DNS/DNSSEC

In conjunction with APRICOT2020

Champika Wijayatunga
Regional Technical Engagement Manager – Asia Pacific

12-16 Feb 2020, Melbourne – Australia

Agenda

- DNS Recap
- Setting up Authoritative and Recursive Servers
- DNS Security concepts
- DNS Security Extensions (DNSSEC)
- Transaction Signatures (TSIG)
- DNSSEC Key Management
- Reverse DNS

DNS Security

Common Uses for Maliciously Registered Domains

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…)

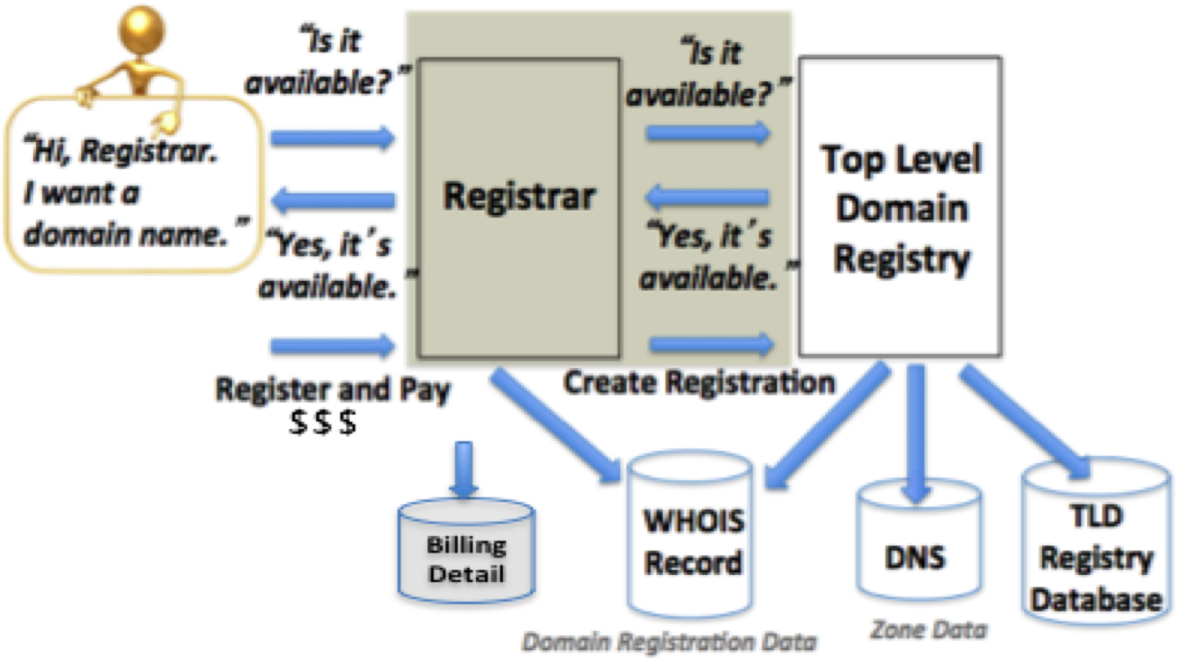
Misused Domain Registrations

Domains compromised or hijacked by criminals or state-sponsored actors

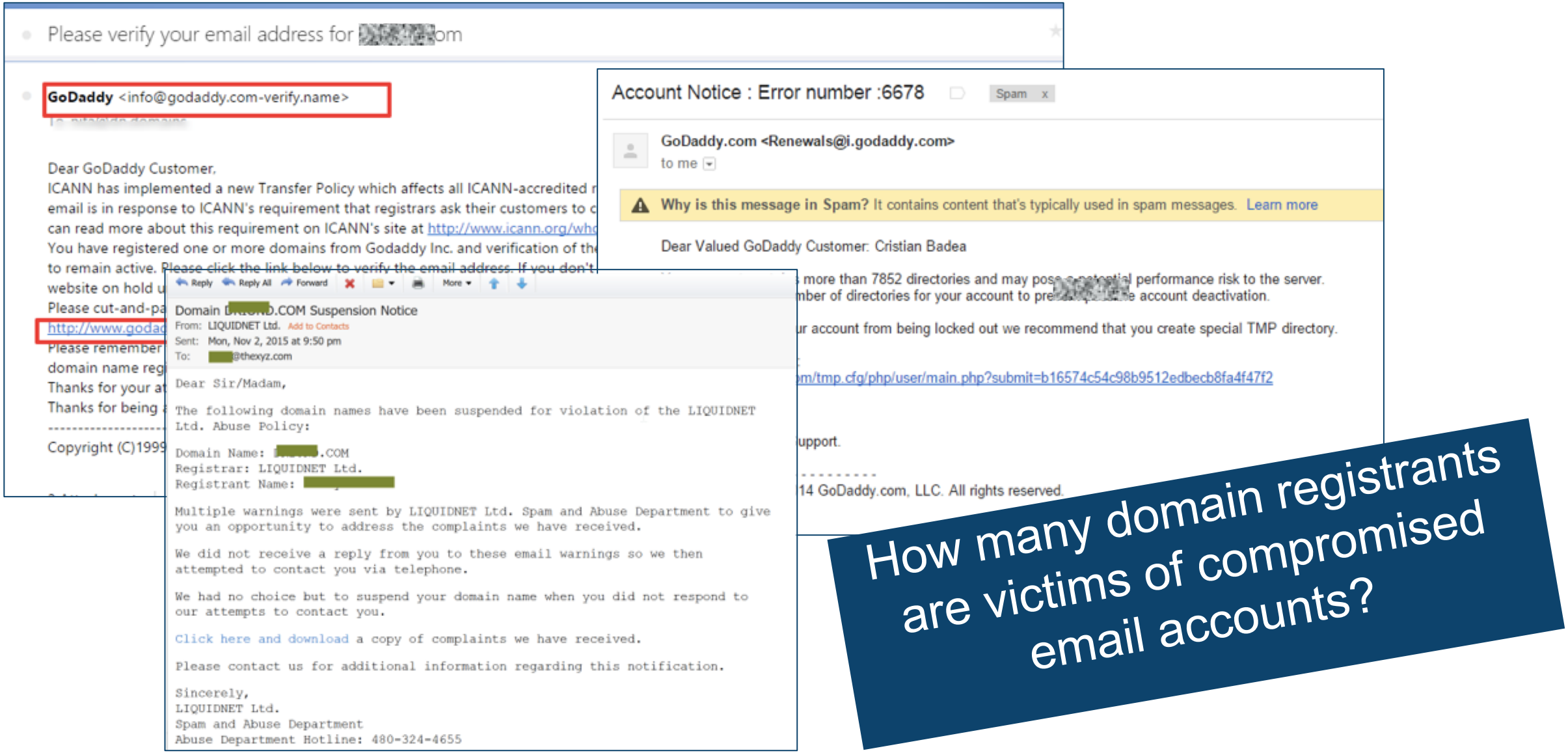
- Host criminal DNS infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Malware (infected devices)
- Changing default resolvers (DNSChanger)
- Poisoning (resolver/ISP)
- Man in the Middle attacks

