Handling Abuse and Misuse in the DNS

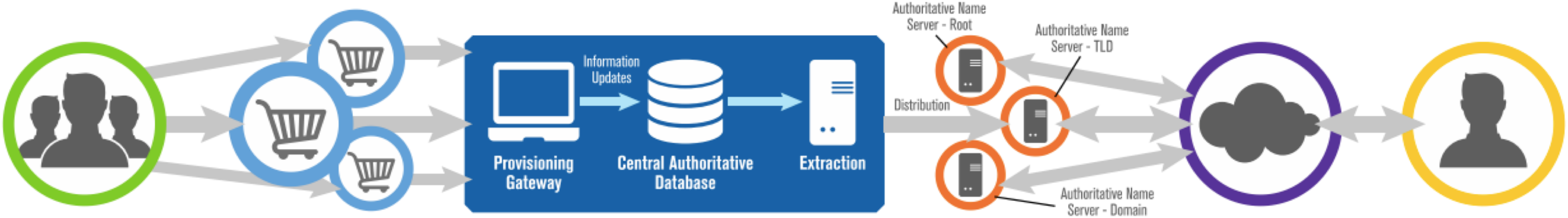
In conjunction with CSNOG2019

Champika Wijayatunga
Regional Security, Stability and Resiliency Engagement Manager – Asia Pacific

29 May 2019

ICANN

The DNS Ecosystem relationships


Information Updates
Provisioning Gateway
Central Authoritative Database
Extraction
Distribution
Authoritative Name Server - Root
Authoritative Name Server - TLD
Authoritative Name Server - Domain

Registrants

Customers who register domain names.

Registrars

Organizations accredited by ICANN that process domain name registrations.

TLD Registry

The registry operator generates the authoritative zone for the TLD and distributes to geographically dispersed name servers.

Name Servers

Name servers respond to queries with the appropriate DNS record for the query.

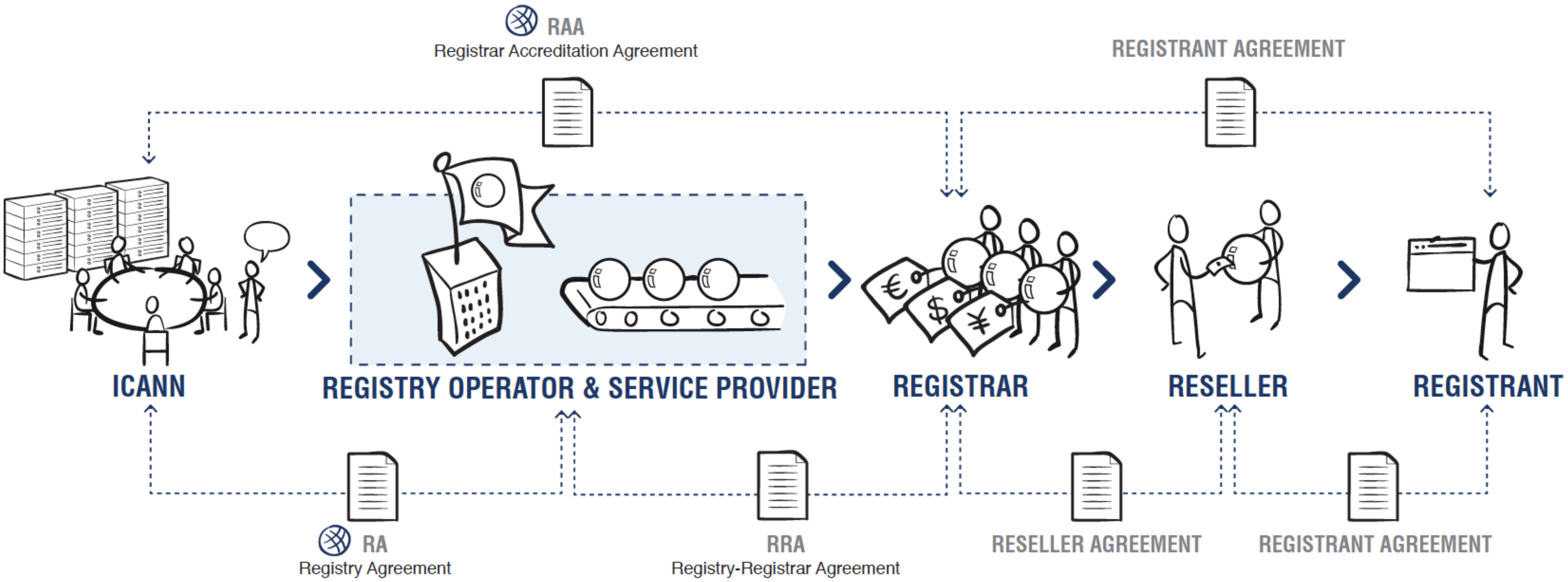
DNS Queries

Recursive name servers send the queries to the authoritative name servers for the TLD.

