บทบาท DNSSEC ในโลกอินเทอร์เน็ต

นายชยา ลิมจิตติ
ที่ปรึกษามูลนิธิศูนย์สารสนเทศเครือข่ายไทย

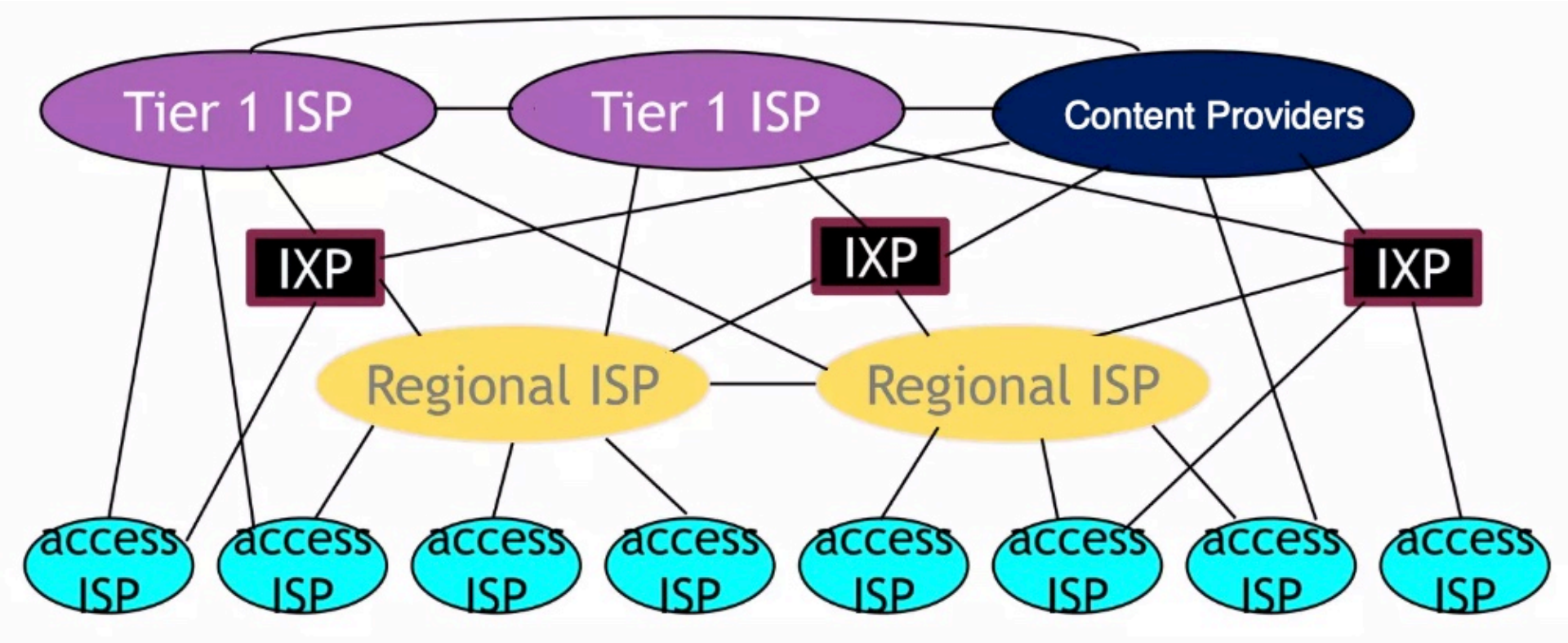
๒๑ พฤศจิกายน ๒๕๖๗

รู้จักกับอินเทอร์เน็ต

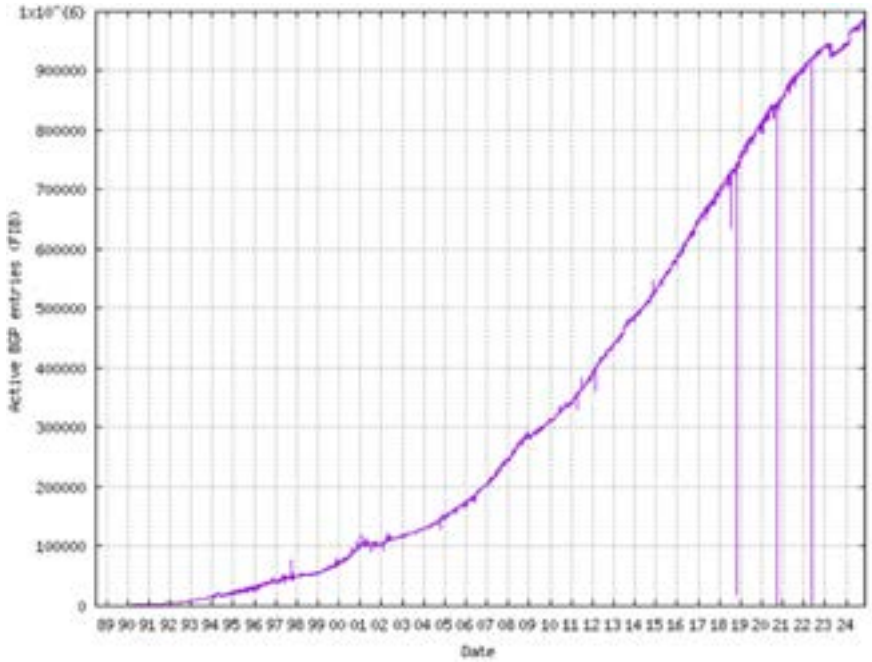
รู้จักอินเทอร์เน็ต

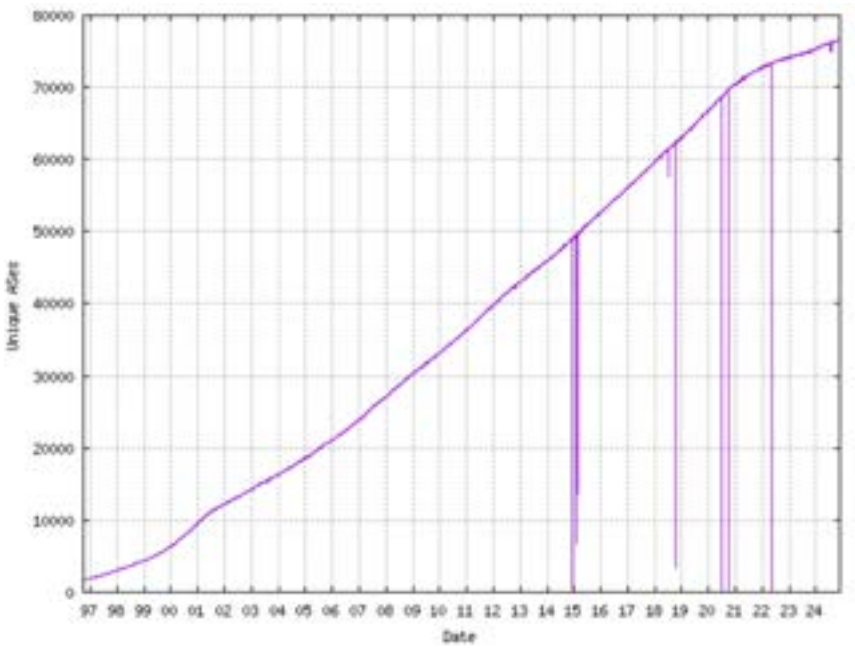
- เครือข่าย (network) ของคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ขนาดต่าง ๆ กัน ที่เชื่อมต่อและติดต่อสื่อสารกันด้วยมาตรฐานเดียวกัน จนเป็นเครือข่ายคอมพิวเตอร์ขนาดใหญ่ครอบคลุมพื้นที่ทั่วโลก
- เครือข่ายที่เชื่อมต่อกันนั้นถือเป็นส่วนหนึ่งของอินเทอร์เน็ต
- Internet เกิดจากโจทย์ทางทหารที่ต้องการการสื่อสารที่ทำงานได้ต่อเนื่องและโจทย์งานวิจัยที่ต้องการใช้งานทรัพยากรร่วมกัน
- ผู้ดูแลเครือข่ายคอมพิวเตอร์เหล่านั้นไม่ได้อยู่ภายใต้สังกัดและนโยบายเดียวกัน
- ผู้ดูแลเครือข่ายคอมพิวเตอร์ไว้วางใจและเชื่อถือซึ่งกันและกัน

โครงสร้างของอินเทอร์เน็ต



การเติบโตของอินเทอร์เน็ต





Date	Prefixes	CIDR Aggregated
13-11-24	987432	543216
14-11-24	987777	544745
15-11-24	988047	545072
16-11-24	987751	546036
17-11-24	988084	546340
18-11-24	988237	547169
19-11-24	988125	547610
20-11-24	987575	548204

