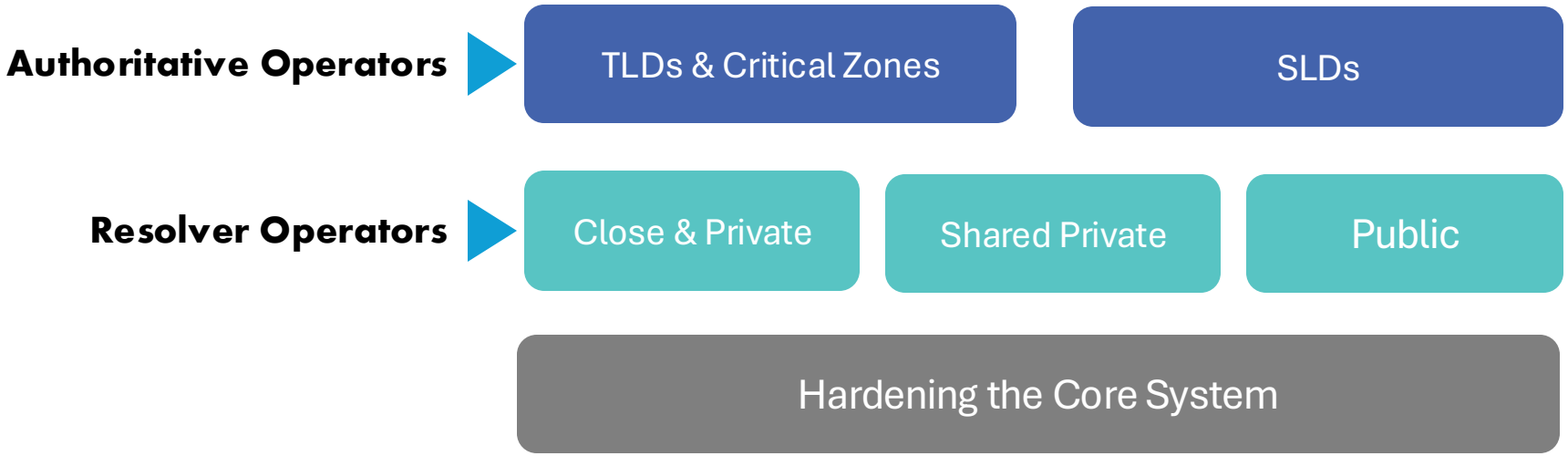
What Is It?

Knowledge-sharing and **I**nstantiating **N**orms for **D**NS
(Domain Name System) and **N**aming **S**ecurity

A simple framework that can help a wide variety of DNS operators, from small to large, to follow both the evolution of the DNS protocol and the best practices that the industry identifies for better security and more effective DNS operations.

***.....** is pronounced "**kindness**"*

Targeted Operators



- Each category has 6-8 practices that we will encourage operators to implement. See www.kindns.org, for more details
- By joining KINDNS, DNS operators are voluntarily committing to adhere to these identified practices and act as "goodwill ambassadors" within the community.

Hardening the Core

In addition to implementing best practices for DNS security and for DNS availability and resilience, all operators must pay ***careful attention to practices for hardening the platforms*** *their DNS services use.*

Core Hardening

1. ACLs **MUST** be implemented to control network traffic to your DNS servers
2. BCP38/MANRS egress filtering **MUST** be implemented
3. The configuration of each DNS server **MUST** be locked down
4. User permissions and application access to system resources **MUST** be limited
5. System and service configuration files **MUST** be versioned
6. Access to management services **MUST** be restricted
7. Access to the system console **MUST** be secured using cryptographic keys and/or two factor authentication mechanism.
8. Credentials Management for customer access **MUST** adhere to best practices

Authoritative DNS Operators of Critical Zones

TLDs & Critical Zones

1. **MUST** be DNSSEC signed and follow key management best practices
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