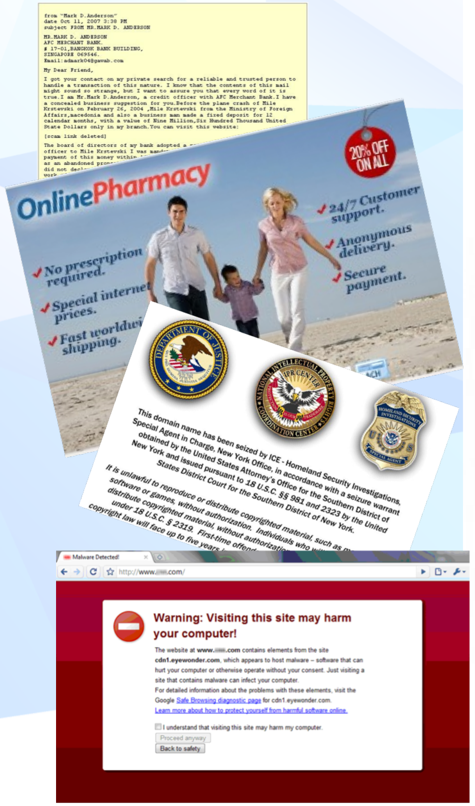
User

The user types a domain name, www.example.com, into a browser. The browser sends the query to recursive name servers in the cloud.

DNS Ecosystem - Contractual relationships



Maliciously Registered Domain Names



```
from "Mark D.Anderson"
date Oct 11, 2007 3:38 PM
subject FROM MR.MARK D. ANDERSON

MR.MARK D. ANDERSON
AFC MERCHANT BANK.
# 17-01,BANGKOK BANK BUILDING,
SINGAPORE 069546.
Email:admark04@gavab.com

My Dear Friend,

I got your contact on my private search for a reliable and trusted person to
handle a transaction of this nature. I know that the contents of this mail
might sound so strange, but I want to assure you that every word of it is
true.I am Mr.Mark D.Anderson, a credit officer with AFC Merchant Bank.I have
a concealed business suggestion for you.Before the plane crash of Mile
Krstevski on February 26, 2004 ,Mile Krstevski from the Ministry of Foreign
Affairs,macedonia and also a business man made a fixed deposit for 12
calendar months, with a value of Nine Million,Six Hundred Thousand United
State Dollars only in my branch.You can visit this website:

[scam link deleted]

The board of directors of my bank adopted a
officer to Mile Krstevski I was mand
payment of this money within
as an abandoned prop
did not decl
work
```

This domain name has been seized by ICE - Homeland Security Investigations, Special Agent in Charge, New York Office, in accordance with a seizure warrant obtained by the United States Attorney's Office for the Southern District of New York and issued pursuant to 18 U.S.C. §§ 981 and 2323 by the United States District Court for the Southern District of New York.

It is unlawful to reproduce or distribute copyrighted material, such as m software or games, without authorization. Individuals who w distribute copyrighted material, without authorizatio under 18 U.S.C. § 2319. First-time offend copyright law will face up to five years

Warning: Visiting this site may harm your computer!

The website at **www.[redacted].com** contains elements from the site **cdn1.eyewonder.com**, which appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that contains malware can infect your computer.

For detailed information about the problems with these elements, visit the Google Safe Browsing diagnostic page for cdn1.eyewonder.com.

Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer.

- Domains registered by criminals for
  - Counterfeit goods
  - Data exfiltration
  - Exploit attacks
  - Illegal pharma
  - Infrastructure (ecrime name resolution)
  - Malware C&C
  - Malware distribution, ransomware
  - Phishing, Business Email Compromise
  - Scams (419, reshipping, stranded traveler…)

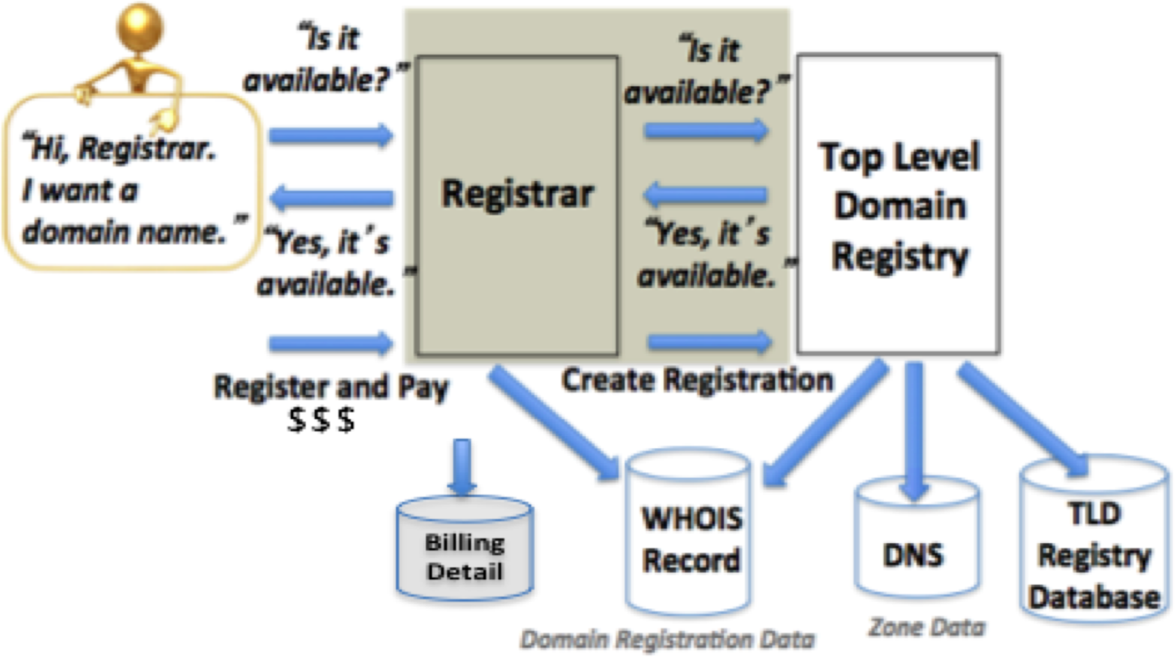
Misused Domain Registrations

- Domains compromised or hijacked by criminals or state-sponsored actors
  - Host criminal DNS infrastructure
  - Domain, NS, or MX Hijacking
  - Hacktivism (e.g., defacement)
  - Tunneling (covert communications)
  - Data Exfiltration
  - Methods
    - Infection (Malware)
    - Configuration change (DNSChanger)
    - Poisoning (resolver/ISP)
    - Man in the Middle attacks