Top 20 Route Count per Originating AS

Prefixes	ASnum	AS Description
11041	AS8151	UNINET, MX
10998	AS16509	AMAZON-02, US
10853	AS9808	CHINAMOBILE-CN China Mobile Communications Group Co., Ltd., CN
7084	AS12479	UNI2-AS, ES
5898	AS7545	TPG-INTERNET-AP TPG Telecom Limited, AU
4932	AS4538	ERX-CERNET-BKB China Education and Research Network Center, CN
4732	AS39891	ALJAWWALSTC-AS, SA
4678	AS11492	CABLEONE, US
4578	AS174	COGENT-174, US
4481	AS18403	FPT-AS-AP FPT Telecom Company, VN
4168	AS7155	VSASAT-SP-BACKBONE, US
3929	AS20940	AKAMAI-ASN1, NL
3905	AS7552	VIETEL-AS-AP Viettel Group, VN
3899	AS9498	BBIL-AP BHARTI Airtel Ltd., IN
3693	AS7713	TELKOMNET-AS-AP PT Telekomunikasi Indonesia, ID
3673	AS9009	M247, RO
3645	AS6327	SHAW, CA
3576	AS22773	ASN-CXA-ALL-CCI-22773-RDC, US
3543	AS10620	Telmex Colombia S.A., CO
3362	AS749	DNIC-AS-00749, US

ที่มา https://www.cidr-report.org/

อินเทอร์เน็ตจากอดีตสู่ปัจจุบัน

- ผู้ใช้เฉพาะกลุ่มกลายเป็นผู้ใช้ทุกกลุ่มของโลก
- เดิมต้องเชื่อมต่อผ่าน PCM / TDM กลายเป็นโครงสร้างพื้นฐานหลักของการติดต่อสื่อสาร
- จากเครื่องมือทำงานของคนกลุ่มเล็ก กลายเป็นสิ่งจำเป็นอย่างยิ่งยวดสำหรับคนทุกกลุ่ม
- Security และ Privacy เป็นประเด็นที่สำคัญมากขึ้นเรื่อย ๆ

Internet Resilience
(ความแข็งแกร่งทนทานของอินเทอร์เน็ต)

- อินเทอร์เน็ตเป็นโครงสร้างพื้นฐานที่สำคัญสำหรับทุกกลุ่ม
- ยุคโควิดตอกย้ำความสำคัญของอินเทอร์เน็ต
- ผู้ดูแลอินเทอร์เน็ตมีความหลากหลาย ทั้งด้านประสบการณ์ ความสามารถ และนโยบายหน่วยงาน จะมั่นใจได้อย่างไรว่าจะไม่เกิดความผิดพลาดในการทำงาน
- ตัวชี้วัด Internet Resilience มีอะไรบ้าง

Internet Resilience
(ความแข็งแกร่งทนทานของอินเทอร์เน็ต)

Internet Society Pulse

A resilient Internet connection is one that maintains an acceptable level of service in the face of faults and challenges to normal operation. In this Pulse focus area we track resiliency metrics using the Internet Resilience Index to help support the development of policies and infrastructure to improve Internet resilience at the local, regional, and global level.

Our overall measure of Internet resilience is based on the following pillars:

Infrastructure
The existence and availability of physical infrastructure that provides Internet connectivity.

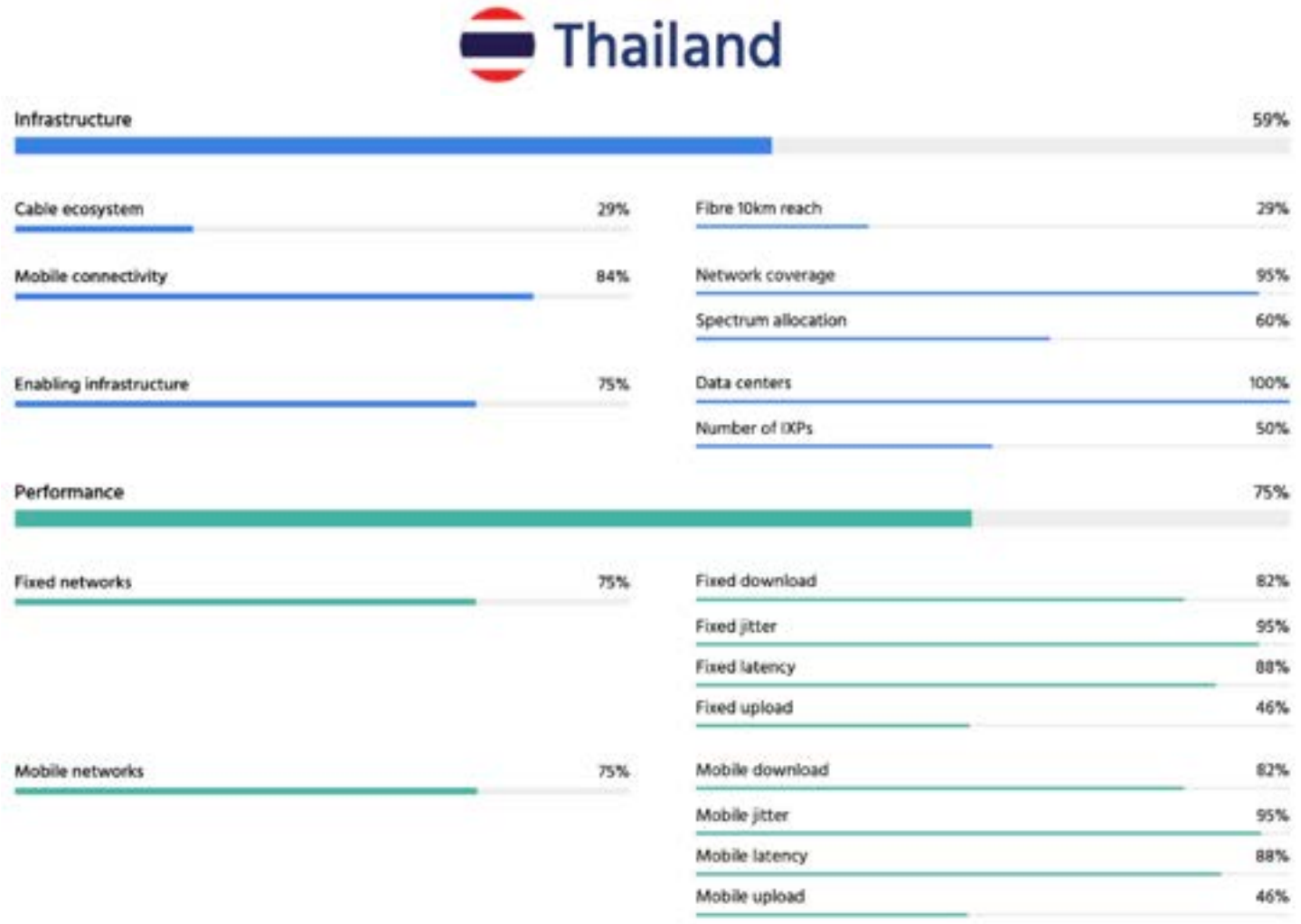
Performance
The ability of the network to provide end-users with seamless and reliable access to Internet services.

Security
The ability of the network to resist intentional or unintentional disruptions through the adoption of security technologies and best practices.

Market Readiness
The ability of the market to self-regulate and provide affordable prices to end-users by maintaining a diverse and competitive market.

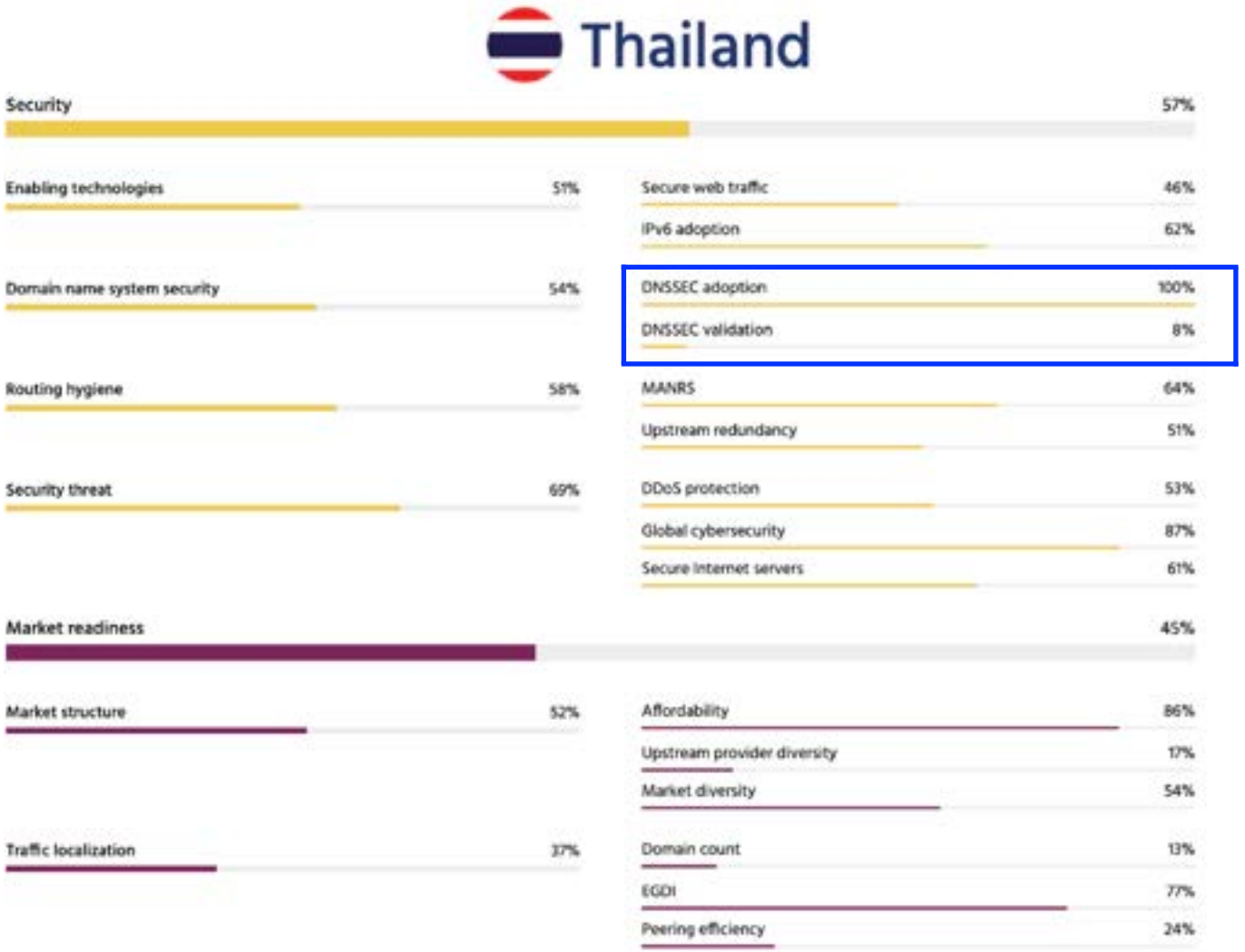
ที่มา https://pulse.internetsociety.org/resilience

