



# Strengthening our Ecosystem through Stakeholder Collaboration

Jia-Rong Low, Sr Director, Asia | 20 August 2015

# Agenda

1

About ICANN and  
the Domain Name  
System (DNS)

2

DNS attacks and  
their impact

3

DNS Security

# What does ICANN do?

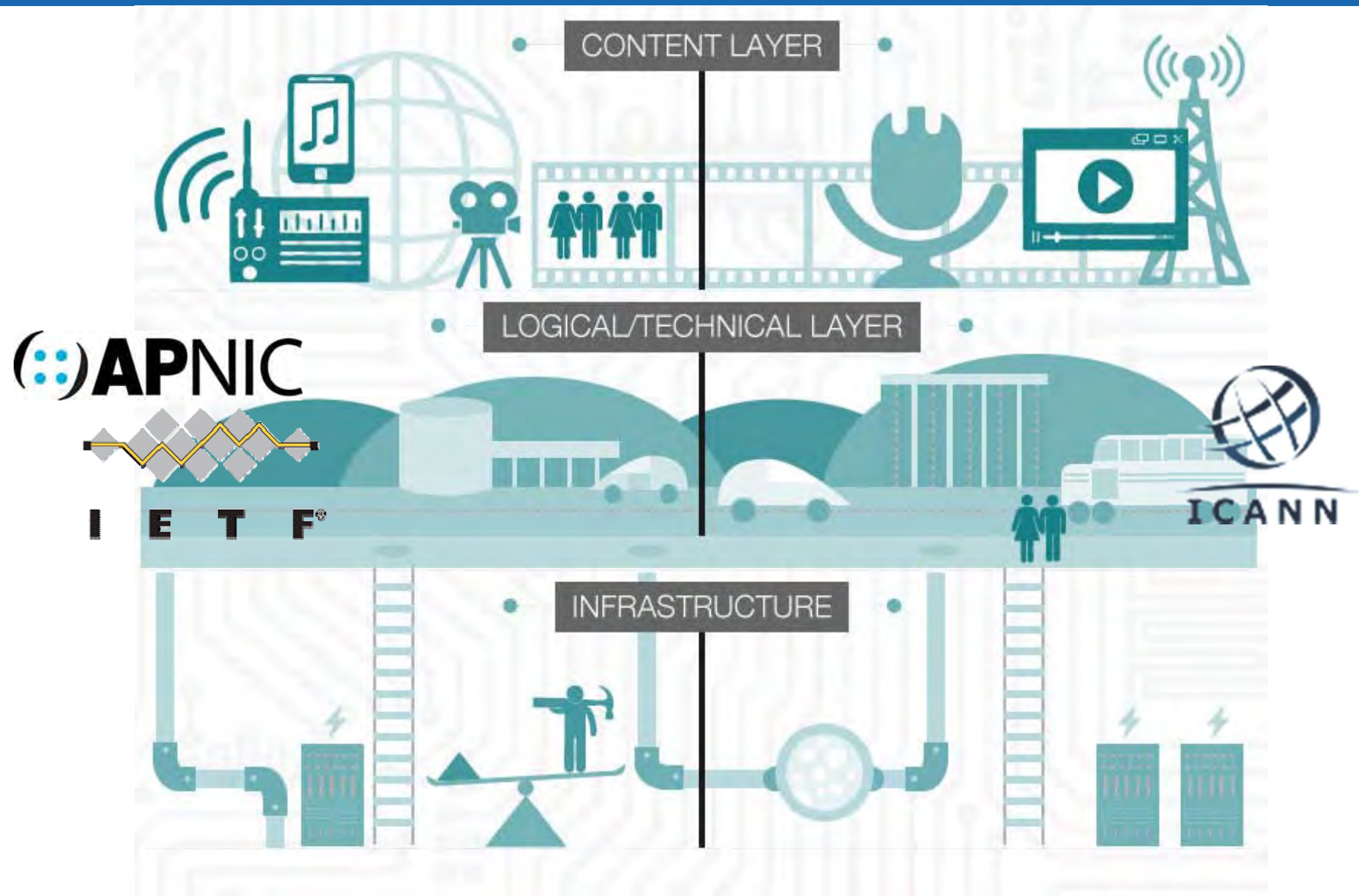
## WHAT DOES ICANN DO?

