



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



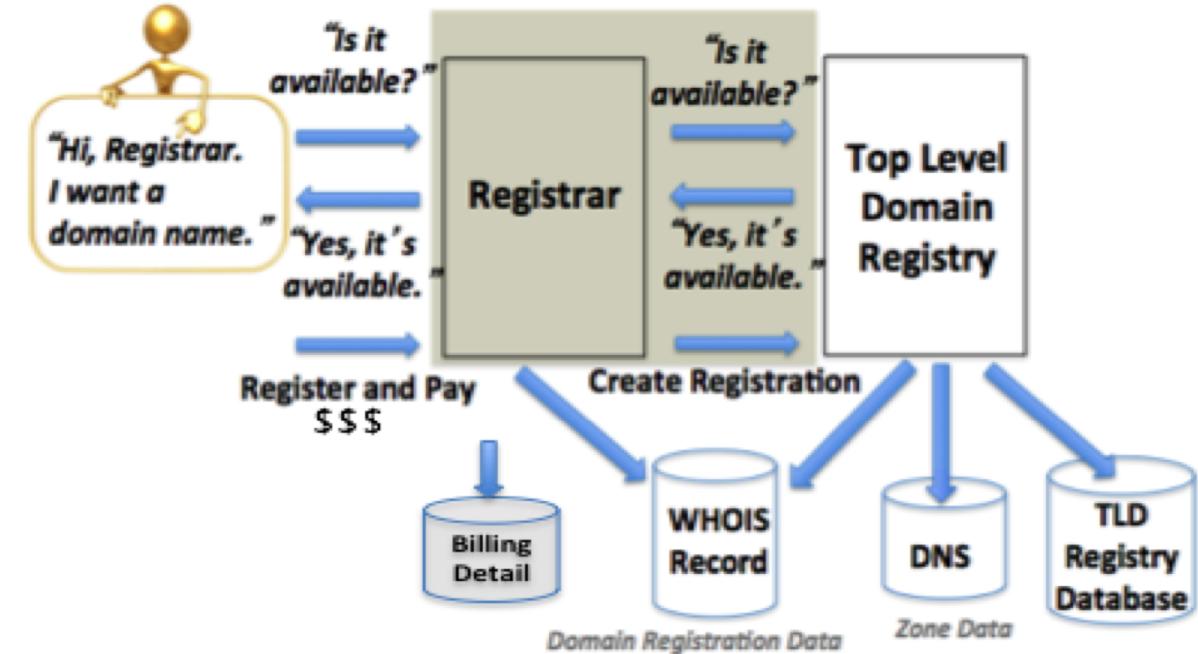
Domains compromised or hijacked by criminals or state-sponsored actors

- 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)

- Please verify your email address for [REDACTED].com

GoDaddy <info@godaddy.com-verify.name>

Dear GoDaddy Customer,
ICANN has implemented a new Transfer Policy which affects all ICANN-accredited registrars. This policy requires that if a domain is transferred from one registrar to another, the email associated with the domain must be verified by the new registrar. This is in response to ICANN's requirement that registrars ask their customers to verify their email addresses before transferring domains. You can read more about this requirement on ICANN's site at <http://www.icann.org/whois-transfer-policy>. You have registered one or more domains from Godaddy Inc. and verification of the email addresses is required to remain active. Please click the link below to verify the email address. If you don't receive an email from us, please check your spam folder or website on hold under "My Account". Please cut-and-paste the following URL into your browser:
<http://www.godaddy.com/verify>

Please remember
domain name regis
Thanks for your att
Thanks for being a

Copyright (C)1999

Domain D[REDACTED].COM Suspension Notice

From: LIQUIDNET Ltd. [Add to Contacts](#)
Sent: Mon, Nov 2, 2015 at 9:50 pm
To: [REDACTED]@thexyz.com

Dear Sir/Madam,

The following domain names have been suspended for violation of the LIQUIDNET Ltd. Abuse Policy:

Domain Name: [REDACTED].COM
Registrar: LIQUIDNET Ltd.
Registrant Name: [REDACTED]

Multiple warnings were sent by LIQUIDNET Ltd. Spam and Abuse Department to give you an opportunity to address the complaints we have received.