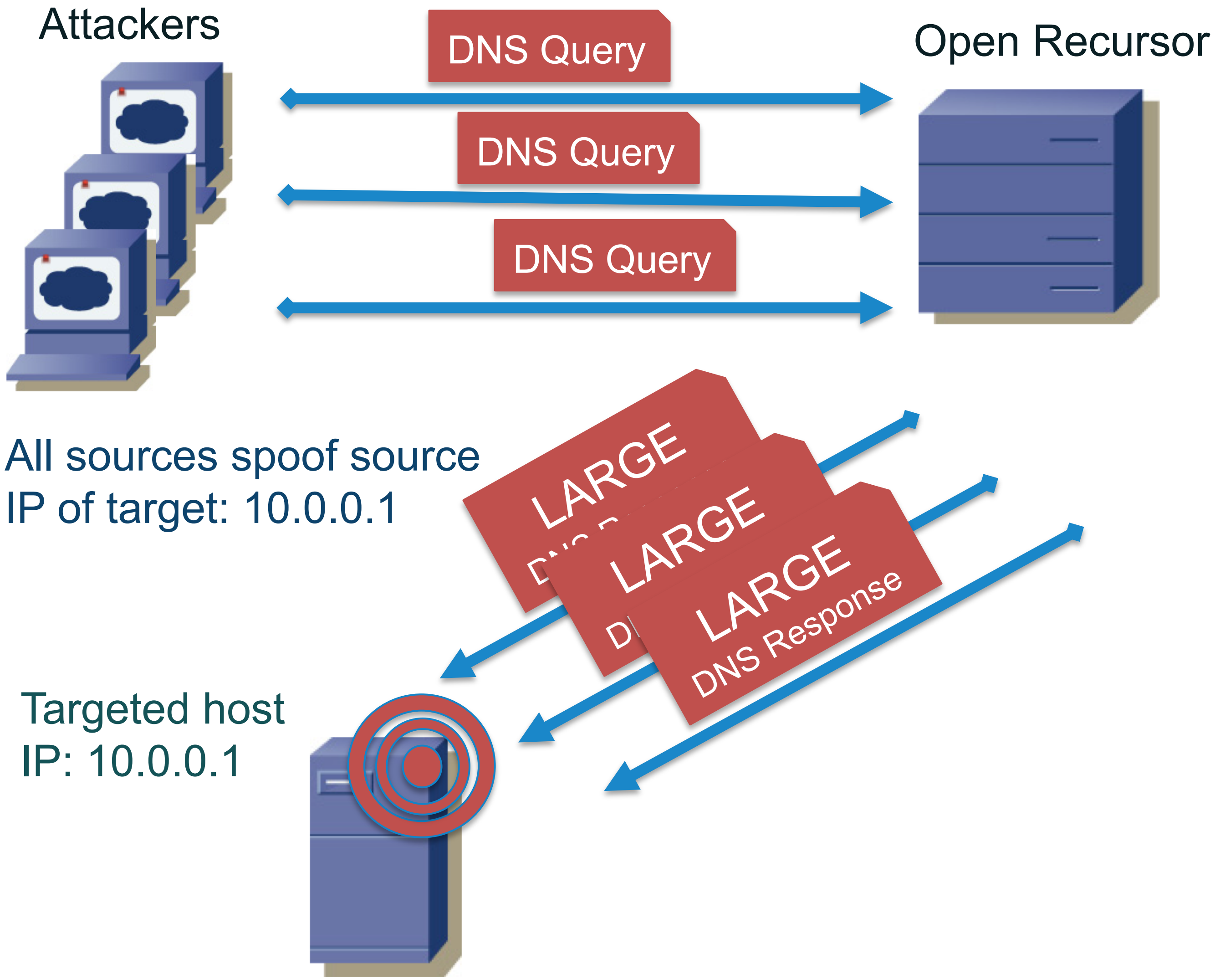
Domain name registrations are attractive targets for attacks

- Process is automated and rapidly provisioned
- Registrar correspondence with registrants is largely email
- Registrant is responsible for registration data accuracy
- Inexpensive registrations are plentiful…