To reach another person on the Internet you have to type an address into your device—a name or a number. That address must be unique, so computers will know where to find each other. ICANN maintains and administers these unique identifiers across the world. Without ICANN's management of this system, known as the Domain Name System (DNS), we wouldn't have a global, scalable Internet where we can find each other.

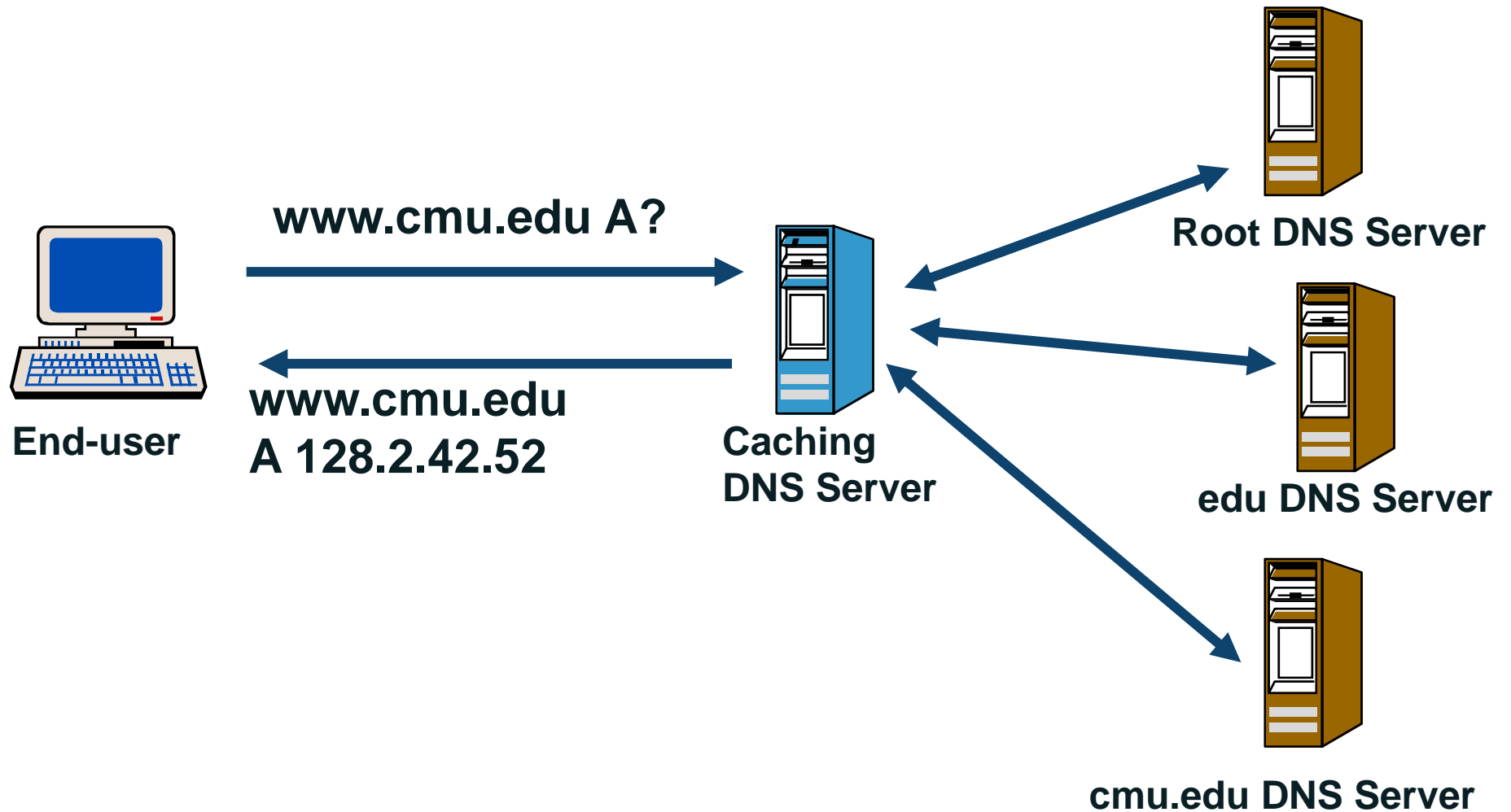


- **IP address**  
(192.0.32.7)  
(2607:f0d0:1002:51::4)
- **Domain Names**  
.com .org .net;  
.my .sg .cn .in .bd;  
.संगठन , .游戏, .شبكة