We did not receive a reply from you to these email warnings so we then attempted to contact you via telephone.

We had no choice but to suspend your domain name when you did not respond to our attempts to contact you.

[Click here and download](#) a copy of complaints we have received.

Please contact us for additional information regarding this notification.

Sincerely,
LIQUIDNET Ltd.
Spam and Abuse Department
Abuse Department Hotline: 480-324-4655

Account Notice : Error number :6678

Spam

GoDaddy.com <Renewals@i.godaddy.com>
to me

⚠ Why is this message in Spam? It contains content that's typically used in spam messages. [Learn more](#)

Dear Valued GoDaddy Customer: Cristian Badea

more than 7852 directories and may pose a potential performance risk to the server. Please reduce the number of directories for your account to prevent [REDACTED] from causing the account deactivation.

To prevent your account from being locked out we recommend that you create special TMP directory.

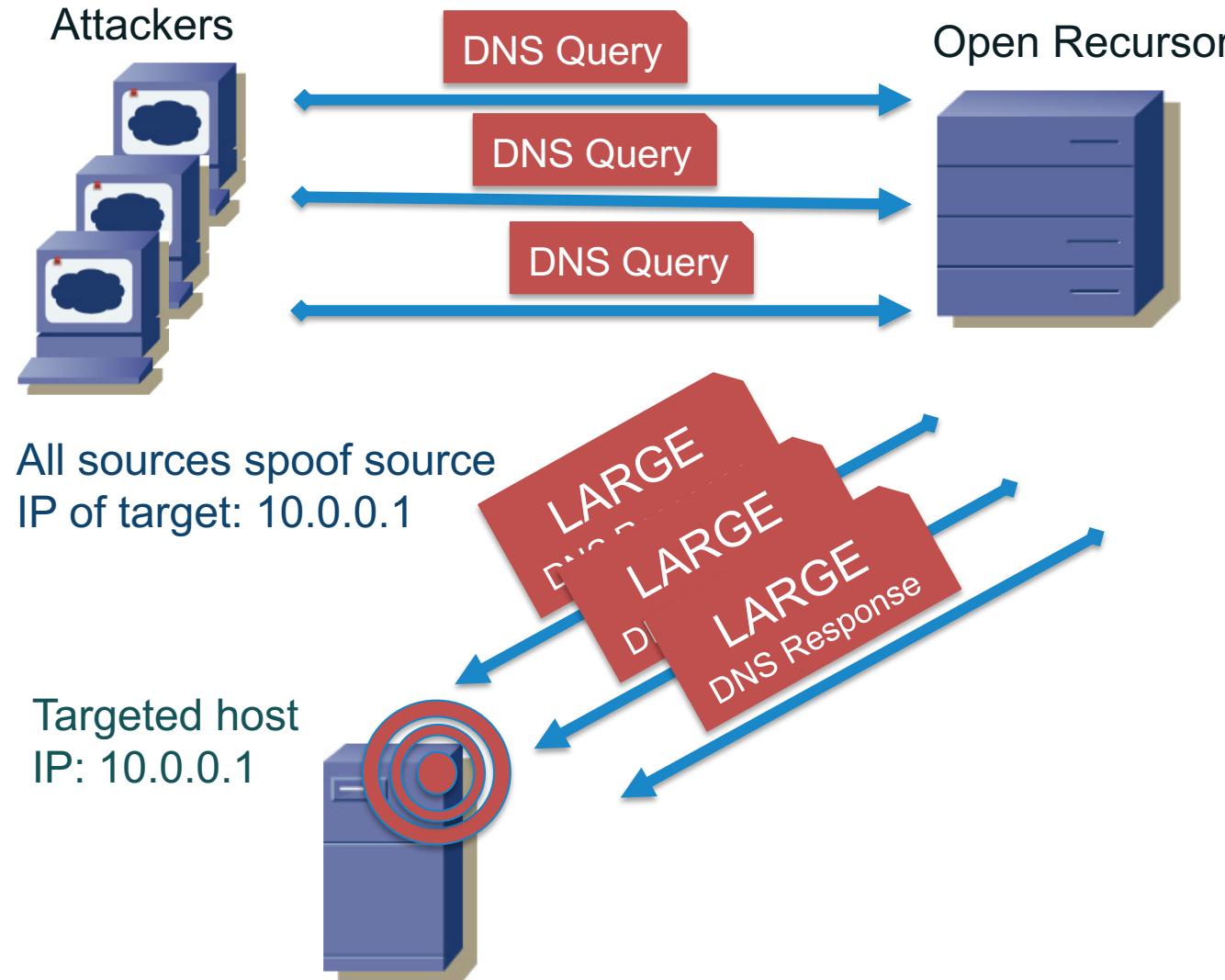
[http://\[REDACTED\]/tmp.cfg/php/user/main.php?submit=b16574c54c98b9512edbecb8fa4f47f2](http://[REDACTED]/tmp.cfg/php/user/main.php?submit=b16574c54c98b9512edbecb8fa4f47f2)