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

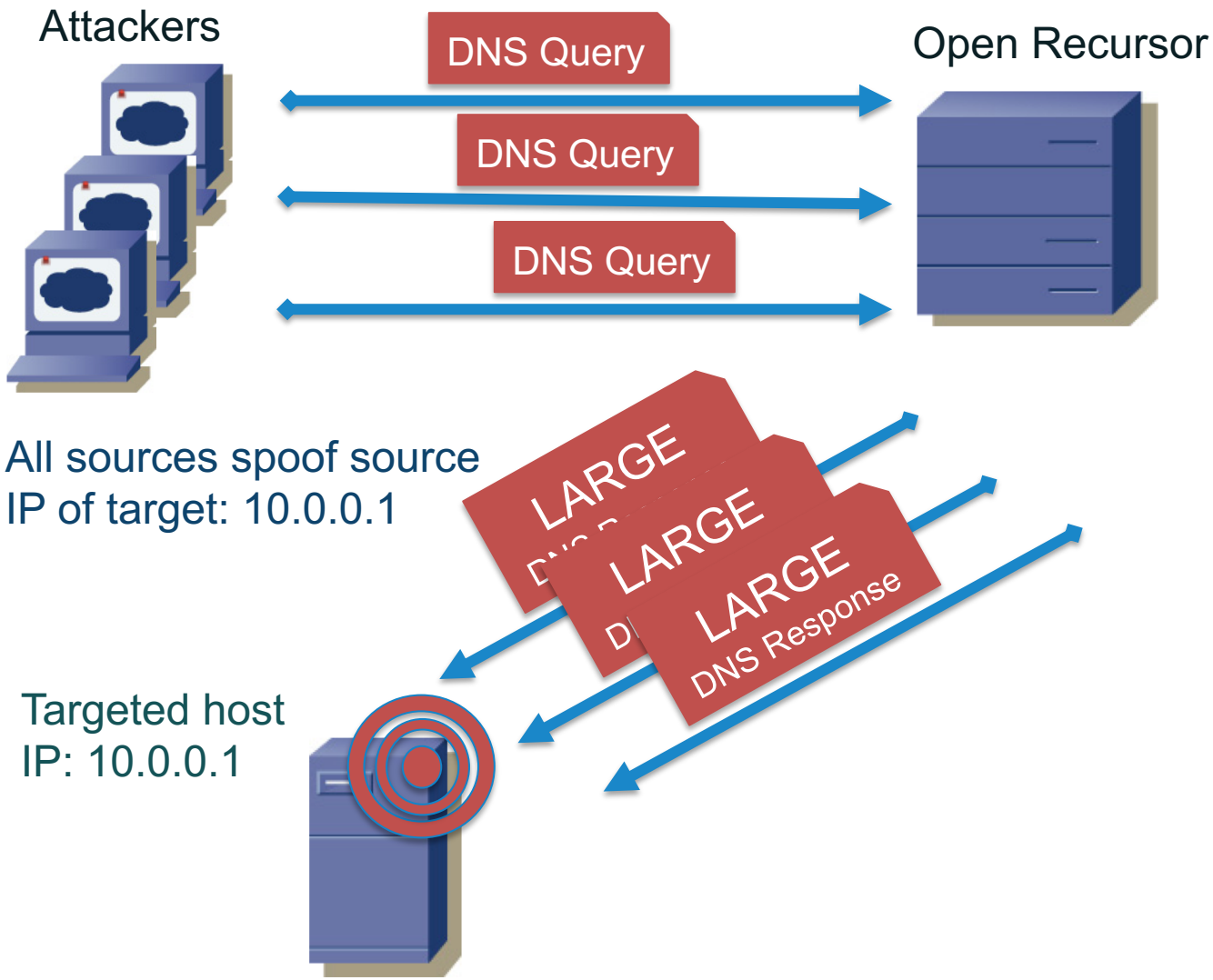


Criminals exploit registrar email correspondence (Phishing)



How many domain registrants are victims of compromised email accounts?

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

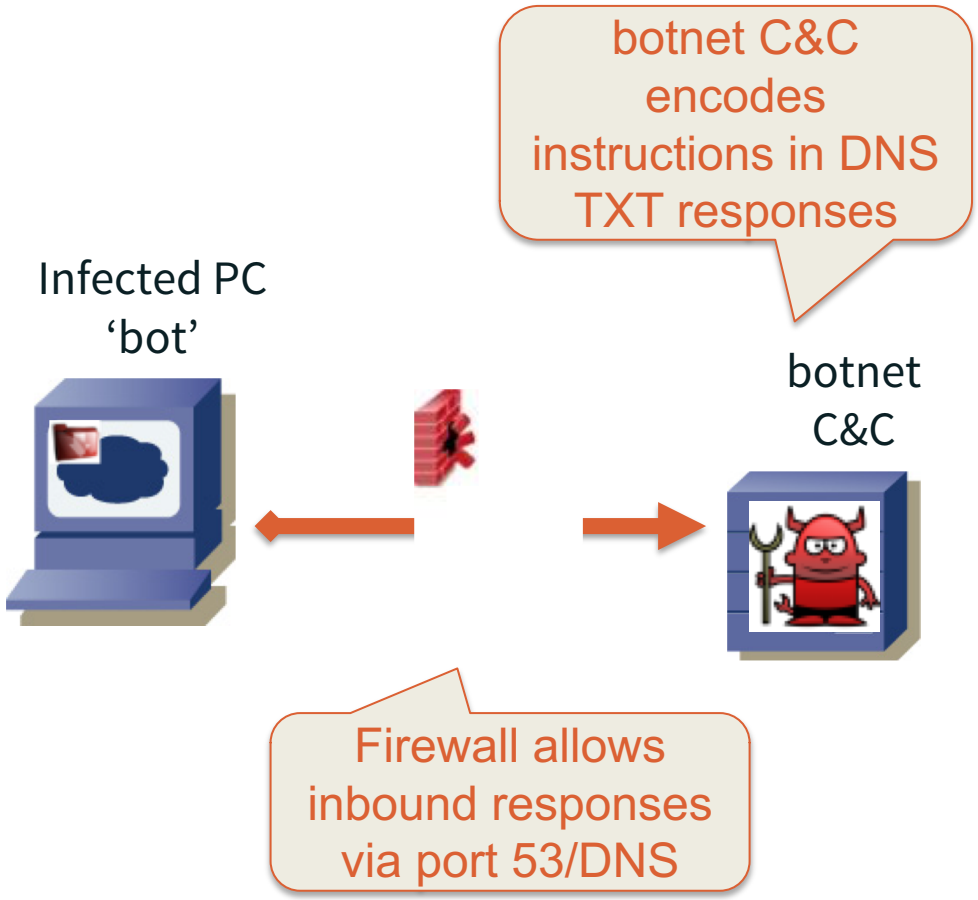
I'll cache this response… and update www.ebay.com