Internet Resilience
(ความแข็งแกร่งทนทานของอินเทอร์เน็ต)



ที่มา https://pulse.internetsociety.org/resilience

Internet Resilience
(ความแข็งแกร่งทนทานของอินเทอร์เน็ต)



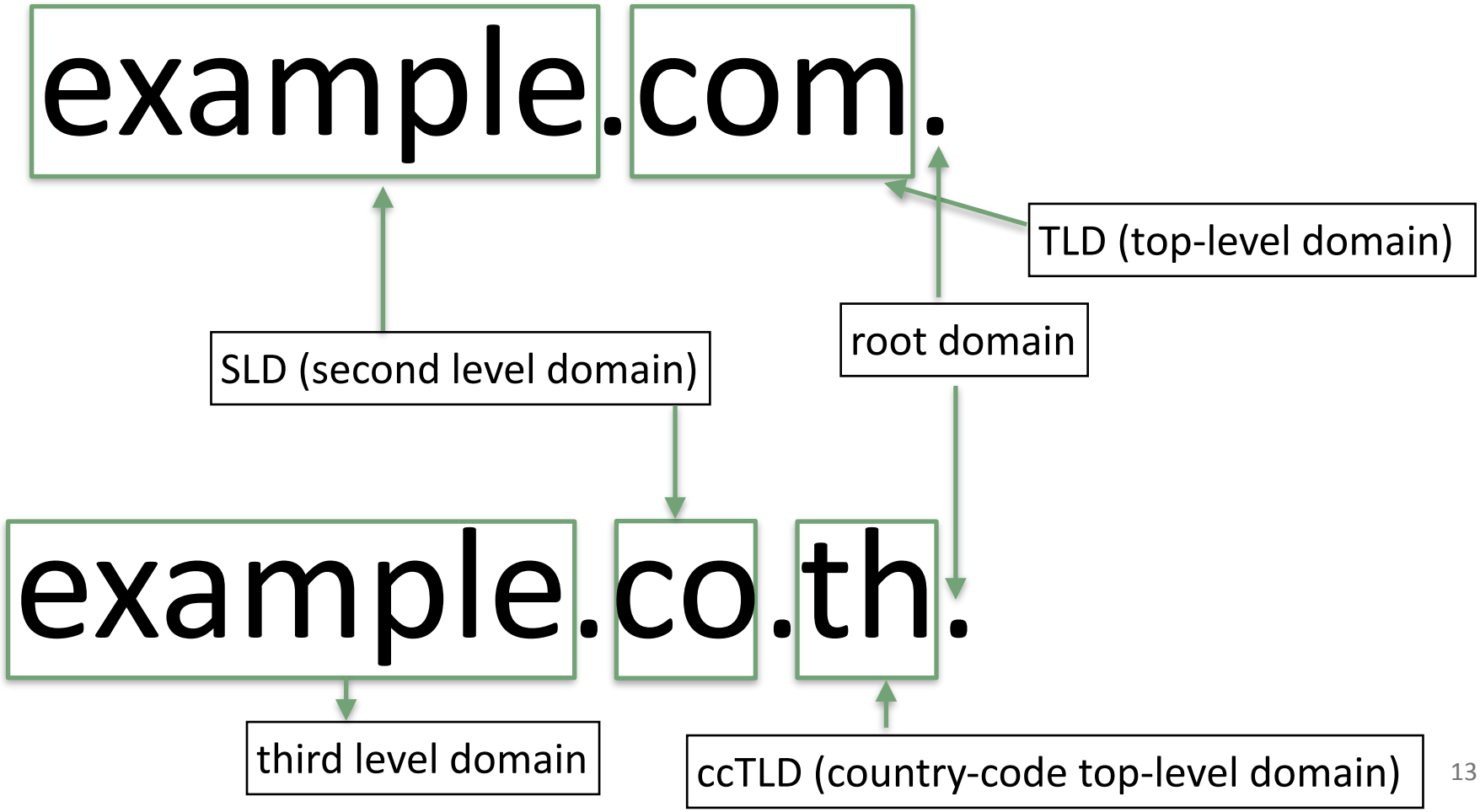
ที่มา https://pulse.internetsociety.org/resilience

ความรู้ทั่วไปเกี่ยวกับชื่อโดเมน

ชื่อโดเมนคืออะไร

- ชื่อโดเมน หรือ Domain Name
- ชื่อแสดงตัวตนบนโลกอินเทอร์เน็ต
- เปรียบได้กับเครื่องหมายการค้า เครื่องหมายบริการ
- ชื่อแสดงแหล่งที่มา ถิ่นฐาน ต้นกำเนิด
- ผู้จดทะเบียนมีสิทธิในชื่อโดเมนนั้น ๆ
- เป็นได้ทั้งภาษาไทย ภาษาอังกฤษ และภาษาอื่น ๆ
  - https://รู้จัก.ไทย
  - https://มูลนิธิทีเอชนิค.ไทย
  - https://www.thnic.or.th