support.

14 GoDaddy.com, LLC. All rights reserved

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



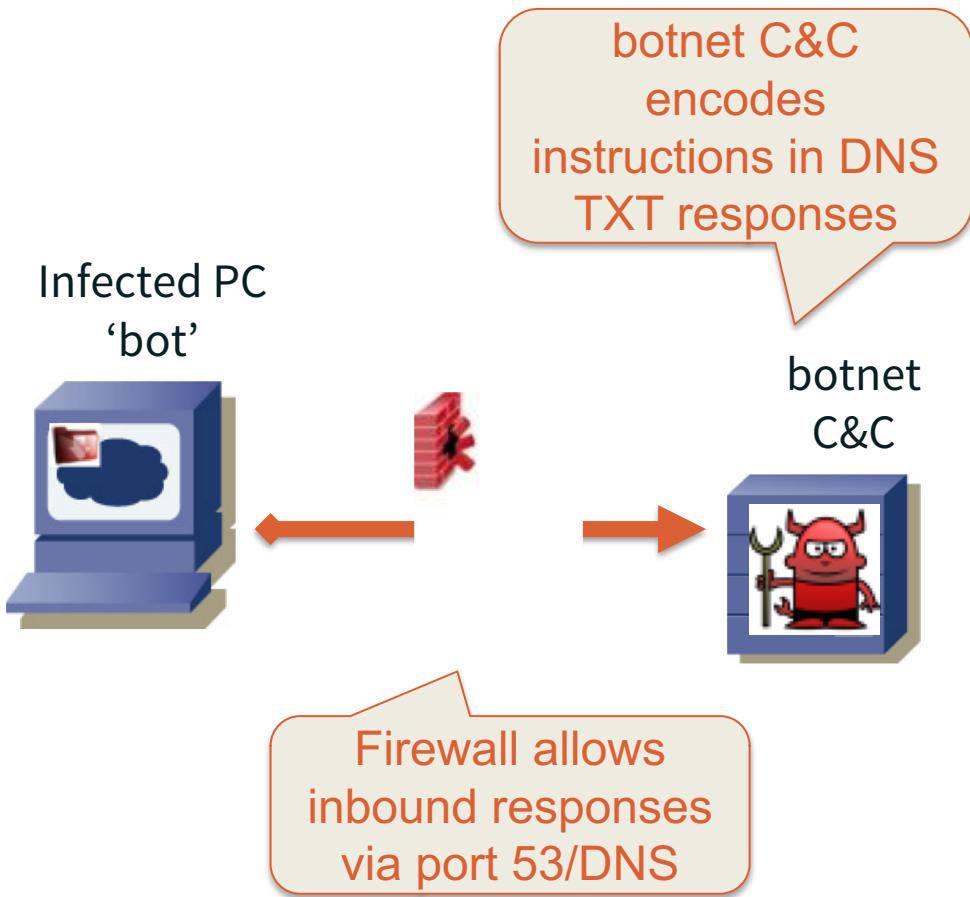
My local resolver



eCrime name