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



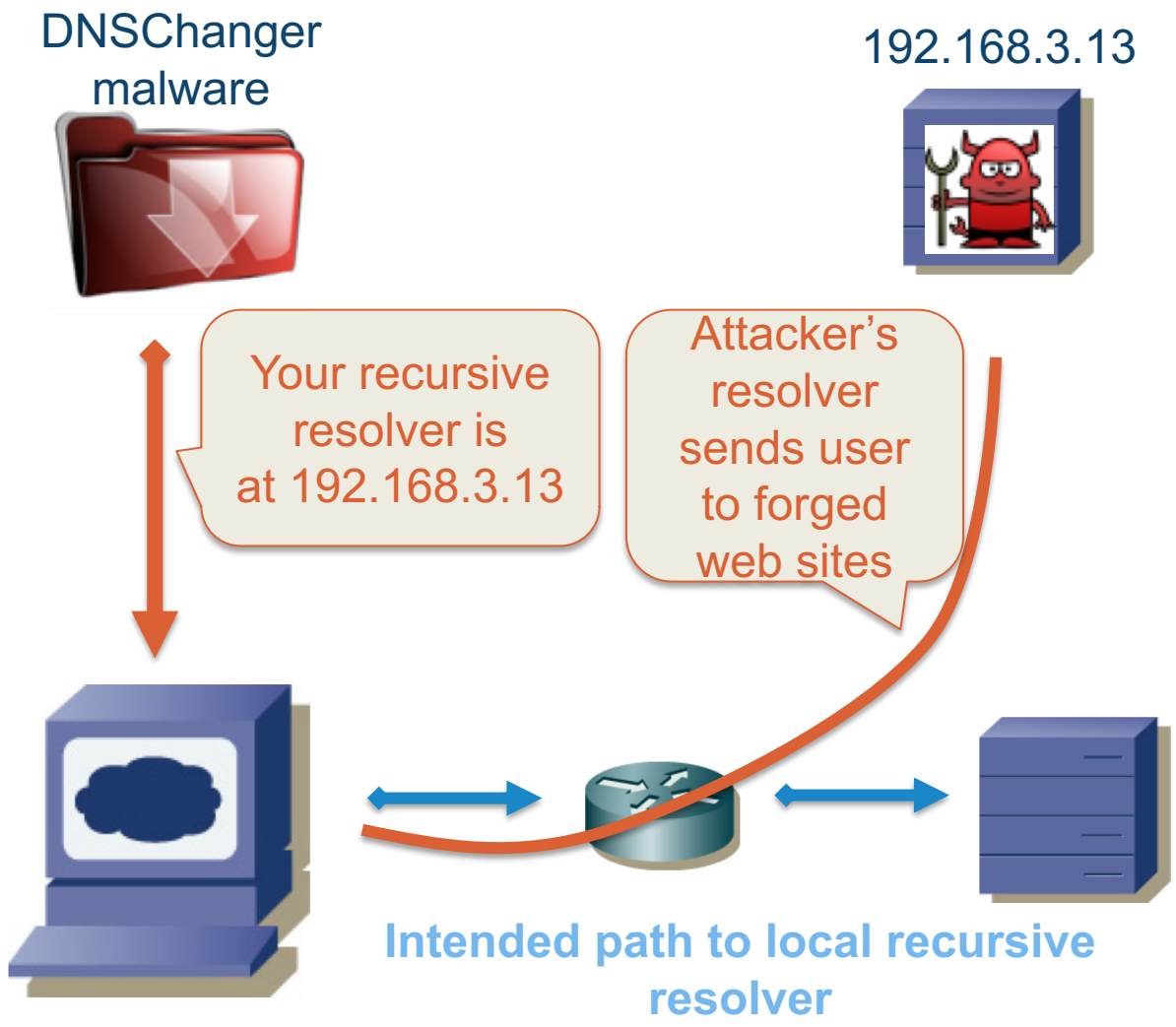
- Malware on infected PC performs TXT lookups to botnet C&C
- TXT responses contain instructions or executables for bot
- Examples in wild:
  - Feederbot
  - Morto