รูปแบบ/โครงสร้างชื่อโดเมน

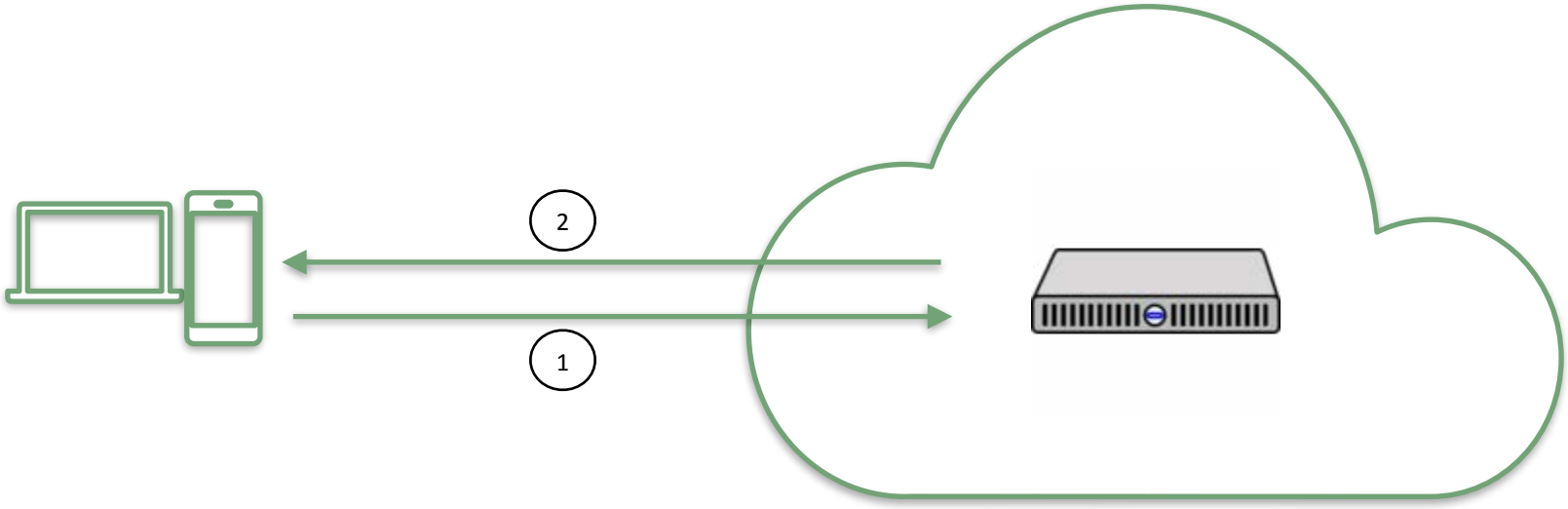


ระบบชื่อโดเมนทำงานอย่างไร

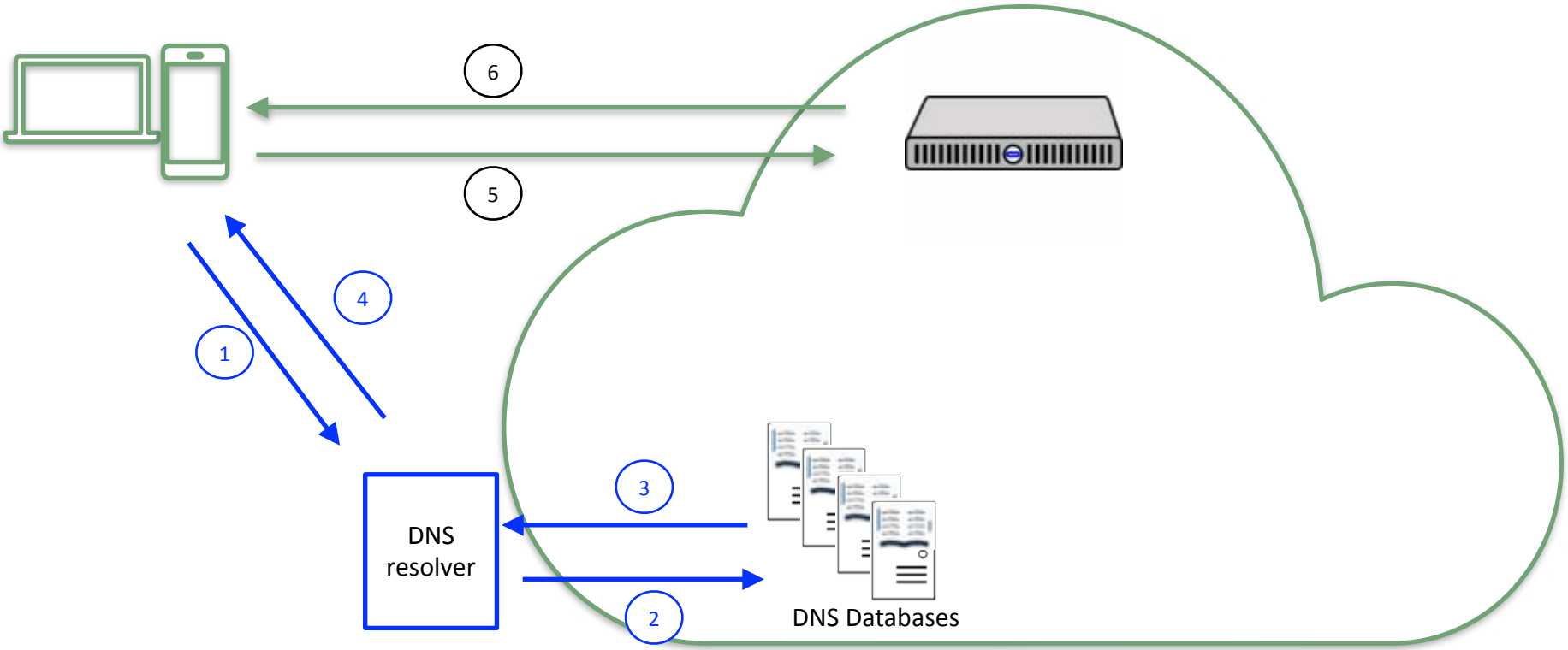
ระบบชื่อโดเมนคืออะไร

- ระบบชื่อโดเมน หรือ Domain Name System
- ระบบที่แปลงชื่อโดเมนไปเป็นหมายเลขไอพี หรืออ้างอิงถึงข้อมูลอื่น ๆ บนโลกอินเทอร์เน็ต
  - www.ncsa.or.th –> 202.139.203.149
  - ถ้าจะส่งเมลถึง ncsa.or.th
    - ให้ส่งไปที่ ncsa-or-th.mail.protection.outlook.com.
  - ข้อมูล TXT (บางส่วน) ของ ncsa.or.th
    - v=DMARC1;p=none;aspf=r
    - v=spf1 include:spf.protection.outlook.com
- เปรียบได้กับสมุดจดชื่อโทรศัพท์
  - สมชาย --> 012-345-6789