# The Internet Architecture



# Domain Name Resolution Process





# DNS attacks and their impact

# Have an online presence or online service?

- [mycompany.com](#)
- [Mybank.com](#)
- [eGov.xx](#)
- [Ministry-of-jiarong.gov.xx](#)
- [myorganisation.org](#)

# DNS attacks can affect you

News

## Major DDoS attacks .cn domain; disrupts Internet in China

It's still unclear where the DDoS attack originated from

By Michael Kan

August 26, 2013 07:20 AM ET 4 Comments



IDG News Service - China's Internet was hit with a major distributed denial of service (DDoS) attack Sunday morning that briefly disrupted and slowed access to sites in the .cn domain.

The DDoS attack was the largest in history against the domain servers for China's .cn ccTLD (country code top level domain), according to the China Internet Network Information Center (CNNIC), which administers the domain.

## How the Syrian Electronic Army took out the New York Times and Twitter sites

**Summary:** *The short, snappy answer is: "All too easily." Here's how it appears to have happened.*



By Steven J. Vaughan-Nichols for Networking | August 28, 2013 -- 21:01 GMT (05:01 SGT)

Follow @sjvn

Once more, the Syrian Electronic Army (SEA), a pro-Syrian strongman Bashar al-Assad organization, has struck on the internet.

This time, SEA hit *The New York Times* (NYT), Twitter, and other popular sites. Unlike previous attacks that relied on phishing attacks to gain password information from the target site's authorized users, SEA is using the weak security of the internet's master address book, the Domain Name System (DNS), to re-route internet traffic from its real destination to SEA-controlled sites.