Poisoning a host (DNSChanger)

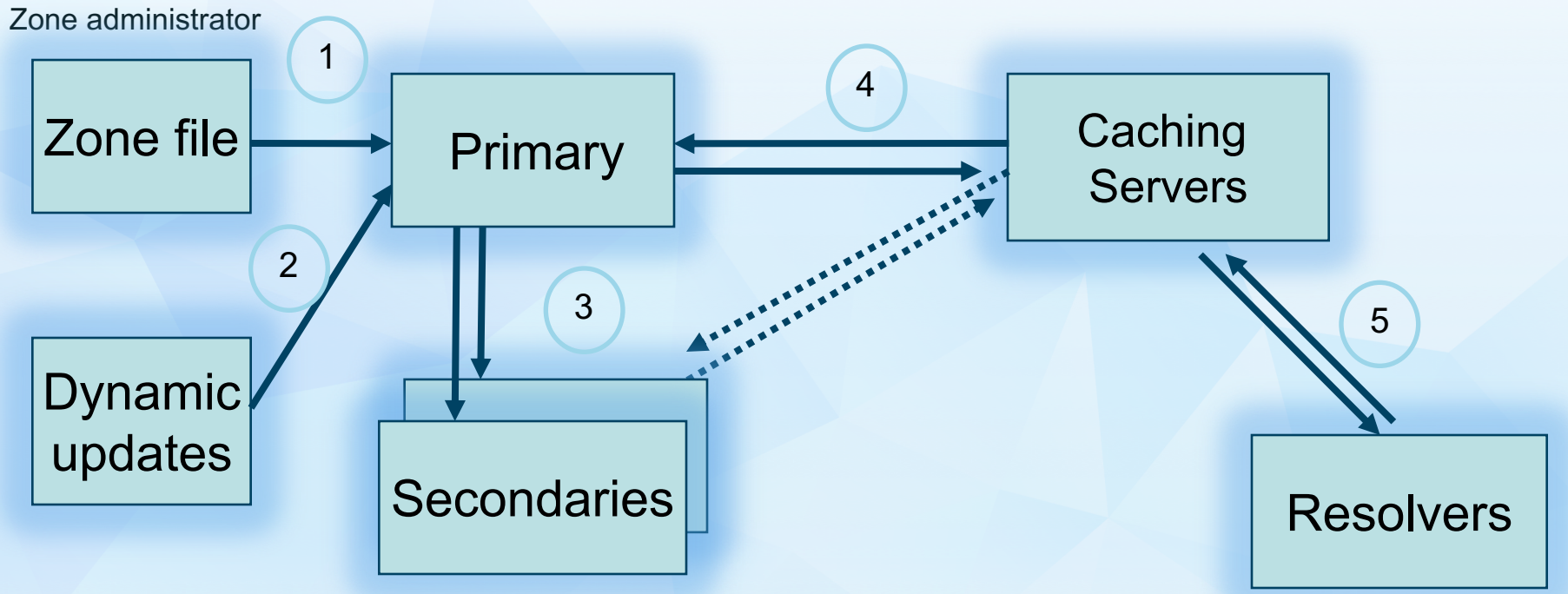
1) The attacker distributes DNS configuration altering malware via
   a) Spam, drive-by download…
   b) Example: DNSChanger malware