การทำงานของอินเทอร์เน็ตเบื้องต้น



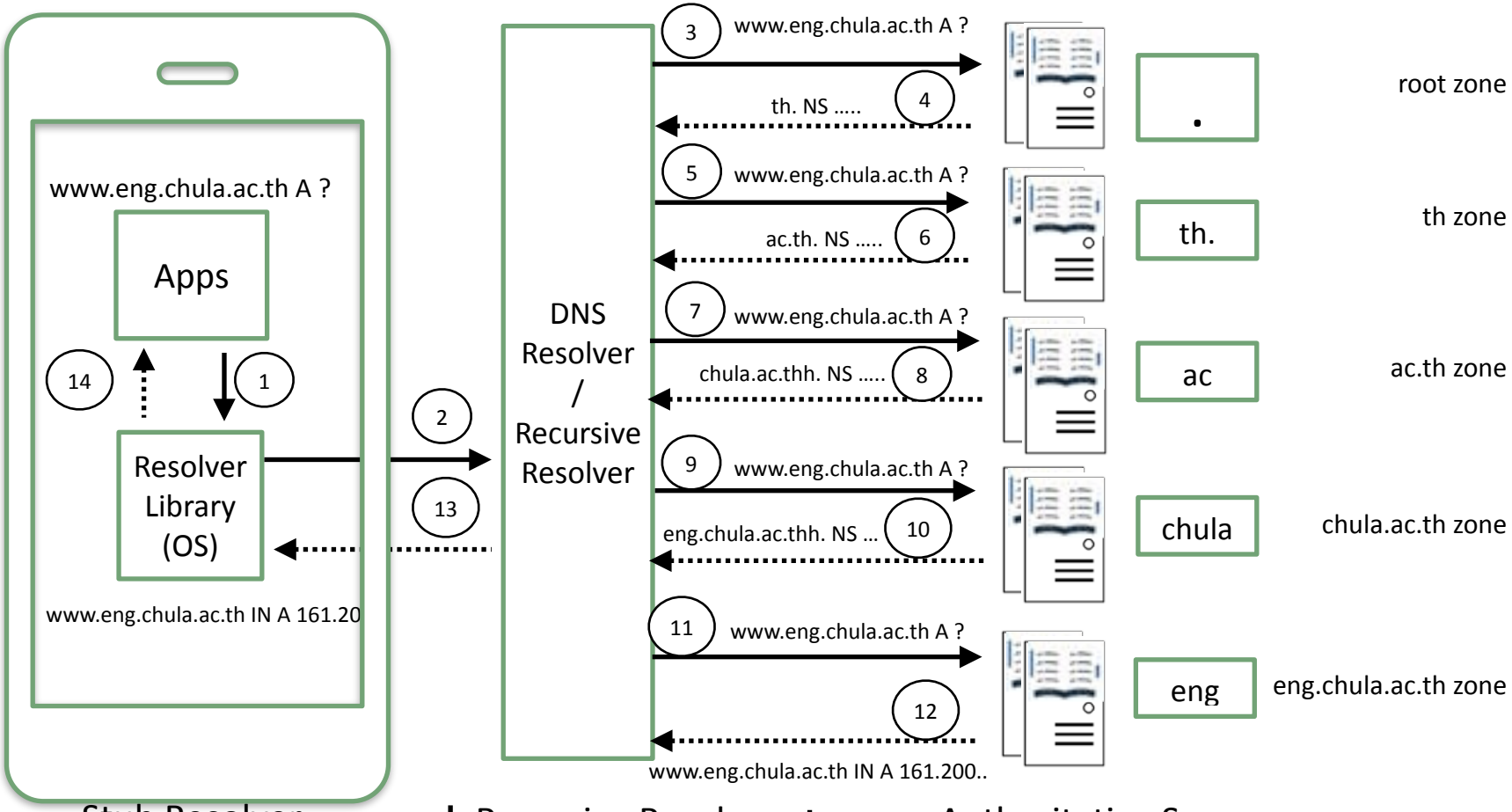
การทำงานของอินเทอร์เน็ตลงลึก



การทำงานของระบบชื่อโดเมน

ถามและตอบผ่าน UDP 53

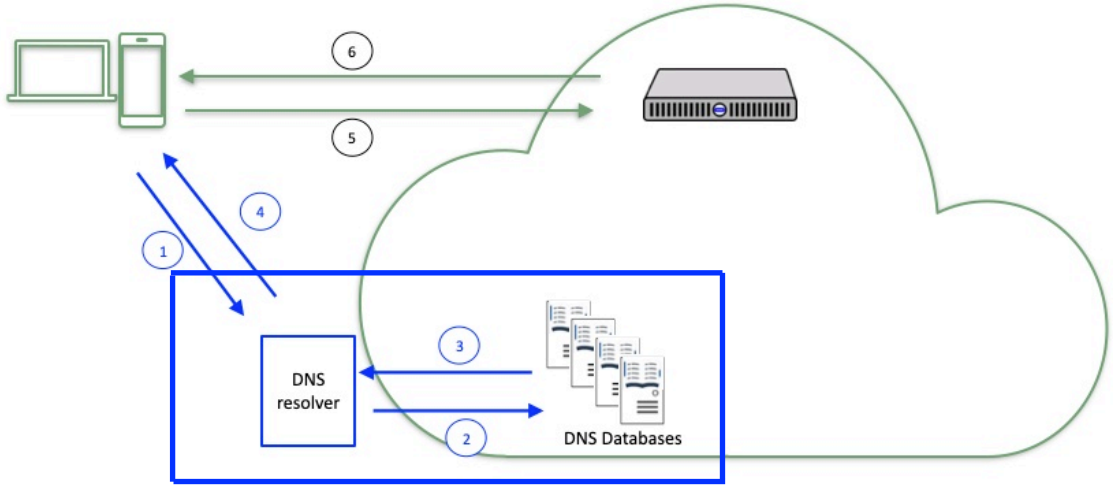
server เหล่านี้อาจจะกระจายอยู่ทั่วโลก



Stub Resolver | Recursive Resolver | Authoritative Servers

servers, laptops, phones, IOT | DMZ/Internet | Internet

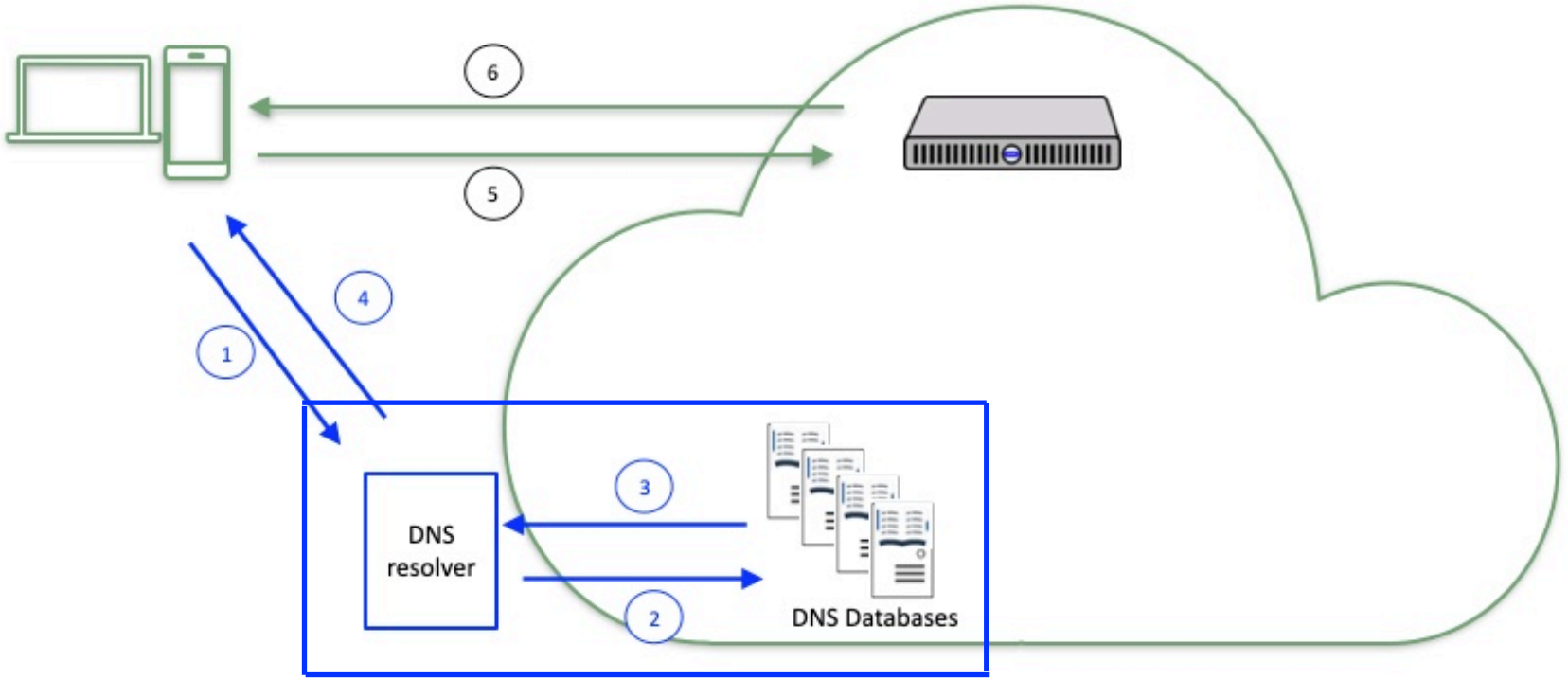
ความสำคัญของระบบชื่อโดเมนกับอินเทอร์เน็ต



ระบบชื่อโดเมนไม่ใช่ระบบทั่วไป
แต่เป็นโครงสร้างพื้นฐานที่สำคัญยิ่งยวด
สำหรับระบบอินเทอร์เน็ต

Domain Name System is not an application but it is the crucial Internet Infrastructure.

ความน่าเชื่อถือของระบบชื่อโดเมน

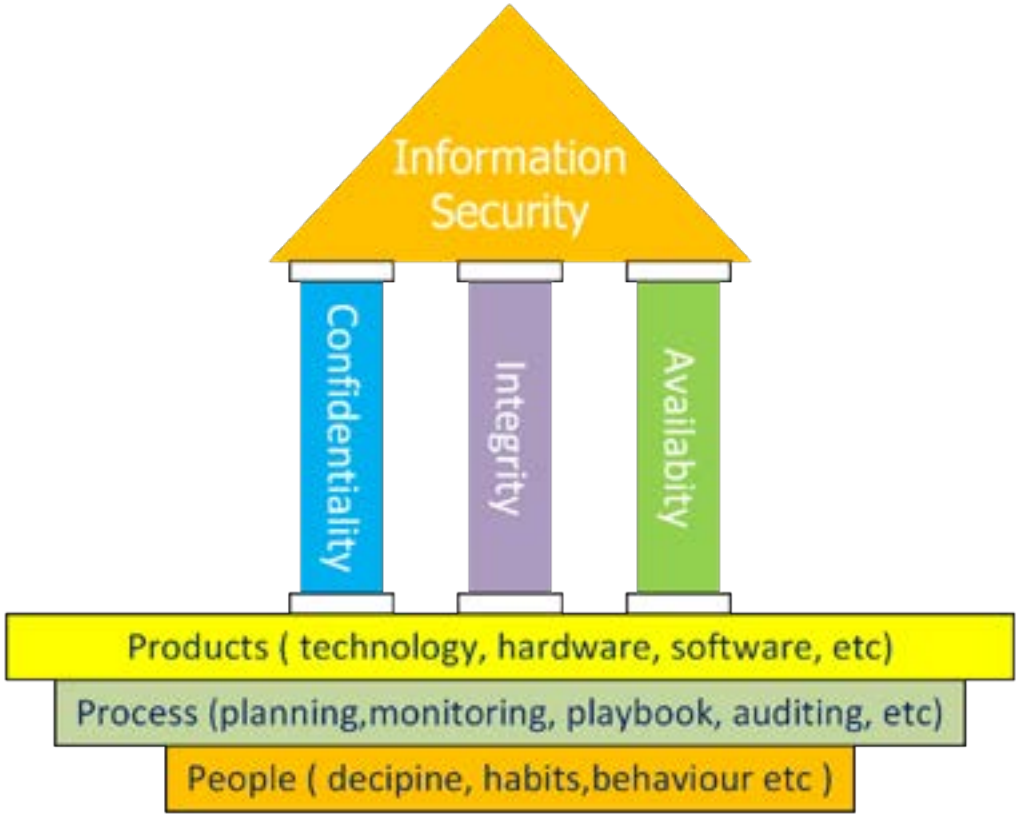


ทุกแอพเชื่อข้อมูลจากระบบชื่อโดเมนโดยไม่มีข้อสงสัยใด ๆ ทั้งสิ้น

แล้ว...ข้อมูลที่ได้จากระบบชื่อโดเมนน่าเชื่อหรือไม่ ??