  Good for consumers, good for attackers, too



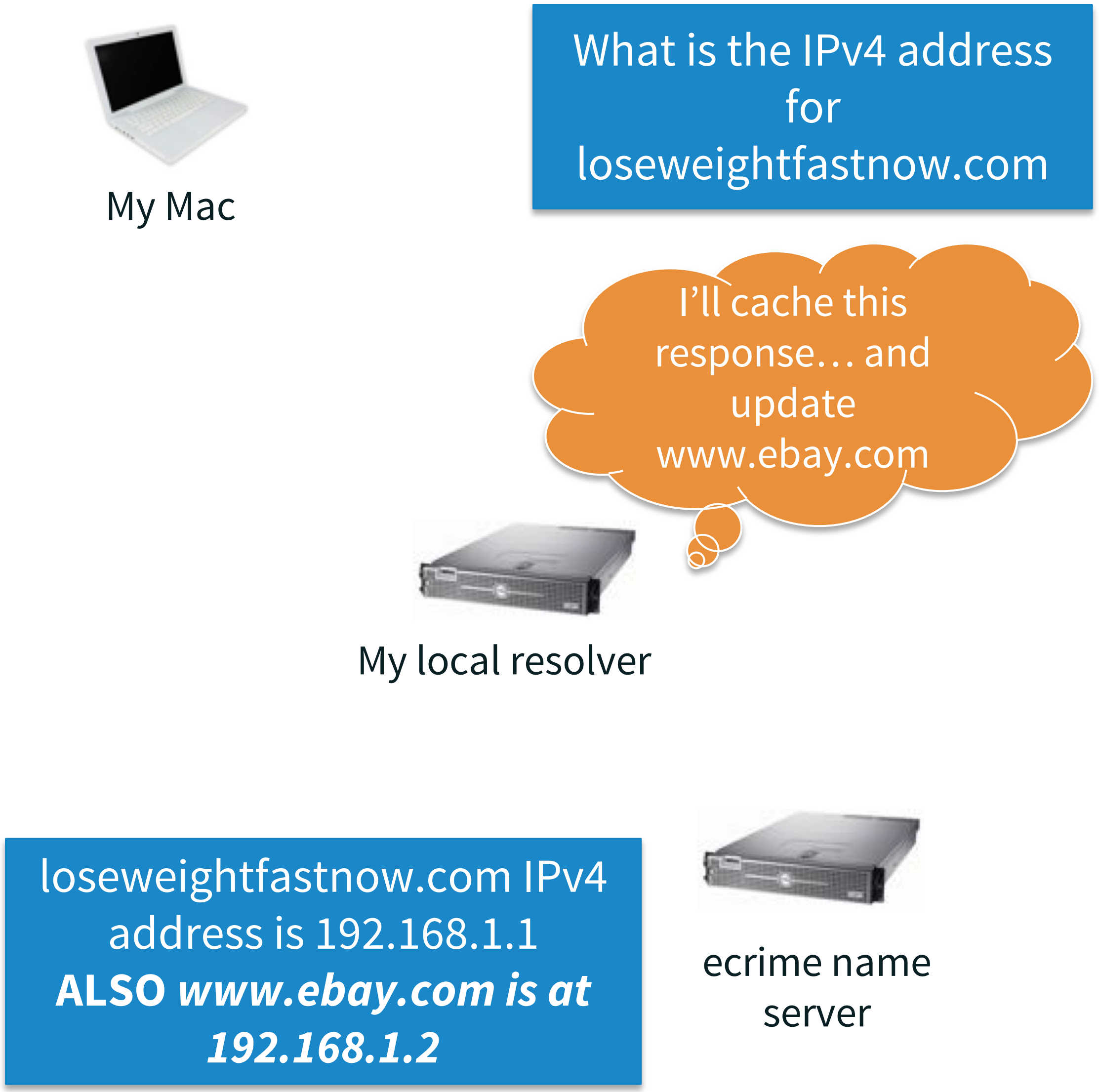
Distributed reflection and amplification attack (DDoS)



- Launch reflection and amplification attack from 1000s of origins
- Each origin uses the target's IP address as its source address
- Reflect through open recursor
- Deliver 1000s of large responses to target

Poisoning a Cache

- Attacker launches a spam campaign where spam message contains http://loseweightfastnow.com
- Attacker's name server will respond to a DNS query for loseweightnow.com with additional malicious data about ebay.com
- Vulnerable resolvers add malicious data to local caches
- The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry



My Mac

What is the IPv4 address for loseweightfastnow.com

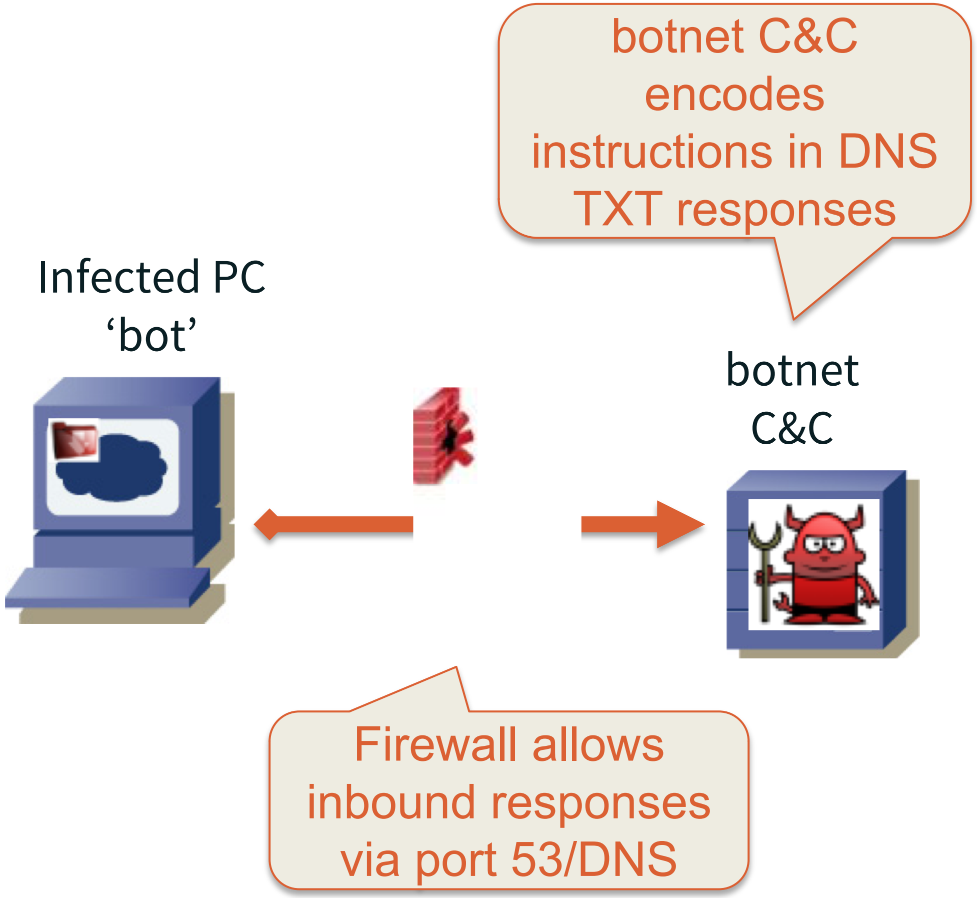
I'll cache this response… and update www.ebay.com