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

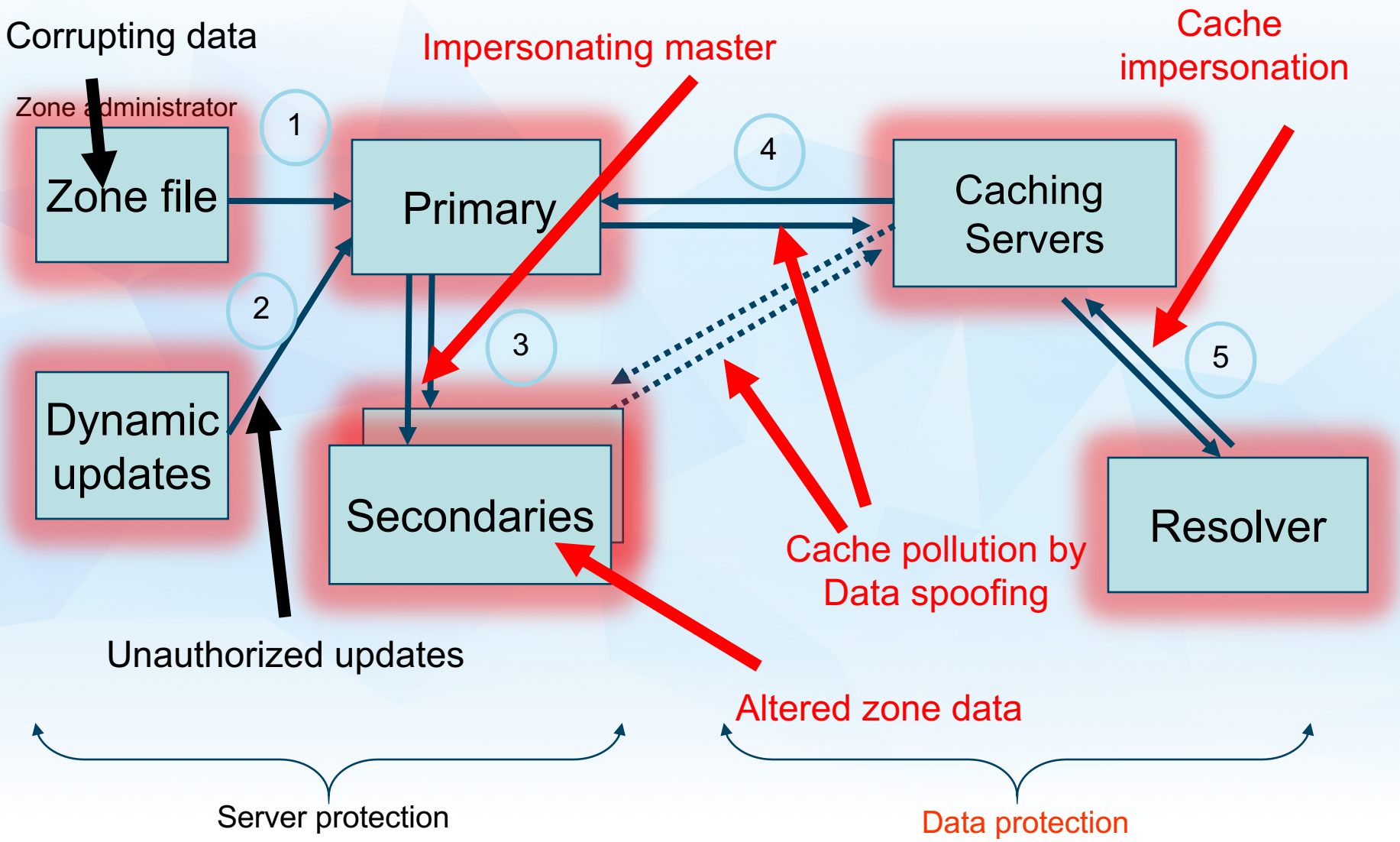
3) Local DNS cache redirects web traffic to a destination of his choosing



DNS: Data Flow



DNS Vulnerabilities



Securing DNS

- There are two aspects when considering DNS Security
  - Server protection
  - Data protection
- Server protection
  - Protecting servers
    - Make sure your DNS servers are protected (i.e. physical security, latest DNS server software, proper security policies, Server redundancies etc.)
  - Protecting server transactions
    - Deployment of TSIG, ACLs etc. (To secure transactions against server impersonations, secure zone transfers, unauthorized updates etc.)
- Data protection
  - Authenticity and Integrity of Data
    - Deployment of DNSSEC (Protect DNS data against cache poisoning, cache impersonations, spoofing etc.)

Technical Requirements

- Networks and Servers (redundant)
- Back office systems.
- Physical and Electronic Security
- Quality of Service (24/ 7 availability!)
- Name Servers
- DNS software (BIND, NSD, etc.)
- Registry software
- Diagnostic tools (ping, traceroute, zonecheck, dig)
- Registry Registrar Protocol

Name Server Considerations

- Support technical standards
- Diverse bandwidth to support above
- Authoritative vs Recursive
- Authoritative Servers must answer authoritatively
- Turn off recursion!
- Recursive Servers should be providing recursion only to designated clients

Know Your SLAs

- Functioning name servers are the most critical/visible service
- All other services also need to be considered
  - Billing
  - Whois server, webservers
  - Registrar APIs
- Consider your service level targets and how you will meet them
- DNS servers always on, other systems mostly on?

Engage with ICANN – Thank You and Questions

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