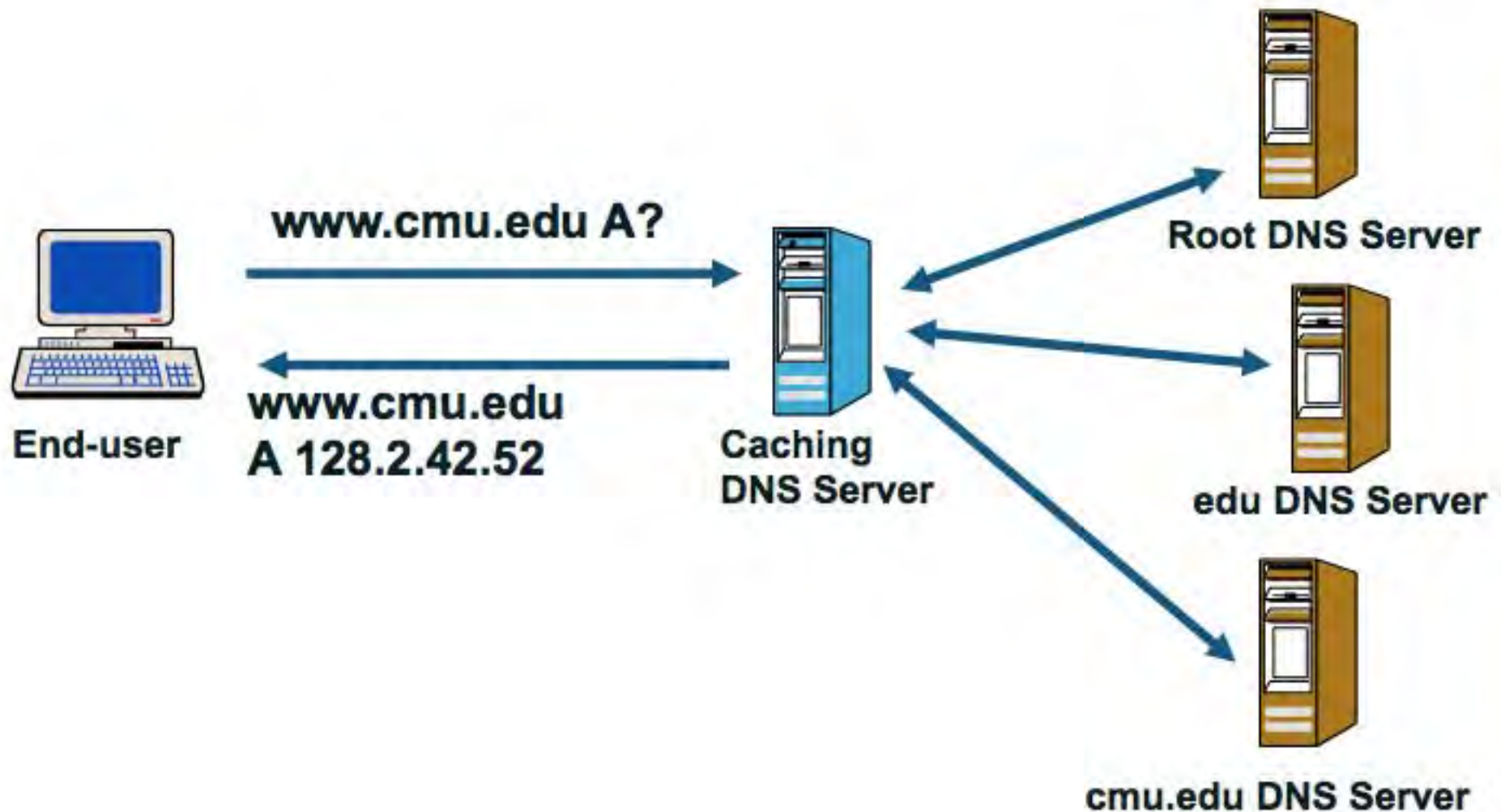
## DNSChanger

From Wikipedia, the free encyclopedia

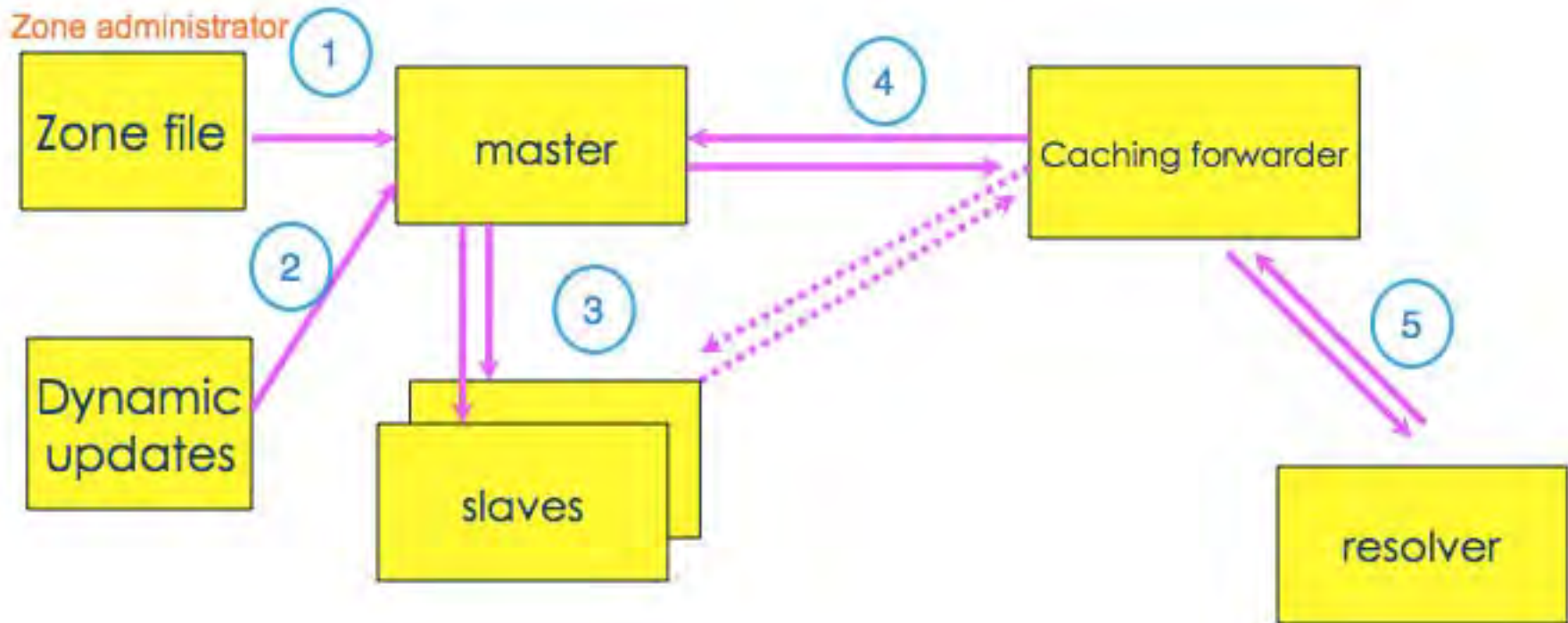
**DNSChanger** was a **DNS hijacking Trojan** active from 2007 to 2011. The work of an Estonian company known as **Rove Digital**, the malware infected computers by modifying a computer's **DNS** entries to point toward its own **rogue name servers**, which then injected its own advertising into Web pages. At its peak, DNSChanger was estimated to have infected over 4 million computers, bringing in at least **US\$14 million** in profits to its operator from fraudulent advertising revenue.<sup>[1]</sup>