My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1
ALSO *www.ebay.com is at 192.168.1.2*

ecrime name server

DNS as a Covert Malware Channel

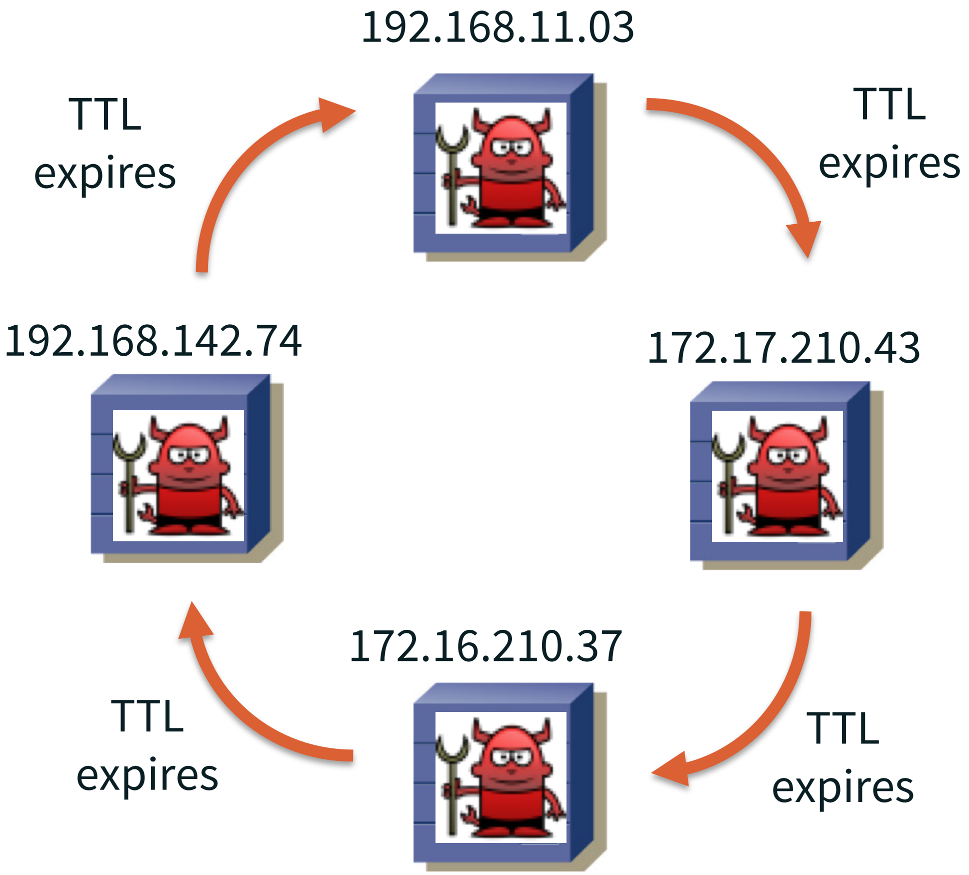

botnet C&C encodes instructions in DNS TXT responses
Infected PC 'bot'
botnet C&C
Firewall allows inbound responses via port 53/DNS

- Malware on infected PC performs TXT lookups to botnet C&C
- TXT responses contain instructions or executables for bot
- Examples in wild:
  - Feederbot
  - Morto

Using the DNS to evade, obfuscate, and make networks agile

- In fast flux, the attackers
  - Associate IP address with a web proxy or nameserver for short time to live (TTL)
  - Then changes IP of host or name server at low TTL frequency to thwart investigators

- In double (fast) flux attacks, they
  - Apply fast flux technique to both web proxy and name server