server

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

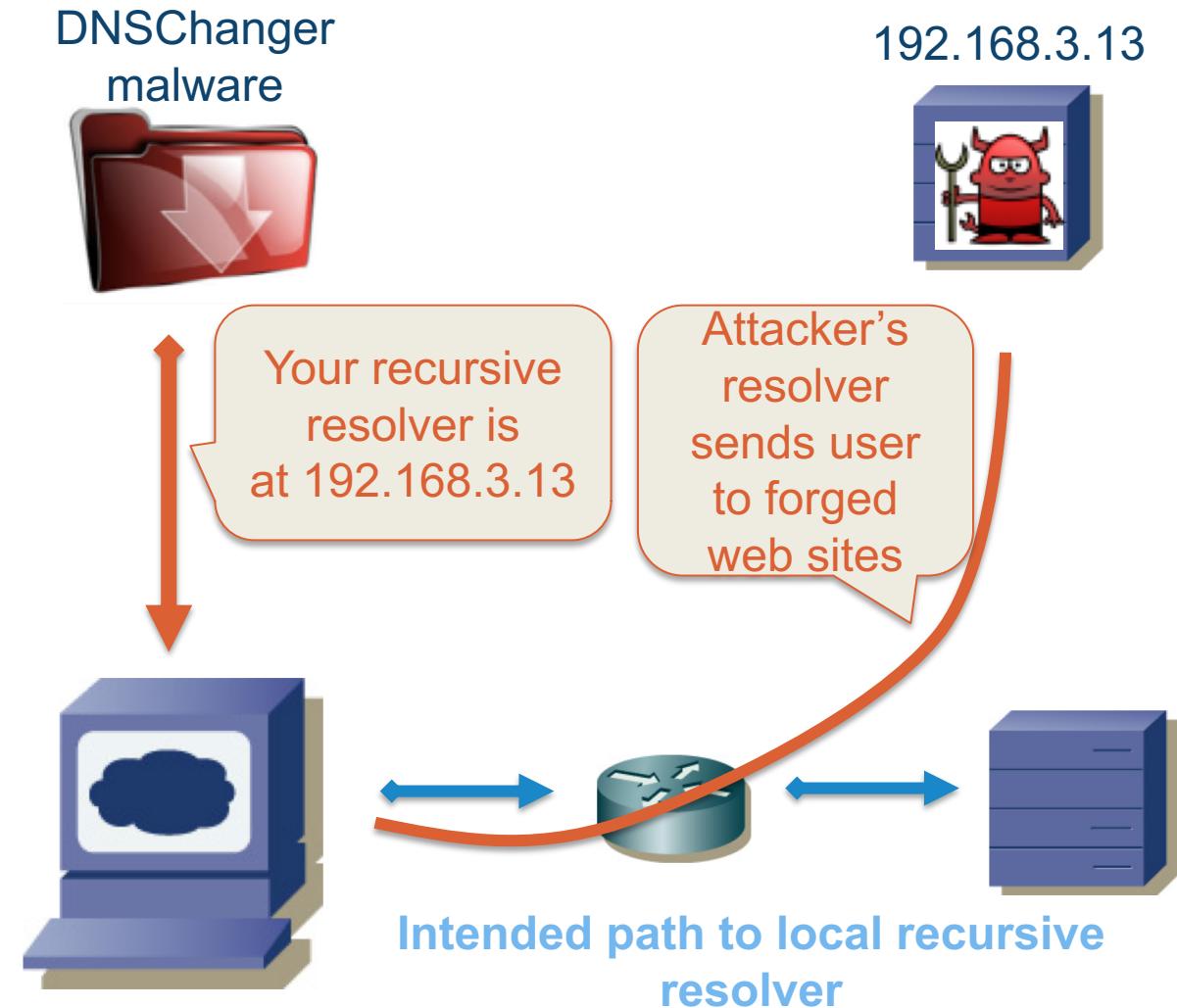
DNS as a Covert Malware Channel



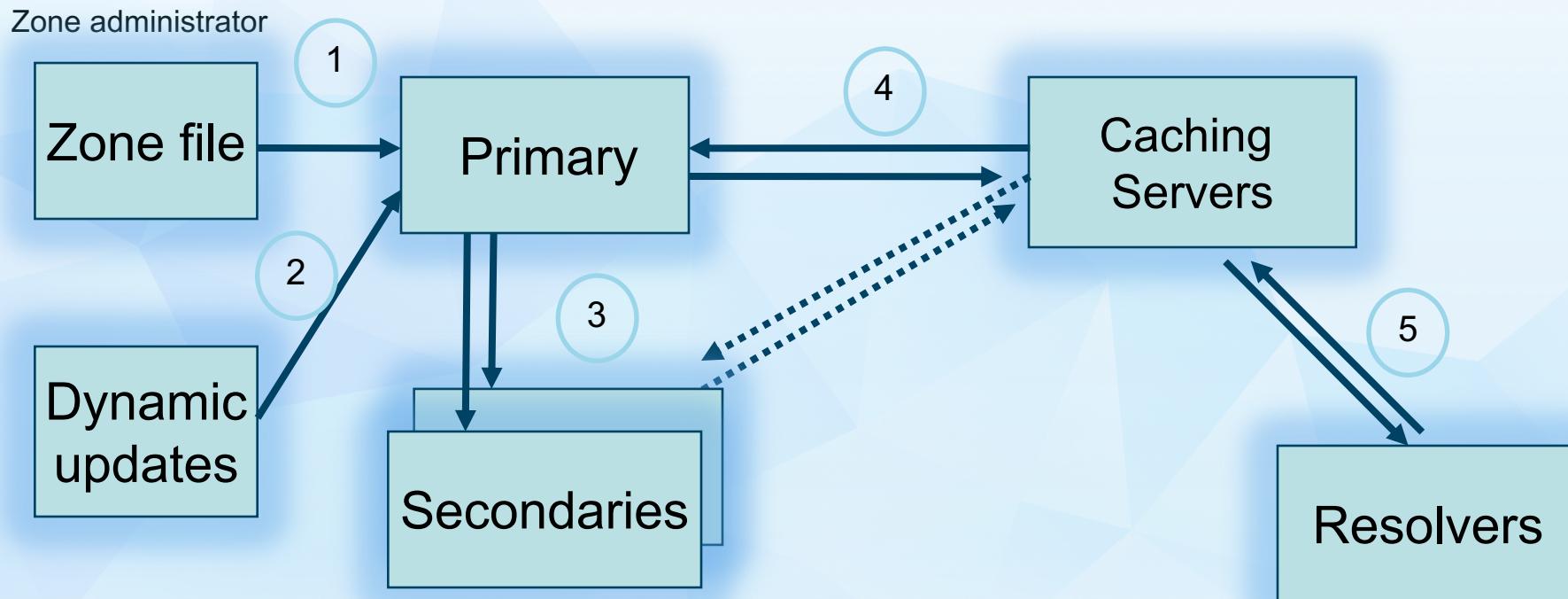
- Malware on infected PC performs TXT lookups to botnet C&C
- TXT responses contain instructions or executables for bot
- Examples in wild:
 - Feederbot
 - Morto

Poisoning a host (DNSChanger)