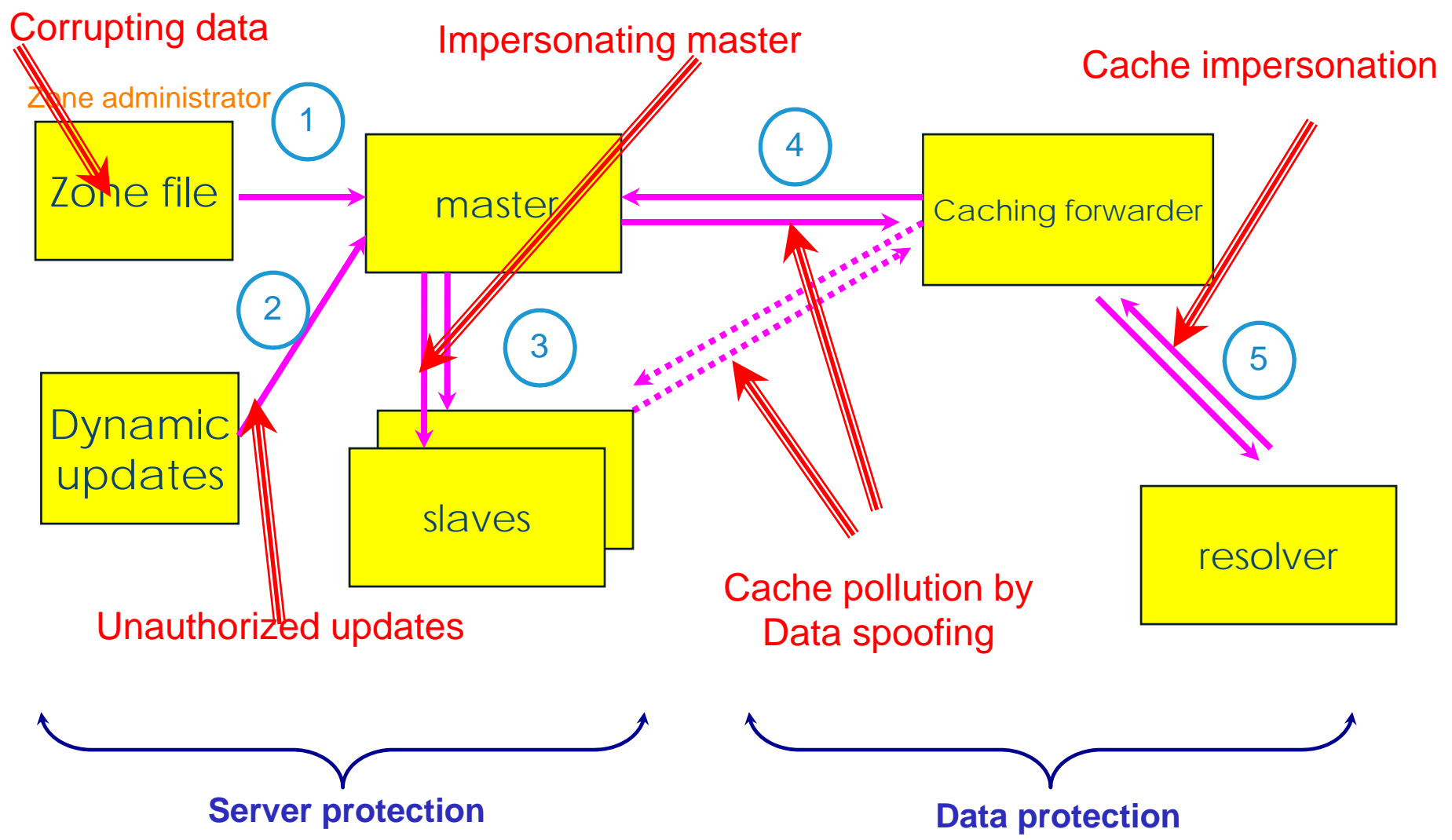
# Domain Name Resolution Process

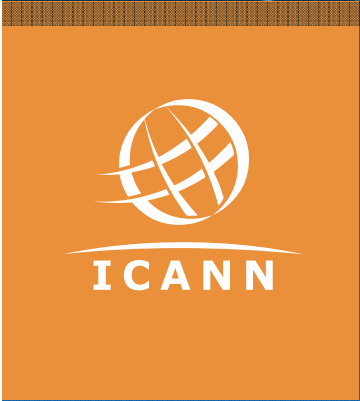
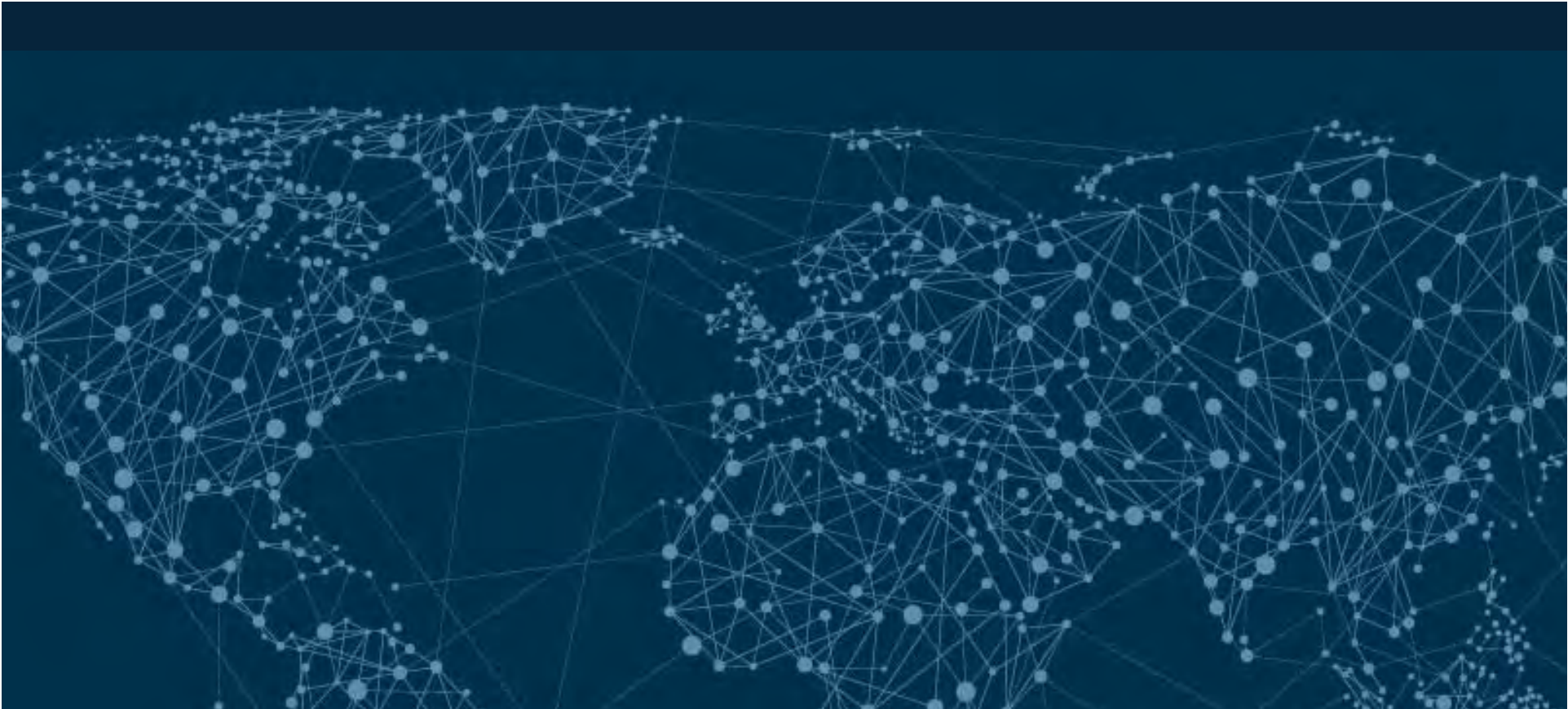


# DNS Data Flow



# DNS Data Flow





# DNS Security

# DNS Security

- 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.)