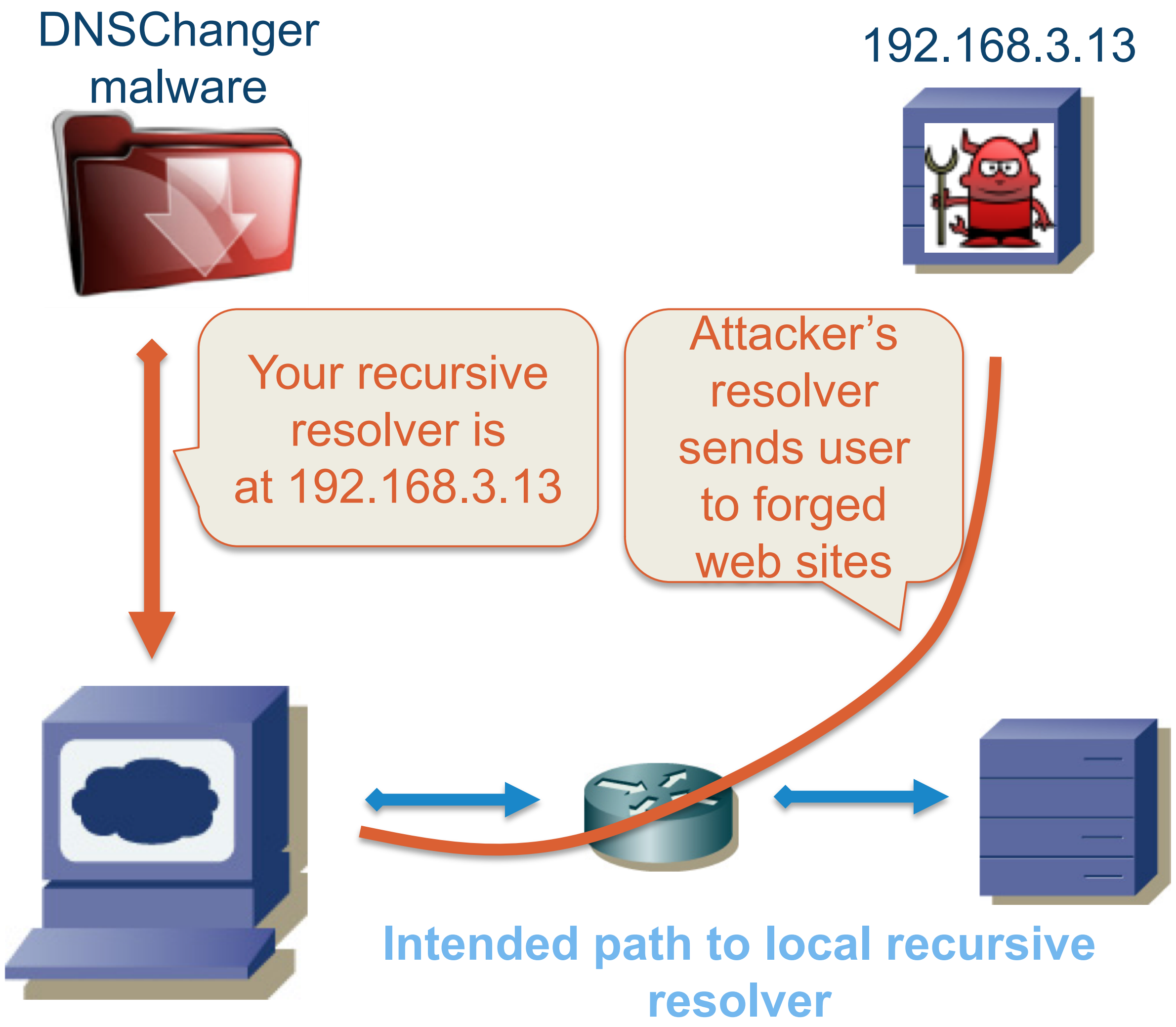


Poisoning a host (DNSChanger)

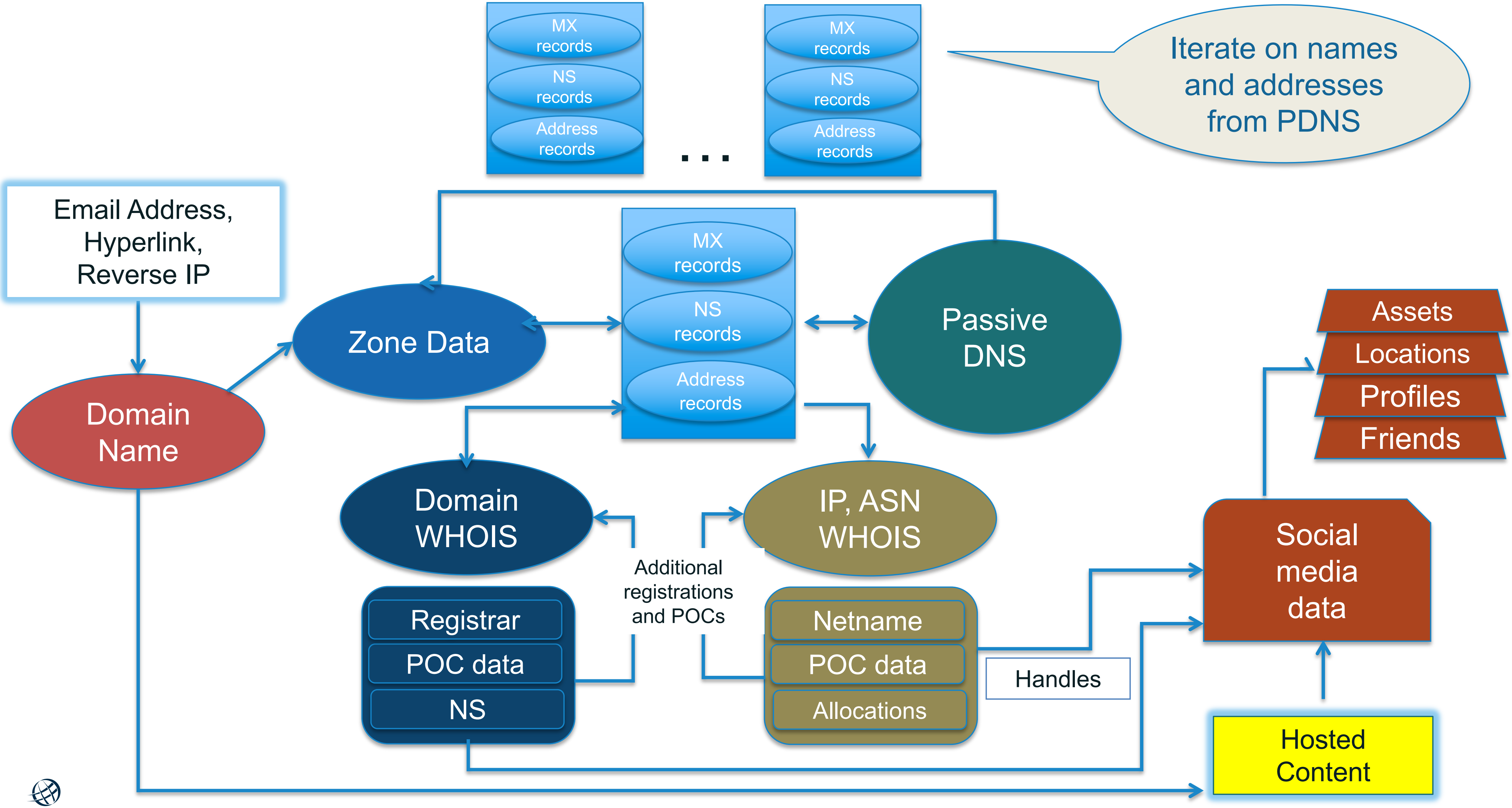
1) The attacker distributes DNS configuration altering malware via
   a) Spam, drive-by download…
   b) *Example: DNSChanger* malware