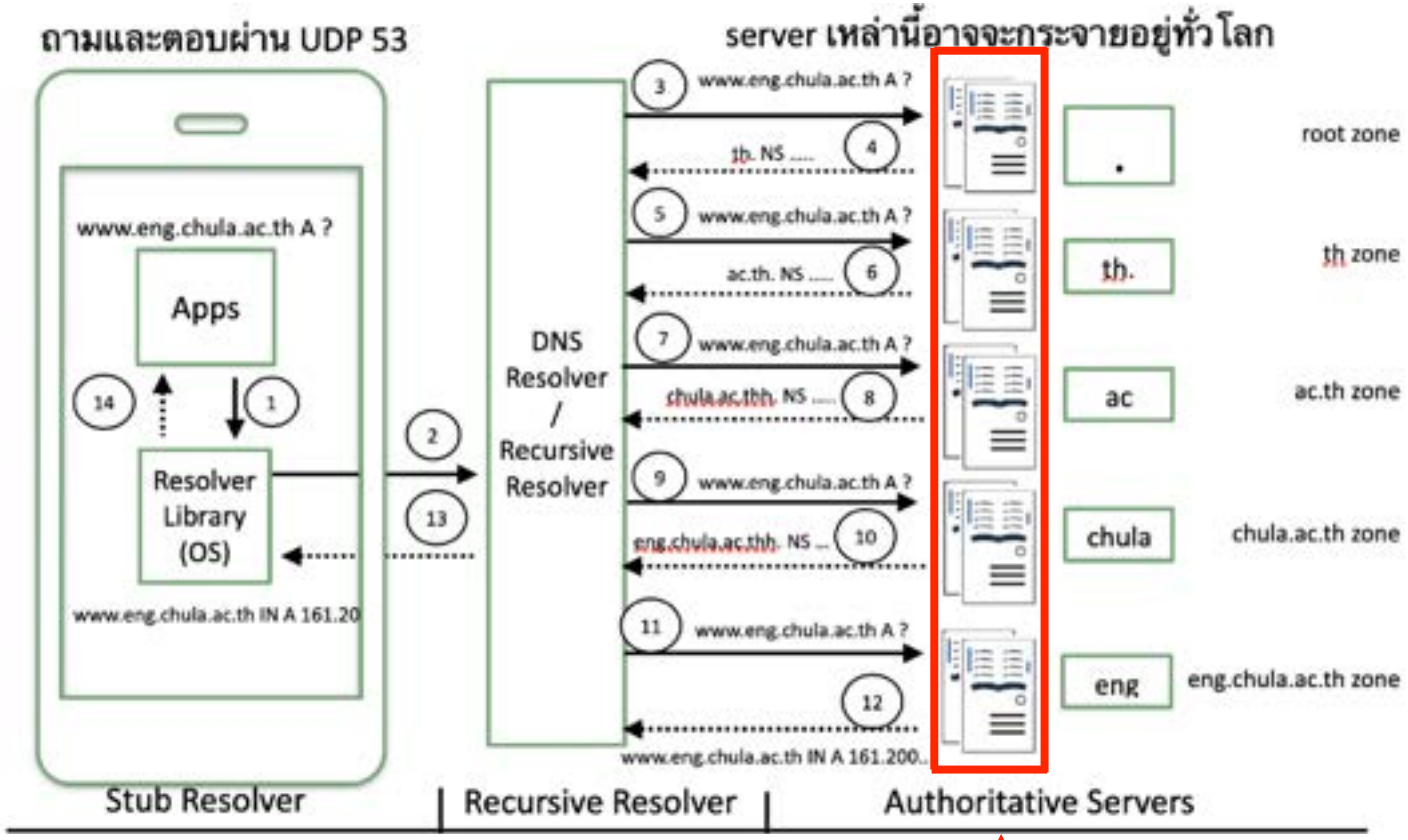
ภัยไซเบอร์ที่เกี่ยวข้องกับชื่อโดเมน

ความมั่นคงปลอดภัยของระบบชื่อโดเมน



https://youtu.be/SWEQ9T6dWUc

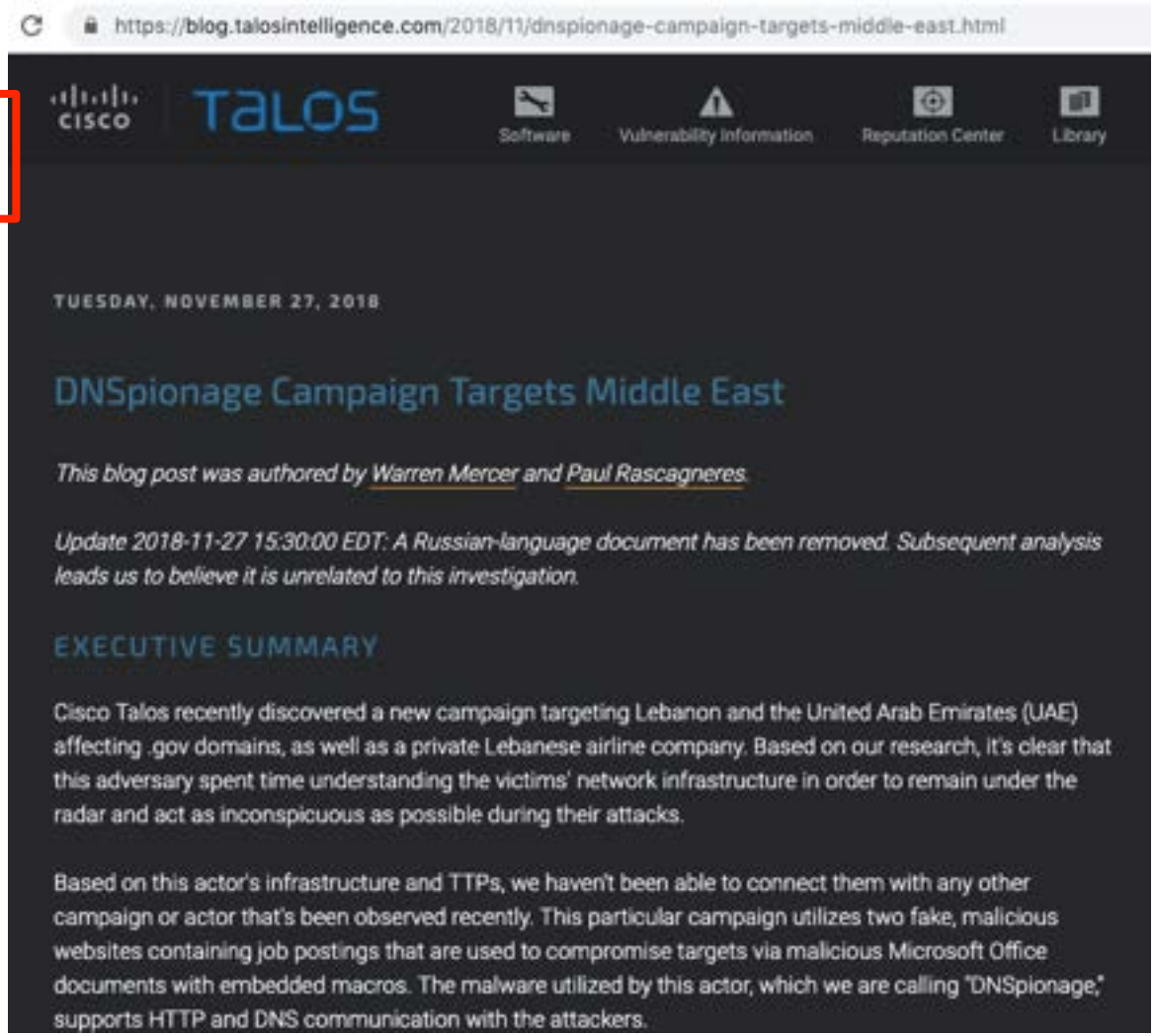
DNS : Integrity



ถ้าข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต

DNS Hijacking ในตะวันออกกลาง

27 พ.ย. 61



https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

สรุปสิ่งที่เกิดขึ้นจากการยึด cc TLD DNS (1)

1. ได้สิทธิแก้ไขข้อมูล DNS (ระดับผู้ใช้หรือระบบ)
2. จัดหา certificate สำหรับโดเมน (https)
3. สร้าง proxy server บนระบบของผู้บุกรุก
4. เปลี่ยน A สำหรับ MX ไปยังระบบของผู้บุกรุก
5. บันทึกชื่อผู้ใช้+รหัสผ่านจากการใช้อีเมล
6. รวบรวมข้อมูลเพื่อใช้ประโยชน์ในอนาคต

สรุปสิ่งที่เกิดขึ้นจากการยึด cc TLD DNS (2)

1.ได้สิทธิแก้ไขข้อมูล DNS (ระดับผู้ใช้หรือระบบ)

2.จัดหา certificate สำหรับโดเมน (https)

3.สร้าง proxy server บนระบบของผู้บุกรุก

4.เปลี่ยน NS สำหรับ TLD ไปยัง NS ของผู้บุกรุก

5.NS ตอบ A ซึ่งเป็น proxy server ของผู้บุกรุก

6.บันทึกชื่อผู้ใช้+รหัสผ่านจากการใช้ proxy

7.รวบรวมข้อมูลเพื่อใช้ประโยชน์ในอนาคต

คำสั่งจาก CISA (1)

Emergency Directive 19-01

22 ม.ค. 62

January 22, 2019

Mitigate DNS Infrastructure Tampering

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 19-01, "*Mitigate DNS Infrastructure Tampering*". Additionally, see the Director's blog post.

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." 44 U.S.C. § 3553(h)(1)–(2)

Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 655(3).