# Cybersecurity challenges – Common Themes



Source: mmCERT

# Cybersecurity – People and Technology

## People

- Awareness
- Security requirements
- Knowledge and skills
- Sharing Security Incident Information

## Technology

- DNS Security Extensions (DNSSEC)
- Root servers



# People – Capacity Building



61

TRAININGS/  
WORKSHOPS  
CONDUCTED

- **Partners/Recipients**
  - TLD Registry Operators on Security, DNSSEC etc
  - Law Enforcement Agencies on DNS Basics, Mitigating DNS abuse/misuse
  - Network Operators; CERTs
- **Knowledge exchange**
  - Europol, Interpol

33

COUNTRIES REACHED



APPROX.

2010

PARTICIPANTS



# People – Information sharing

- **Exchange of threat/incident intelligence**

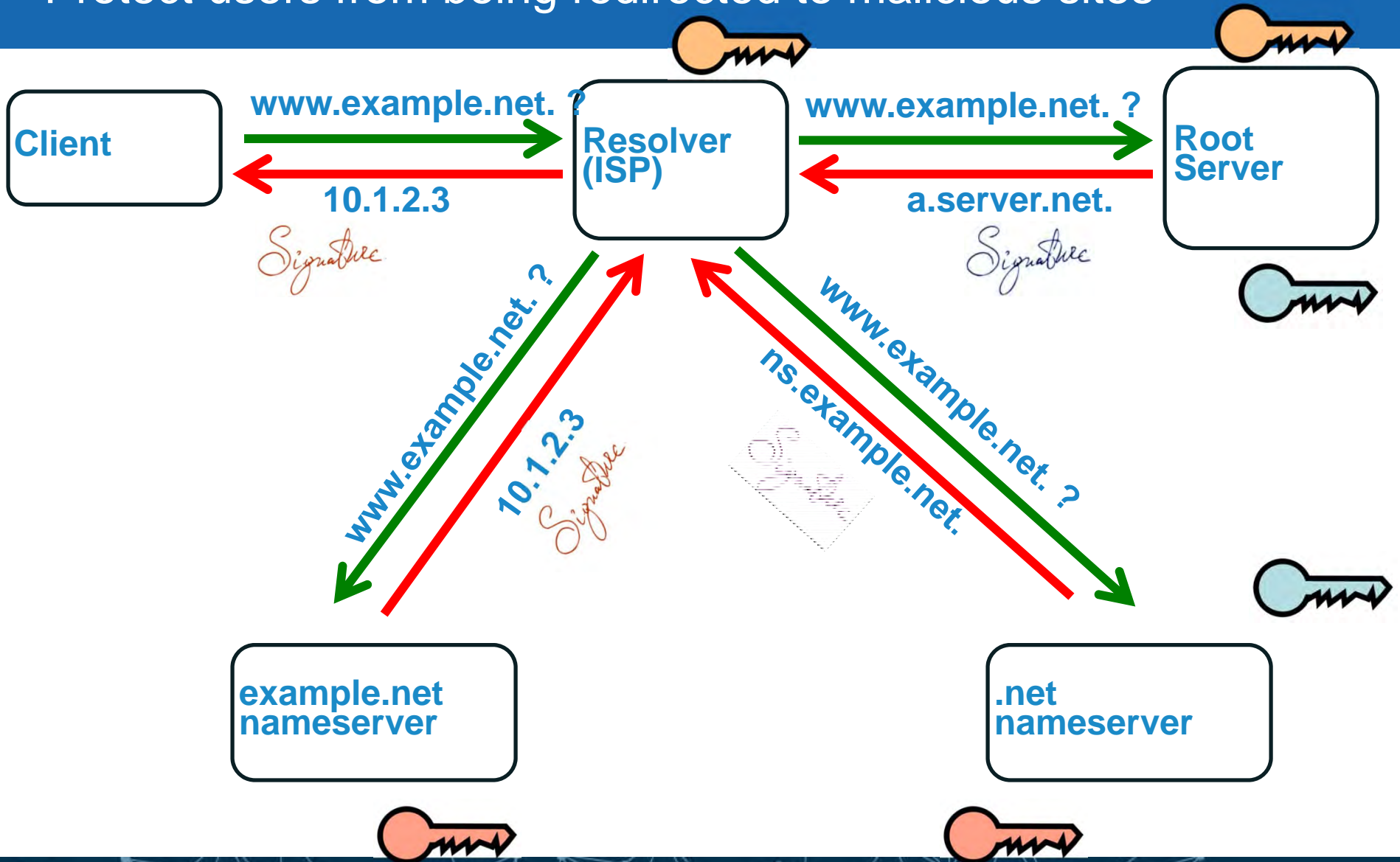
- Attacks against ccTLDs, registrars
- Coordinated response to threats
- Vulnerability disclosure