2) Attacker alters DNS configuration of infected PC to cause all requests to go to a malicious nameserver run by attackers

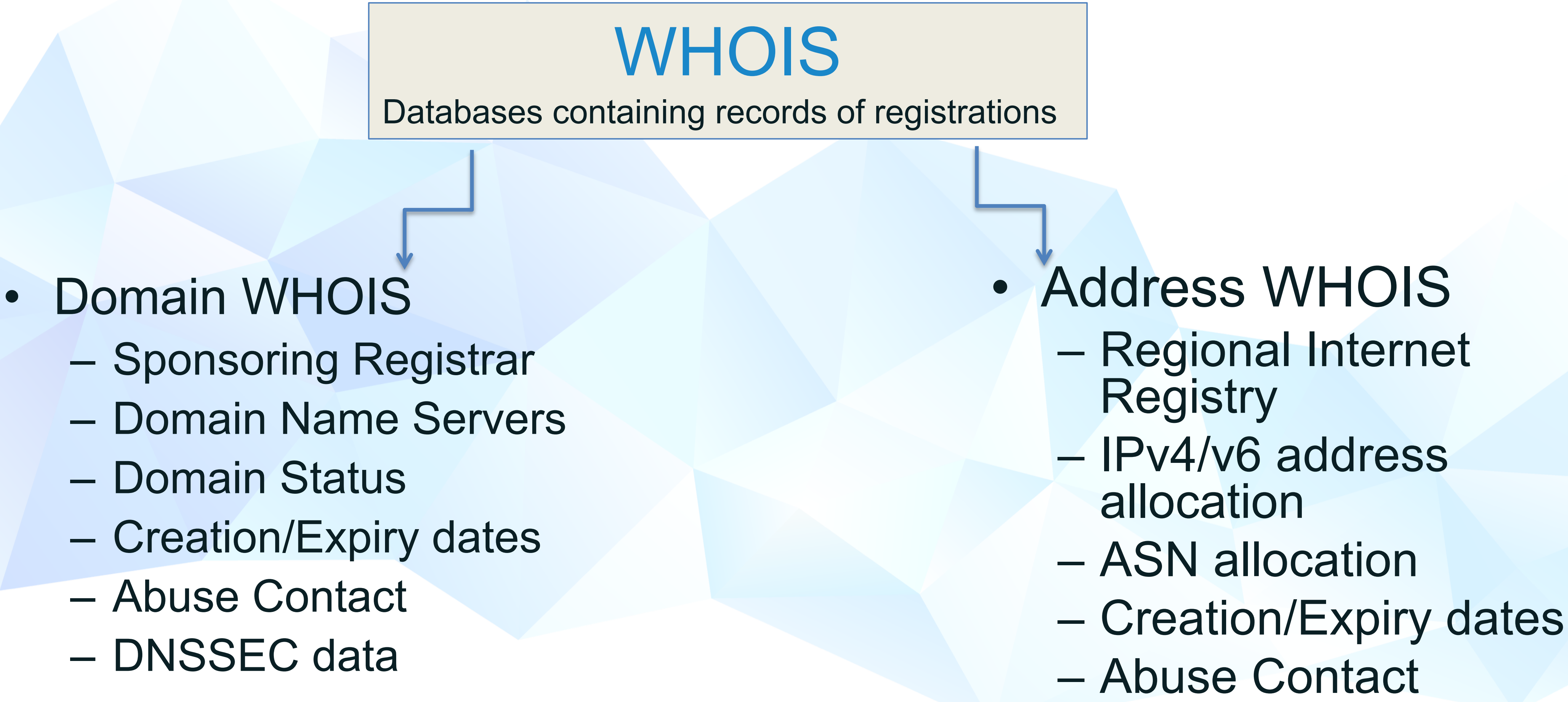
3) Local DNS cache redirects web traffic to a destination of his choosing


DNSChanger malware
192.168.3.13
Your recursive resolver is at 192.168.3.13
Attacker's resolver sends user to forged web sites
Intended path to local recursive resolver