Federal agencies are required to comply with these directives. 44 U.S.C. § 3554 (a)(1)(B)(v)

These directives do not apply to statutorily-defined "national security systems" nor to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. § 3553(d), (e)(2), (e)(3), (h)(1)(B).

https://cyber.dhs.gov/ed/19-01/

คำสั่งจาก CISA (2)

24 ม.ค. 62

Why CISA issued our first Emergency Directive

By Christopher Krebs, Director

January 24, 2019

On Tuesday January 22nd, I released Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*, directing Federal civilian agencies to take a series of immediate actions in response to a global Domain Name System (DNS) hijacking campaign. This is the first Emergency Directive issued by the Cybersecurity and Infrastructure Security Agency (CISA) under authorities granted by Congress in the Cybersecurity Act of 2015, and we took this action after carefully considering the current and potential risk posed to Federal agencies.

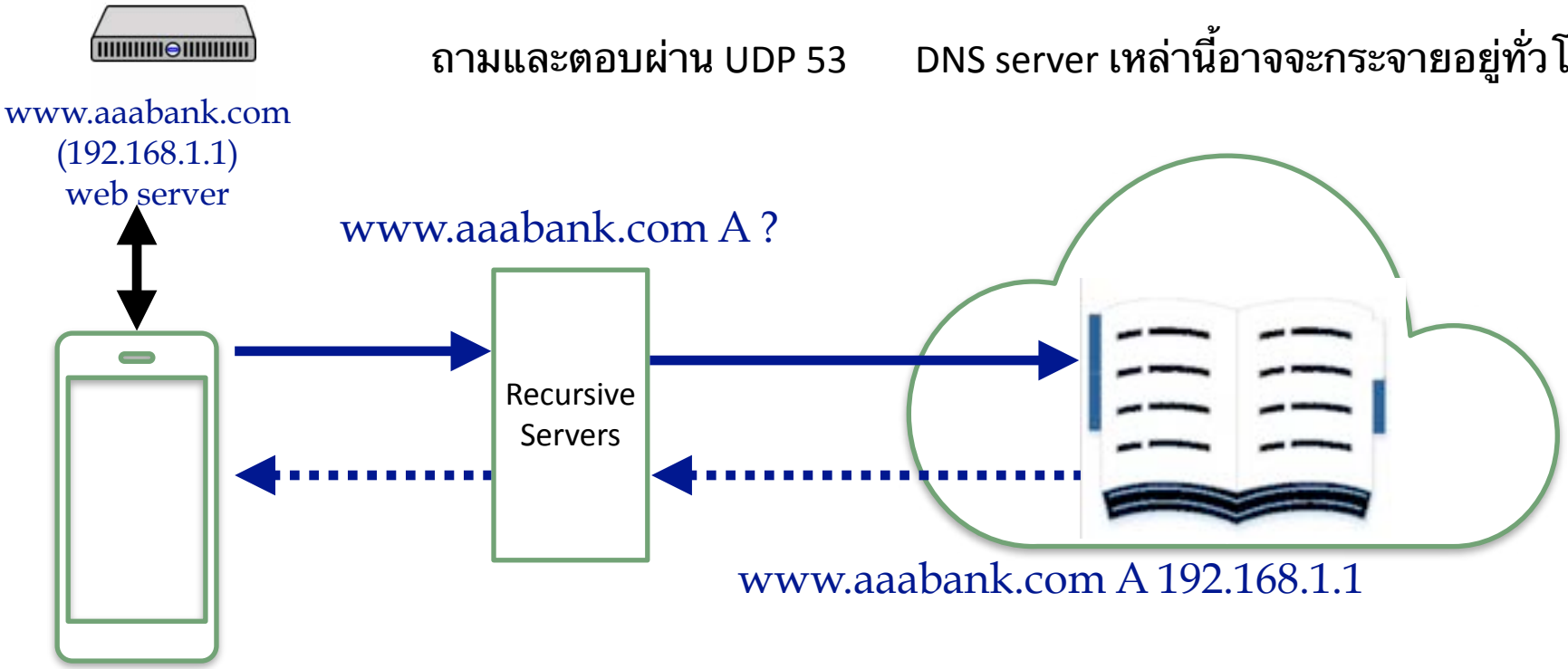
https://cyber.dhs.gov/blog/#why-cisa-issued-our-first-emergency-directive

คำสั่งจาก CISA (3)

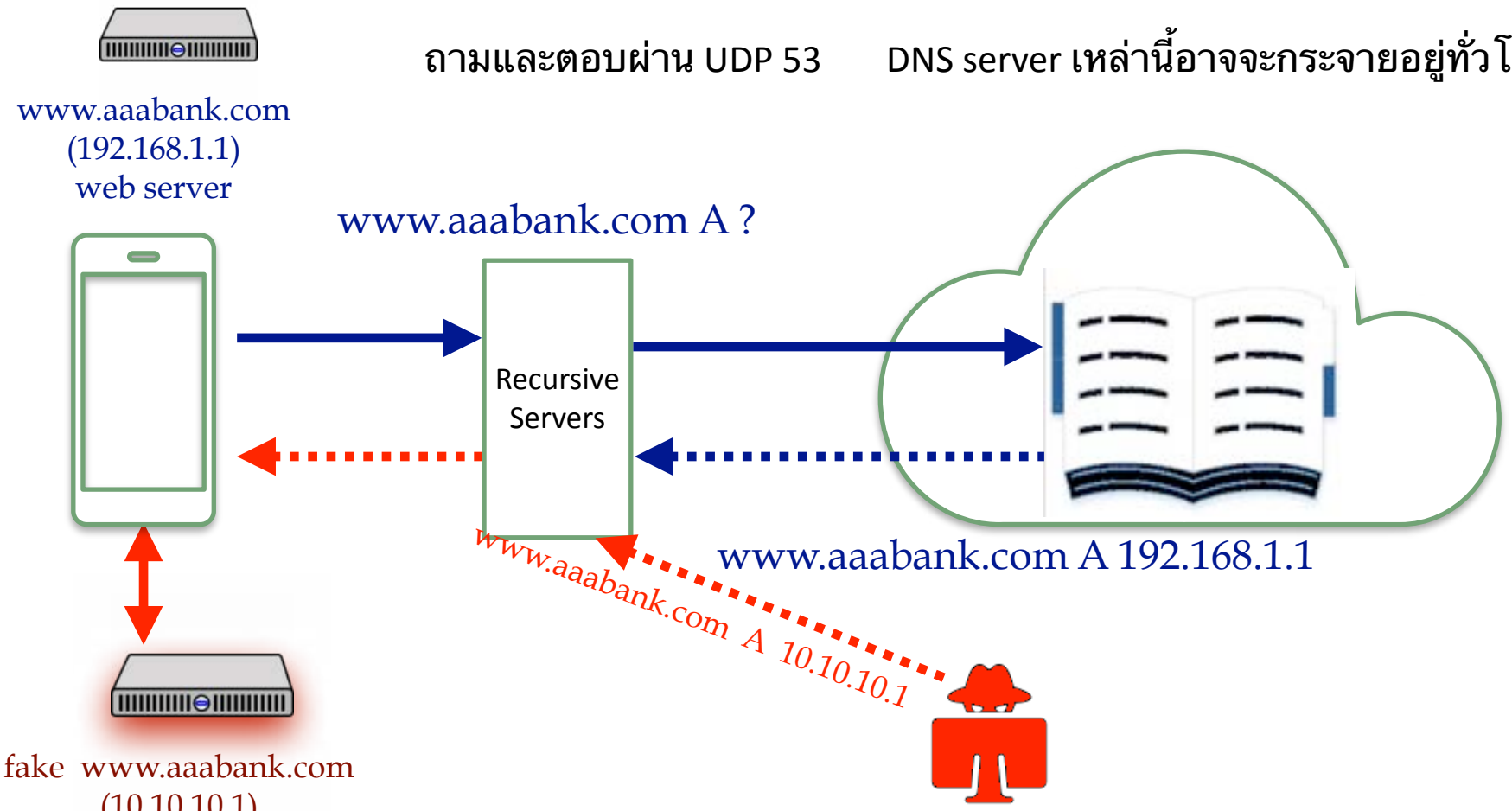
22 ม.ค. 62

- Audit DNS Records
  - ตรวจสอบว่าข้อมูล DNS ถูกต้องภายใน 10 วัน
- Change DNS Account Passwords
  - เปลี่ยนรหัสผ่านของทุกบัญชีที่แก้ไขข้อมูล DNS ได้ภายใน 10 วัน
- Add Multi-Factor Authentication to DNS Accounts
  - เพิ่ม MFA ให้กับทุกบัญชีที่แก้ไขข้อมูล DNS ได้ภายใน 10 วัน
- Monitor Certificate Transparency Logs
  - เริ่มตรวจสอบการเพิ่ม certificate ของโดเมนของหน่วยงานในระบบของ Certificate Transparency (CT) อย่างสม่ำเสมอภายใน 10 วัน

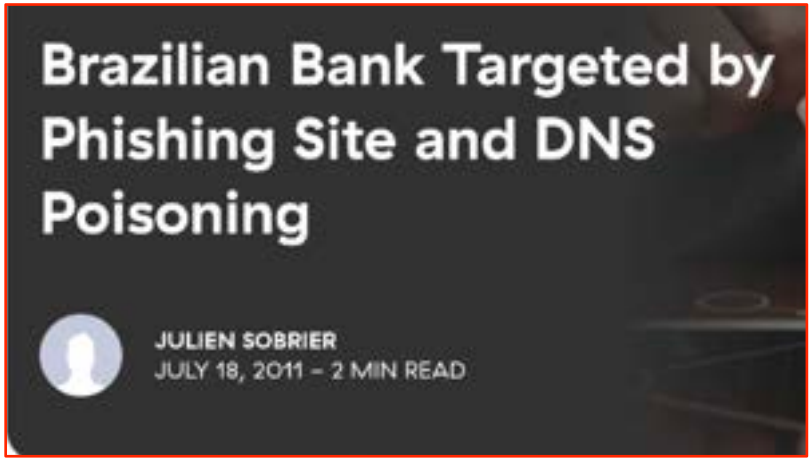
DNS : Integrity



DNS : Integrity Treat



DNS Poisoning



https://www.zscaler.com/blogs/security-research/brazilian-bank-targeted-phishing-site-and-dns-poisoning
https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/dns-hijacking-brazil-banks/

แนวทางสร้างความมั่นคงปลอดภัยให้กับระบบชื่อโดเมน

ICANN ประกาศเรื่องการโจมตีระบบ DNS

15 ก.พ. 62

Alert Regarding Published Reports of Attacks on the Domain Name System

This page is available in: English | العربية | Español | Français | Русский | 中文

LOS ANGELES – 15 February 2019 – The Internet Corporation for Assigned Names and Numbers (ICANN) today announced that it is aware of several recent public reports regarding malicious activity targeting the Domain Name System (DNS). We have no indication that any ICANN organization systems have been compromised, and we are working with relevant community members to investigate reports of attacks against top-level domains (TLDs). For some reporting on this issue, please refer to these sources:

- United States Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive 19-01: "Mitigate DNS Internet Tampering", 22 January 2019.
- "Why CISA Issued our first Emergency Directive", United States DHS CISA blog, 24 January 2019.
- "Global DNS Hijacking Campaign: DNS Record Manipulation at Scale", FireEye, 9 January 2019.
- "Widespread DNS Hijacking Activity Targets Multiple Sectors", Crowdstrike blog, 25 January 2019.
- "Statement on man-in-the-middle attack against Netnod", Netnod statement, 5 February 2019.
- "Revisiting How Registrants Can Reduce the Threat of Domain Hijacking", Verisign blog, 11 February 2019.

https://www.icann.org/news/announcement-2019-02-15-en

ICANN เรียกร้องให้ตรวจสอบข้อมูล DNS โดยใช้ DNSSEC

22 ก.พ. 62

ICANN Calls for Full DNSSEC Deployment, Promotes Community Collaboration to Protect the Internet

This page is available in: English | العربية | Español | Français | Русский | 中文

LOS ANGELES – 22 February 2019 – The Internet Corporation for Assigned Names and Numbers (ICANN) believes that there is an ongoing and significant risk to key parts of the Domain Name System (DNS) infrastructure.

In the context of increasing reports of malicious activity targeting the DNS infrastructure, ICANN is calling for full deployment of the Domain Name System Security Extensions (DNSSEC) across all unsecured domain names. The organization also reaffirms its commitment to engage in collaborative efforts to ensure the security, stability and resiliency of the Internet's global identifier systems.

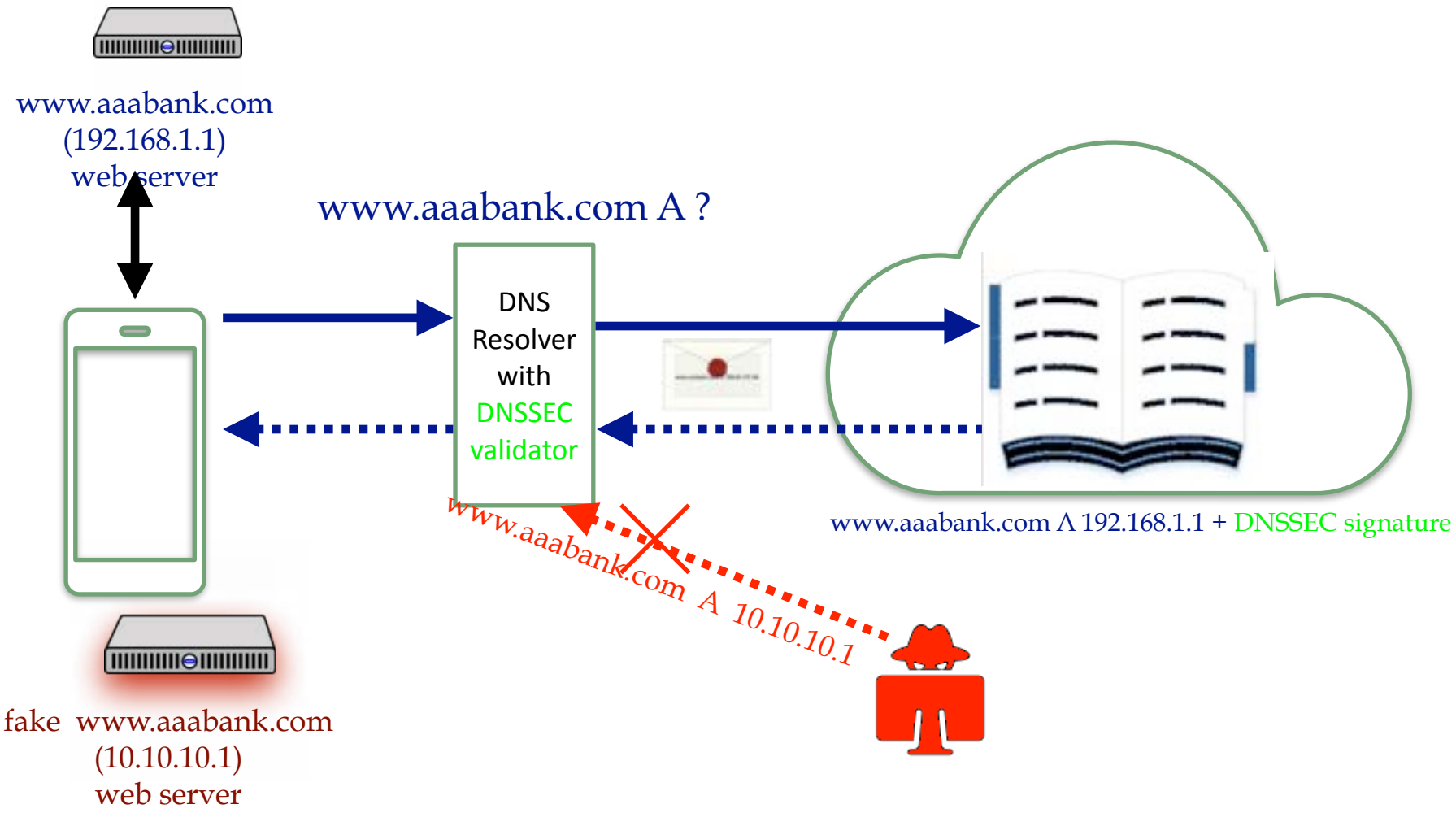
As one of many entities engaged in the decentralized management of the Internet, ICANN is specifically responsible for coordinating the top-most level of the DNS to ensure its stable and secure operation and universal resolvability.

https://www.icann.org/news/announcement-2019-02-22-en

จะใช้งาน DNSSEC ได้อย่างไร

- คำเต็มคือ Domain Name System Security Extensions
- ใช้งานจริงครั้งแรกเมื่อปี 2548 โดย ประเทศสวีเดน (.se)
- ประเทศไทย (.th) ใช้งาน DNSSEC เป็นประเทศแรกในเอเชีย เมื่อปี 2552
- root zone (.) ใช้งาน DNSSEC เมื่อปี 2553
- ผู้ดูแลระบบ (ฝั่งดูแลชื่อโดเมน) ลงชื่อดิจิทัล (sign) ข้อมูลชื่อโดเมนของหน่วยงาน
- ผู้ดูแลระบบ (ฝั่งผู้ใช้งาน / ISP) เปิดใช้งาน DNSSEC validator
- ผู้ใช้ไม่สามารถเปิด (หรือปิด) ได้

DNSSEC in action



ระบบชื่อโดเมนไม่ใช่ระบบทั่วไป
แต่เป็นโครงสร้างพื้นฐานที่สำคัญยิ่งยวด
สำหรับระบบอินเทอร์เน็ต

Domain Name System is not an application but it is the crucial Internet Infrastructure.

ขอเชิญชวนผู้ดูแลระบบทุกภาคส่วน

- ทีมดูแล DNS resolver
  - เปิดใช้งาน DNSSEC Validator
- ทีมดูแลชื่อโดเมนของหน่วยงาน
  - ลงนามดิจิทัลกับชื่อโดเมนของหน่วยงาน
- การจัดทำ TOR หน่วยงานรัฐ
  - กำหนดเรื่องเปิดใช้งาน DNSSEC ในเอกสารจัดซื้อจัดจ้าง
- หน่วยงานกำกับดูแล
  - ให้หน่วยงาน CII เปิดใช้งาน DNSSEC
  - ให้ผู้ให้บริการ (ISP) เปิดใช้งาน DNSSEC

พูด-คุย ถาม-ตอบ