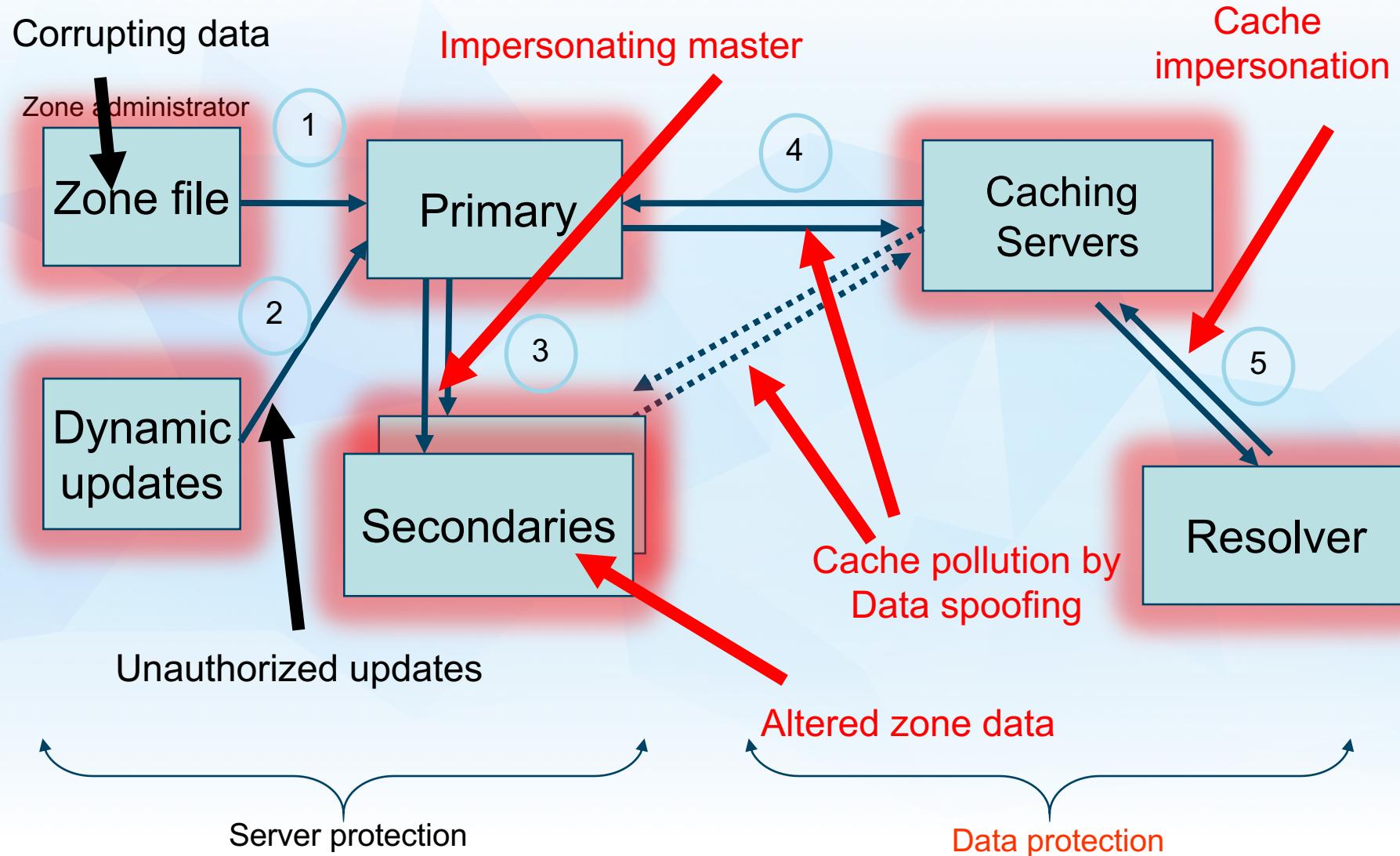
- 1) The attacker distributes DNS configuration altering malware via
 - a) Spam, drive-by download...
 - b) *Example: DNSChanger malware*
- 2) Attacker alters DNS configuration of infected PC to cause all requests to go to a malicious nameserver run by attackers
- 3) Local DNS cache redirects web traffic 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