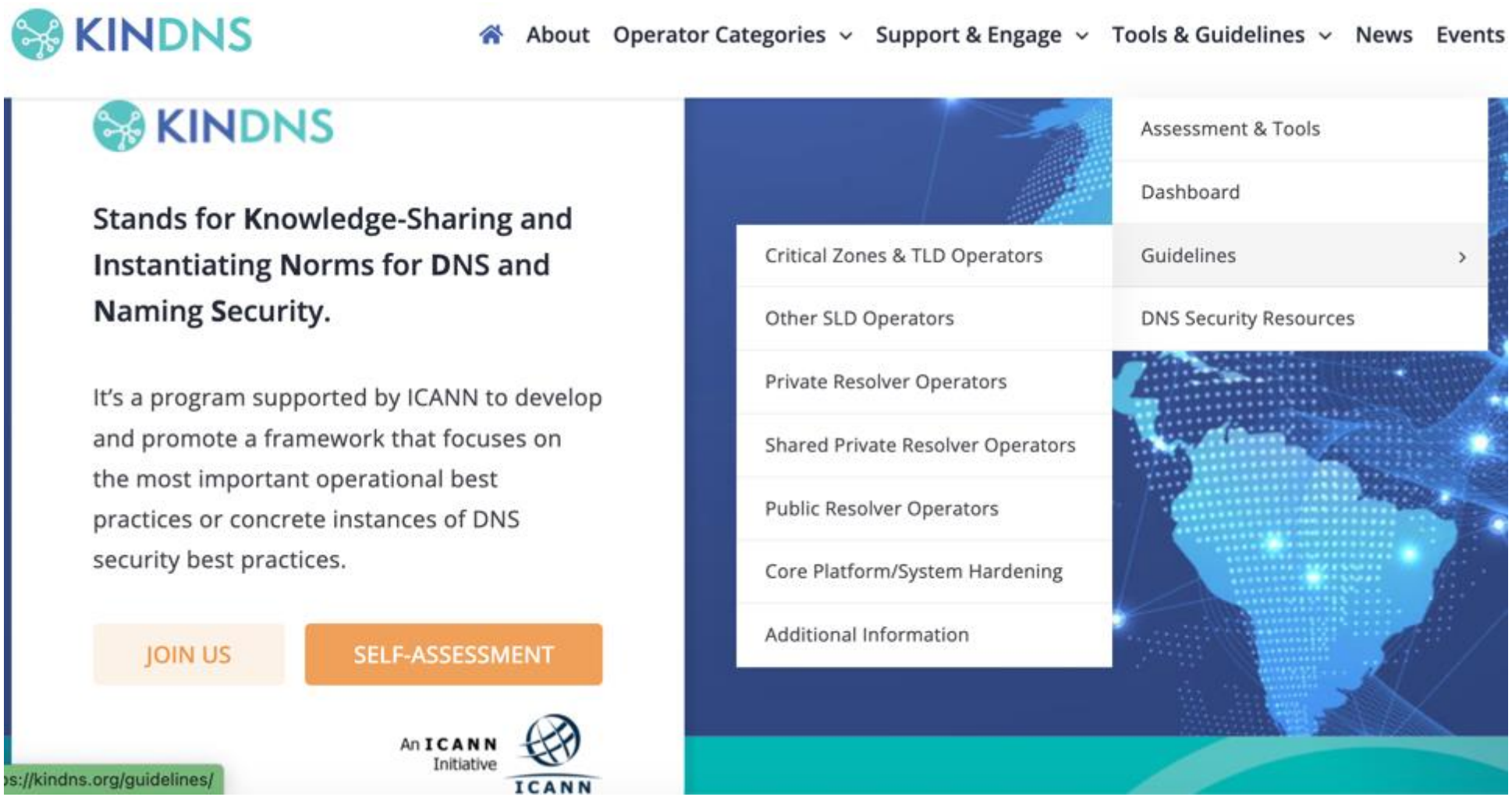
Shared Private Resolver Operators

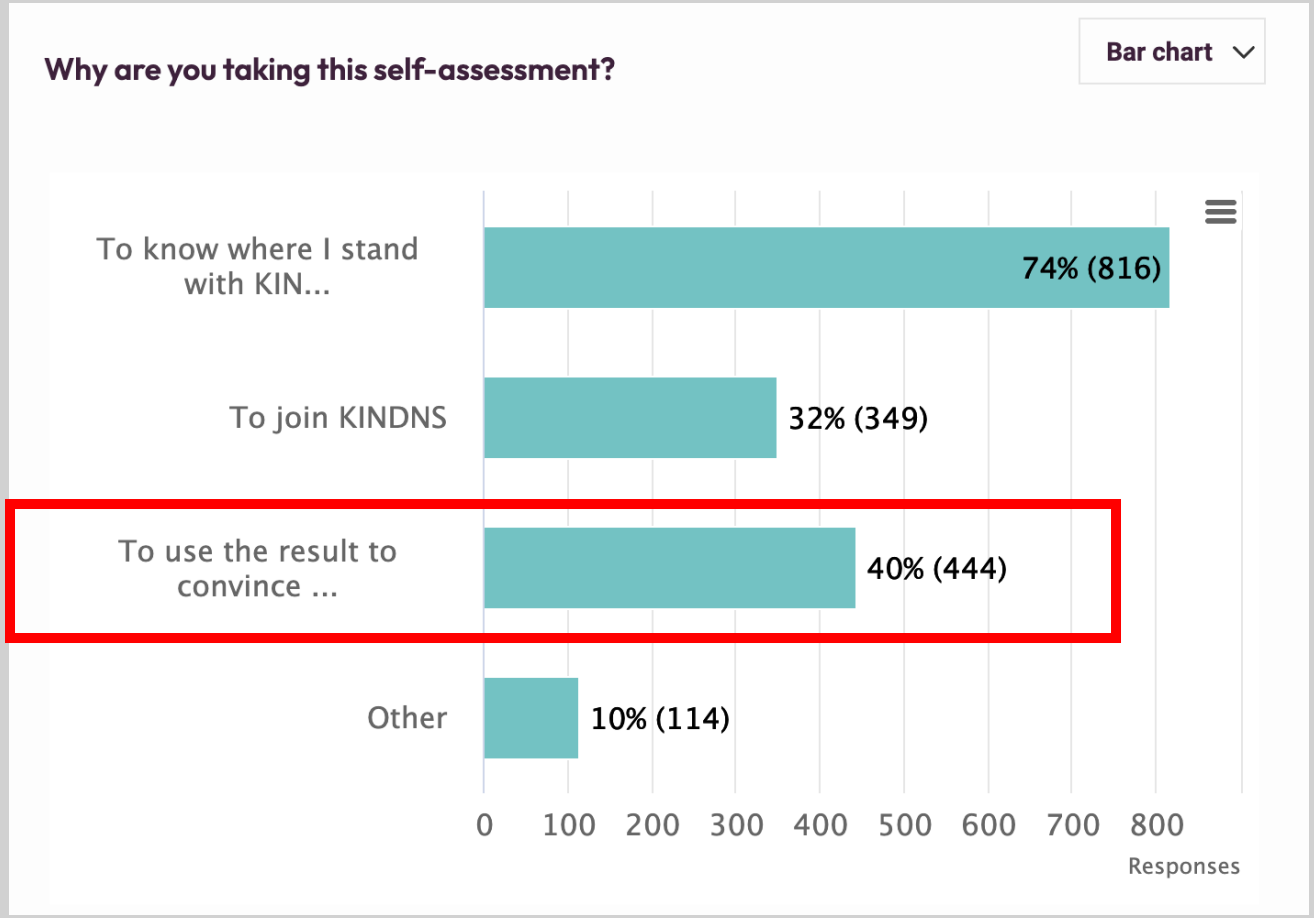
Shared private resolver operators are typically ISPs or similar hosting service providers. They offer DNS resolution services to their customers (mobile, cable/DSL/fiber users, as well as hosted servers and applications).

Shared Private resolvers

1. DNSSEC validation **MUST** be enabled
2. ACL statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that make up your DNS infrastructure **MUST** be monitored
7. For privacy consideration: Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

Practices are documented




Why are you taking this self-assessment?
Bar chart
To know where I stand with KIN...
74% (816)
To join KINDNS
32% (349)
To use the result to convince ...
40% (444)
Other
10% (114)
0
100
200
300
400
500
600
700
800
Responses

Some external additional tools

1. **Zonemaster**: https://zonemaster.net/

   A program that tests a DNS zone configuration with different sanity checks configured in an engine and provides a zone health report.

2. **DNSviz**: https://dnsviz.net/

   Provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and lists configuration errors detected by the tool.

3. **SuperTool**: https://mxtoolbox.com/SuperTool.aspx

   An integrated tool that can perform several kind of diagnostics on a domain name, IP address or host name.

4. **CheckMyDNS**: https://cmdns.dev.dns-oarc.net/

   Check the features and configuration of the resolver your browser uses.

5. **Internet.nl**: https://internet.nl/

   Check DNS, Email and Web for latest security standards

Stay Informed and Contribute

Website	www.kindns.org
Twitter	https://twitter.com/4KINDNS
E-Mail	info@kindns.org
Mailing list	kindns-discuss@icann.org https://mm.icann.org/mailman/listinfo/kindns-discuss