- **Collaborate to look at specific issues**

- **Phishing**
  - Research, target bad domains (Anti-Phishing Working Group)
- **Spam**
  - Work with Governments; Regional Internet Registries; ISOC
- **Crime**
  - DNS abuse/misuse; DDoS attack
  - Work with Law Enforcement Agencies
- **Global Cybersecurity Cybercrime Initiative**
  - OECD, other academic institutions

# Tech – DNSSEC:

Protect users from being redirected to malicious sites



# DNSSEC: So what's the problem?

- Not enough IT departments know about it or are too busy putting out other security fires.
- When they do look into it they hear old stories of FUD and lack of turnkey solutions.
- Registrars\*/DNS providers see no demand leading to “chicken-and-egg” problems.

\*but required by new ICANN registrar agreement

# What you can do

- ***For Companies:***
  - Sign your corporate domain names
  - Just turn on validation on corporate DNS resolvers
- ***For Users:***
  - Ask ISP to turn on validation on their DNS resolvers
- ***For All:***
  - Take advantage of DNSSEC education and training




# Tech - Root Servers: Internet Stability and Resiliency



- Root nodes keep Internet traffic local and resolve queries faster
- Make it easier to isolate attacks
- Reduce congestion on international bandwidth

- Ongoing project to expand distribution of L-Root globally
- Over 150 L-root instances worldwide
- 11 installed in APAC



 DATE	 HOST NAME	 CITY/COUNTRY
Sept 2013	Solomon Telekom	Honiara, Solomon Islands
Feb 2014	Fiji International	Nadi, Fiji
April 2014	Vodafone Fiji	Suva-Nausori, Fiji
July 2014	21Vianet	Beijing, China
Sept 2014	Micron 21	Melbourne, Australia
Oct 2014	Internet Domain Name System Beijing Engineering Research Centre (ZDNS)	Beijing, China
Nov 2014	BASIS Technologies	Dum Dum, India
Jan 2015	True Internet Co	Bangkok, Thailand
Feb 2015	Philippine Long Distance Telephone Company	Manila, Philippines
Mar 2015	Vocus	Mangere, New Zealand
May 2015	Pandi	Jakarta, Indonesia

# Root Servers: Host an L-Root

- Contact ICANN Asia Pacific Hub
  - [apachub@icann.org](mailto:apachub@icann.org)
- What you'll need:
  - L-Root Node host provides hardware
  - ICANN runs systems on it
  - Zero-dollar contract



# Thank you and Questions



## Thank You and Questions

Email: [jiarong.low@icann.org](mailto:jiarong.low@icann.org)

Website: [icann.org](http://icann.org)



[twitter.com/icann](https://twitter.com/icann)  
[twitter.com/icann4biz](https://twitter.com/icann4biz)



[gplus.to/icann](https://plus.google.com/icann)



[facebook.com/icannorg](https://facebook.com/icannorg)



[weibo.com/ICANNorg](https://weibo.com/ICANNorg)



[linkedin.com/company/icann](https://linkedin.com/company/icann)



[flickr.com/photos/icann](https://flickr.com/photos/icann)



[youtube.com/user/icannnews](https://youtube.com/user/icannnews)



[slideshare.net/icannpresentations](https://slideshare.net/icannpresentations)