Knowledge gathering to handle DNS abuse



Registration Data Directory Service



WHOIS

Databases containing records of registrations

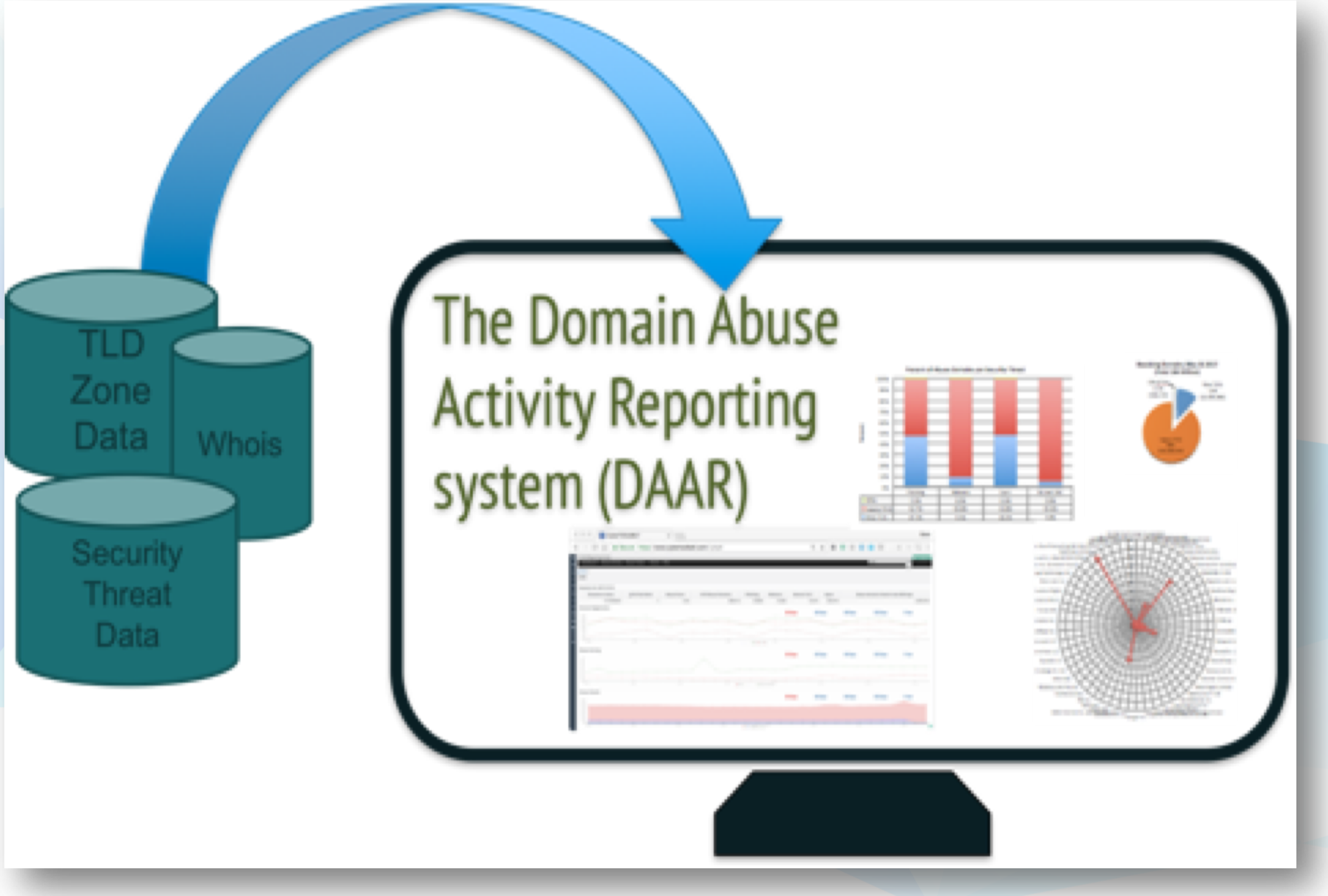
- Domain WHOIS
  - Sponsoring Registrar
  - Domain Name Servers
  - Domain Status
  - Creation/Expiry dates
  - Abuse Contact
  - DNSSEC data

- Address WHOIS
  - Regional Internet Registry
  - IPv4/v6 address allocation
  - ASN allocation
  - Creation/Expiry dates
  - Abuse Contact

Steps to handle domain abuses

1. Collect evidence of abuse
2. Determine hosting provider or registrar
   A. Is there a reseller of that registrar involved?
3. Contact hosting provider or registrar abuse desk
   A. Provide evidence of abuse
   B. Point out registration or content problems
   C. Ask if a TOS, ICANN, ccTLD registry domain suspension policy applies
4. No success? Contact registry
   A. Same supporting info as registrar
5. Escalate
   A. Sharing/intel networks
   B. National CERT or local LE
   C. WHOIS Data Problem Reporting System
   D. ICANN compliance

If you are looking at a suspicious domain, someone else is, too.



The Domain Abuse Activity Reporting system (DAAR)

The Domain Abuse Activity Reporting system

A system for reporting on domain name registration and abuse data across TLD registries and registrars

How does DAAR differ from other reporting systems?

- Studies all gTLD registries and registrars for which we can collect zone and registration data
- Employs a large set of reputation feeds (e.g., blocklists)
- Accommodates historical studies
- Studies multiple threats: phishing, botnet, malware, spam
- Takes a scientific approach: transparent, reproducible

Project Goals

- DAAR data can be used to
  - Report on threat activity at TLD or registrar level
  - Study histories of security threats or domain registration activity
  - Help operators understand or consider how to manage their reputations, their anti-abuse programs, or terms of service
  - Study malicious registration behaviors
  - Assist operational security communities

The purpose of DAAR is to provide data to support community, academic, or sponsored research and analysis for informed policy consideration

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann