Advancing Network Security Research

Detection

DNS

Counter Measures

Yin Minn Pa Pa
1TC5501B
3rd August,2012(Friday)
11:30AM-1:00PM

• Scope of Studies

DNS

- As an attacker :
  - Have challenge to build Flexible and Reliable Server Infrastructure

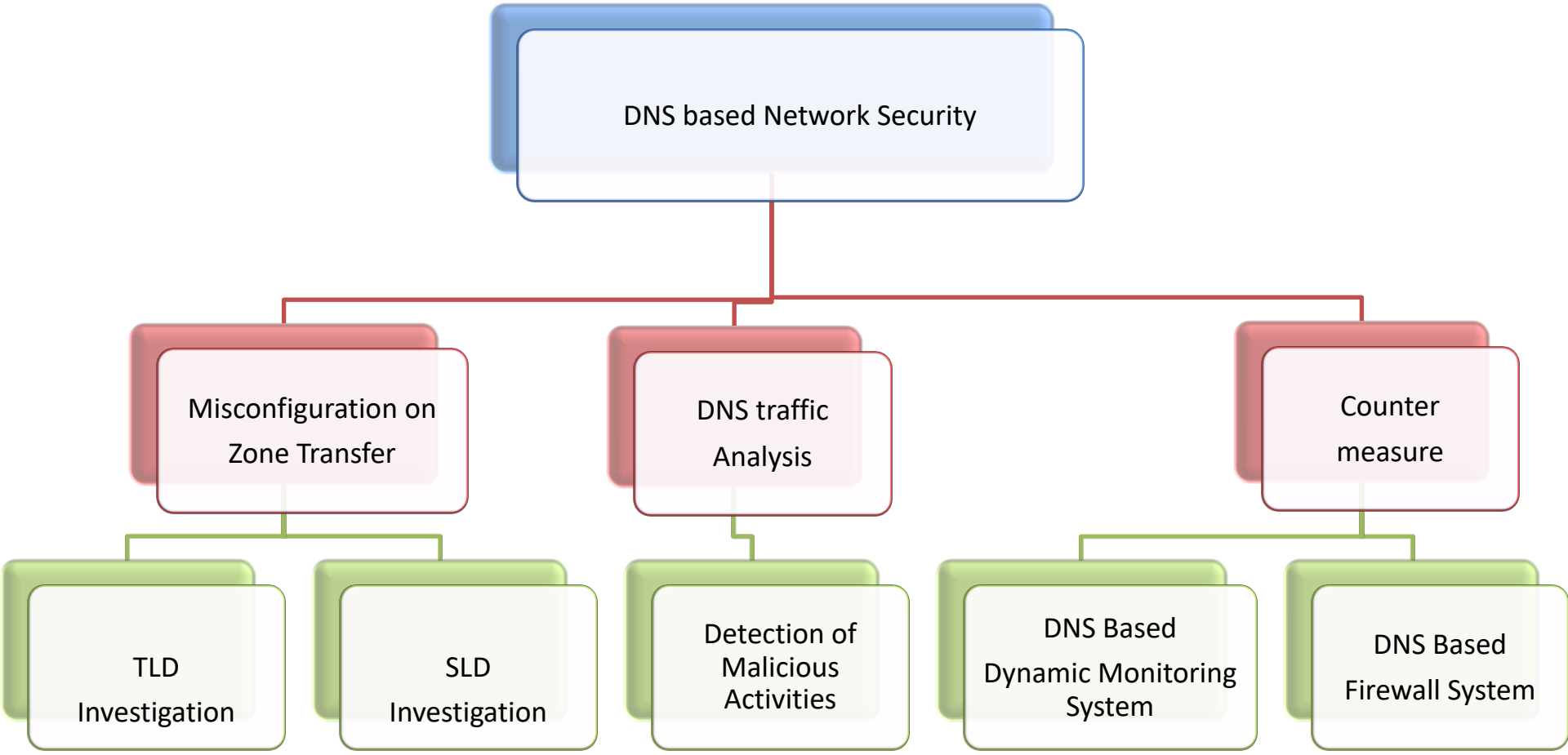
DNS IS EXTENSIVELY USED BY TODAY'S INTERNET APPLICATION
(THE MOST IN TOUCH PROTOCOL TO END USERS)

WORLD WIDE DISTRIBUTED DATABASES
(ROBUSTNESS)

- As a security researcher:
  - Why not think DNS as launch pad for Detection and Counter Measure against malicious activities.

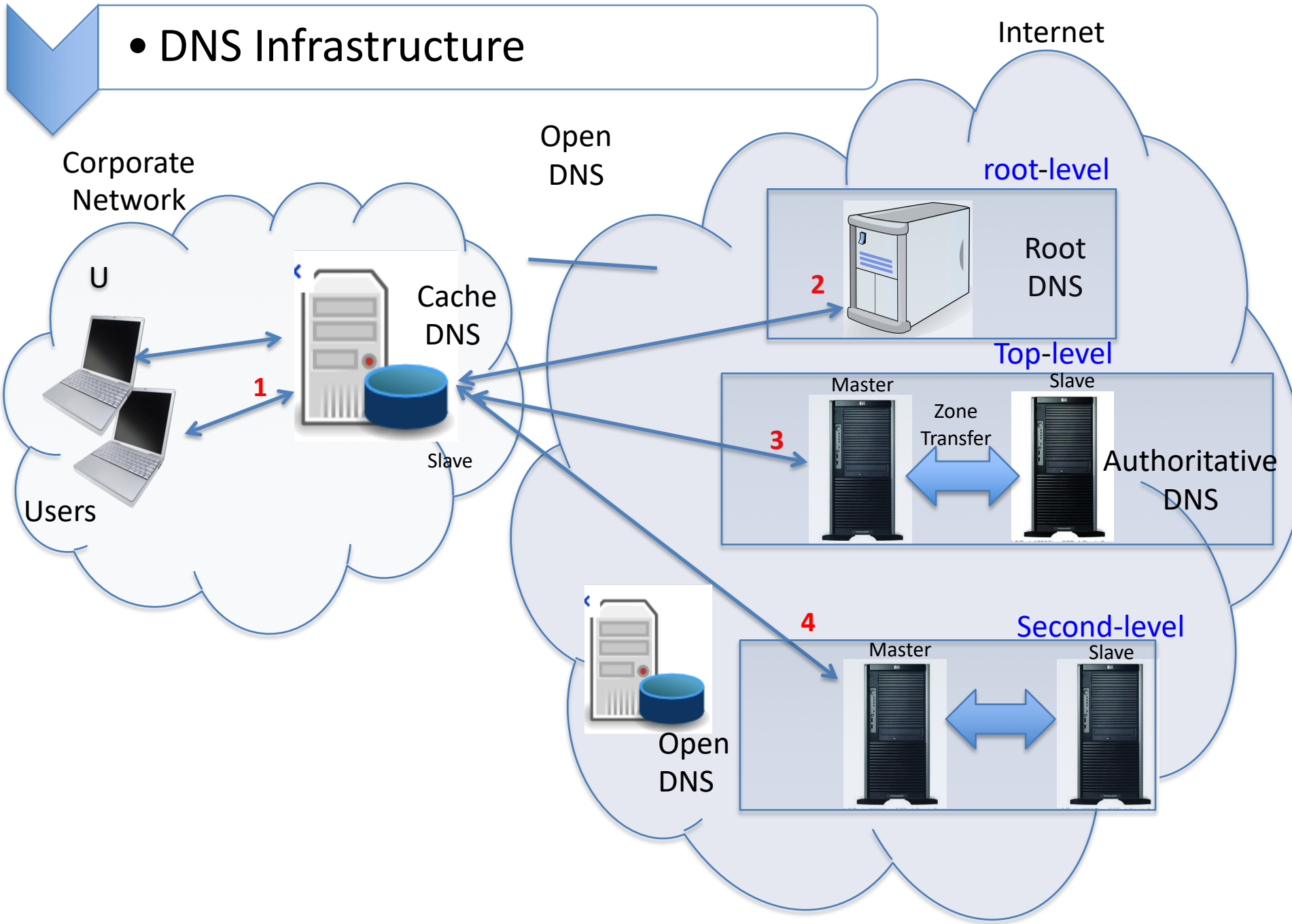
- DNS server problems in Myanmar

• Scope of Studies

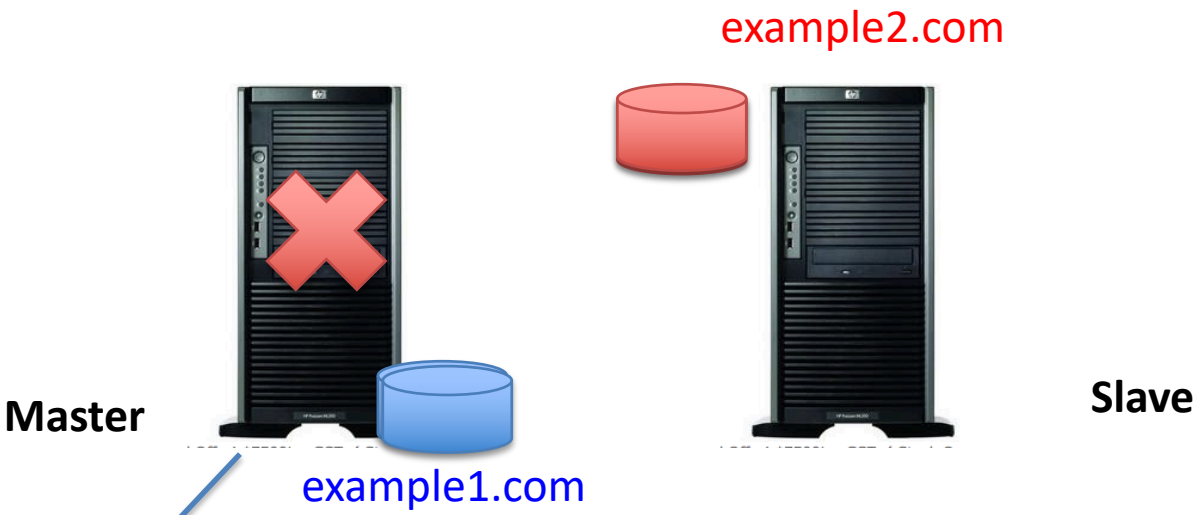


Contents

• DNS Infrastructure



• Overview of Zone Transfer



3

• Current Studies(Investigation on zone transfer)

Search engine based Investigation on misconfiguration of zone transfer in name servers authoritative to answer for TLD and SLD

Related Study

- **Have Legal Issues**
- **At Most two domains**

- **Related Studies (Downloaded Approach)**
  - A.J. Kalafut [1] -> .com/.net
  - Wanrooijet al.[2]->.nl
  - The Measurement Factory [3]-> 3.22% of . com and .net zones

Our Study

- **Legal Issues free approach**
- **Wider Scope of Investigation**
- **Hierarchical Investigation**

• Current Studies(Investigation on zone transfer)

▪ Motivations

▪ When an organization does not use a public/private DNS mechanism to separate its external DNS information from its internal private DNS information, the organization is fully exposed to the Internet.

▪Resource Records (84 different information) can be leaked

Examples:

▪webmail0.zcu.cz. 86400 IN HINFO "PC-SERVER" ”LINUX-OS”

▪RouterBBR-4HG.kek.jp.3600 IN A 130.87.181.132

▪tanabemac3.kek.jp. 3600 IN A 130.87.76.149

▪t.ipmu.jp. 3600 IN TXT "google-site-verification=VLeiAE4TOL9j4jsf_lnu4ltSsjPqTZWeZ8-5sIASQ_8”

▪zonetransfer.me. 301 IN TXT "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS changes”

▪dzc.zonetransfer.me. 7200 IN TXT "AbCdEfG"

▪testing.zonetransfer.me. 301 IN CNAME www.zonetransfer.me.

▪_sip._tcp.zonetransfer.me. 14000 IN SRV 0 0 5060 www.zonetransfer.me.

3

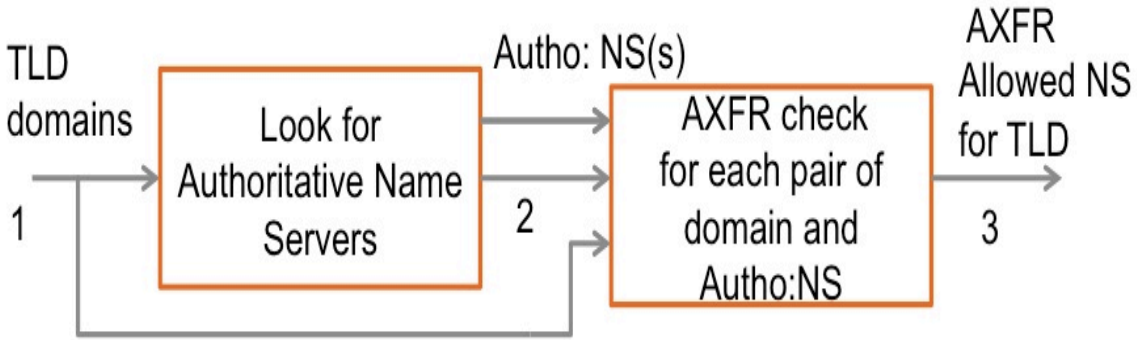
• Current Studies(Investigation on zone transfer)

▪ Data Collection

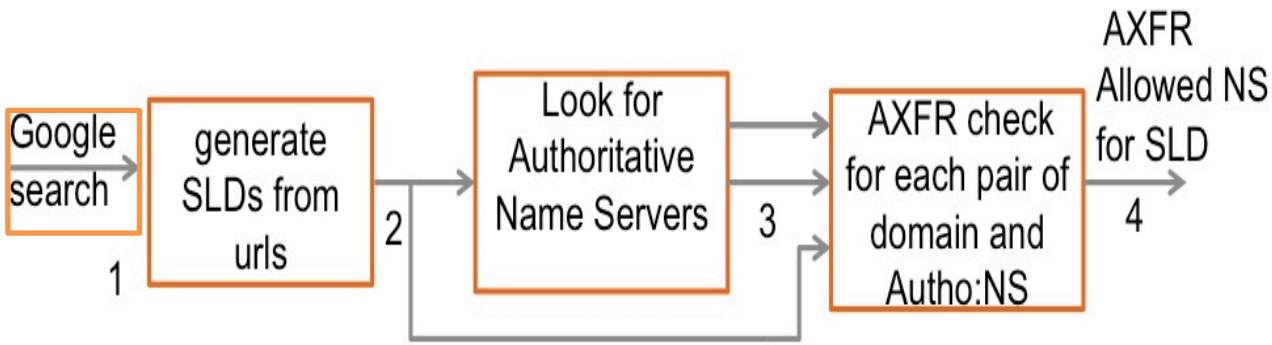
- According to IANA(Internet Assigned Number Authority)
  - ccTLD -> 249
  - gTLD -> 22
  - IDN -> 4
- By the result of scripts (Net:DNS)
  - Total domains for the investigation -> 314
  - Authoritative Name Servers for 314 domains -> 1284
- Google Site Search for SLDs
  - Sites of ccTLD (Multi Link Add-on) -> 156,648
  - Filtered Second Level domains -> 34,164
  - Authoritative Name Servers for 34,164 domains -> 46,416

• Current Studies(Investigation on zone transfer)

- Methodology



TLD investigation Steps
1.TLD list
2.Query NS
3.Query A
4.Query SOA
5.Authority Check
6.Check AXFR



SLD Investigation Steps
1Google Approach
2.Generate SLD
3.Query NS
4.Query A
5.Query SOA
6.Authority Check
7.Check AXFR

3

• Current Studies(Investigation on zone transfer)

- Results(Both TLD and SLD layers)

Level	Domains	Vulnerable	%	Name Servers	Misconfigure Name Server (by domain)	Misconfigure Name Server (by IP)	%
Top-level	314	53	17	1,284	84	82	7
Second Level	34,164	6,234	18	46,416	5,394	4,973	12

3

• Current Studies(Investigation on zone transfer)

- Results(Top-Layer -ccTLDs)

- Top-level domains that allow zone transfer to anyone for their domains are:
  - [AERO. AN. AO. ARPA. AW. BB. BD. BI. BM. BV. CI. CR. CW. CY. DO. ER. ET. FO. GD. GE. GP. GQ. GT. GY. INT. IQ. KM. KW. MC. MG. ML. MO. MP. MW. NI. NP. PF. PG. PK. PW. SC. SJ. SL. SV. TC. TJ. TO. UK. VG. XN--FZC2C9E2C. XN--XKC2AL3HYE2A. XN--YGBI2AMMX. YE.]
  - (As of July 15 ,2012)
- 9 top-level domains (.bv,.cs,.dd,.eh,.gb,.pw,.sj,.ss,.yn) are not currently in active.

• Current Studies(Investigation on zone transfer)

- Results(Second Layer-SLD)

Fig-Percentage of Misconfiguration

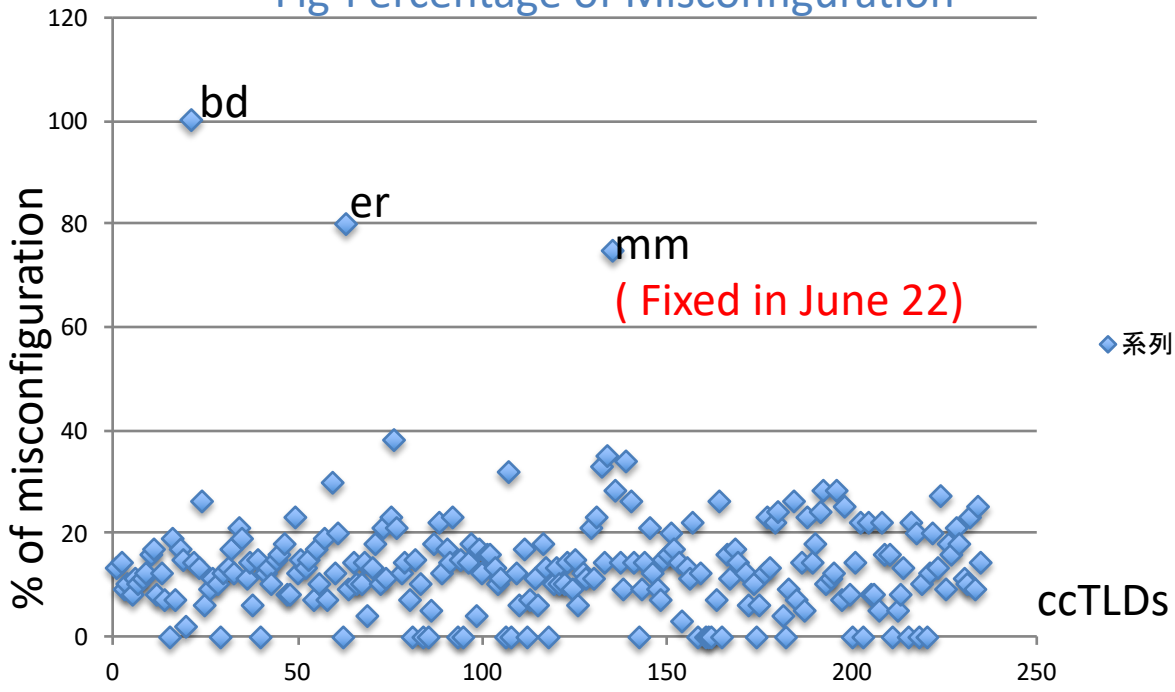
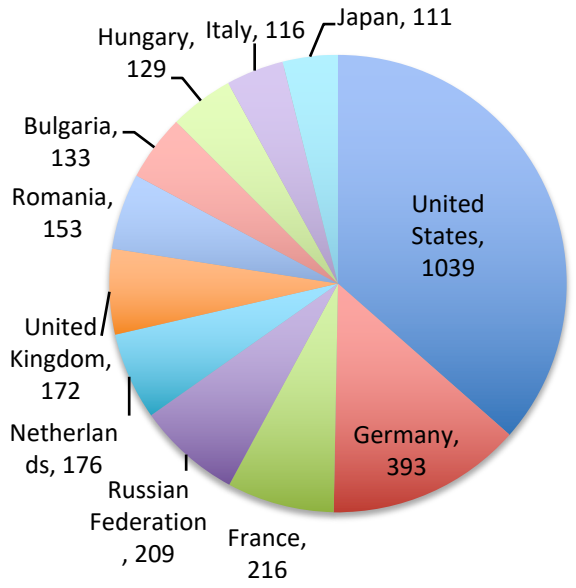
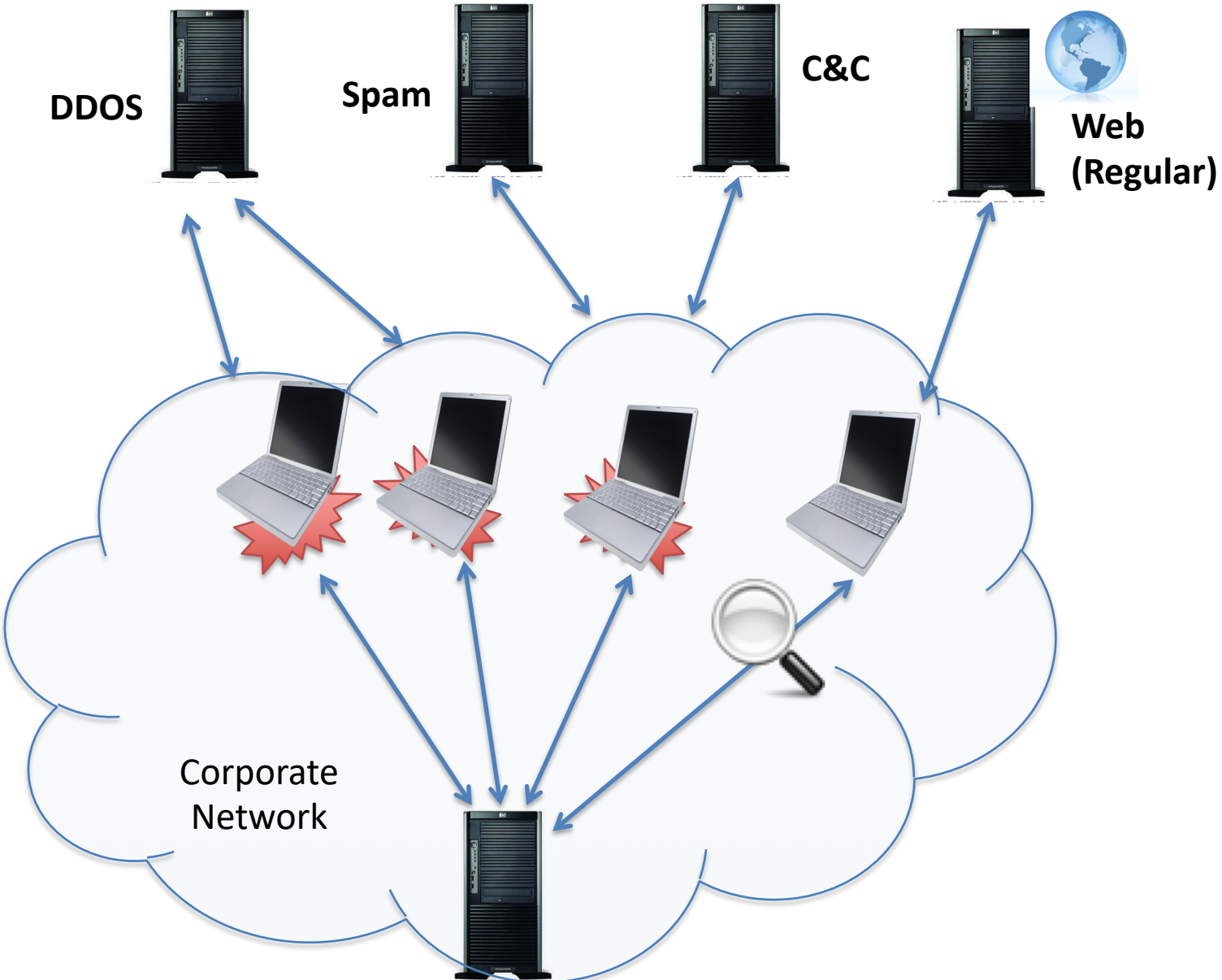


Fig-Location of Misconfigured DNS



- ck,fj,fk,gn,gt,jm,lr,sv) -> No Name Server for SLD
- 27 ccTLDs -> No Misconfiguration in both TLD & SLD
- bd,er,mm -> Misconfiguration on both TLD & SLD

• DNS Traffic and Malicious Online Activities



3

• Current Studies(DNS traffic Analysis)

- Main Objective
  - To characterize the signatures of DNS traffic of malicious activities
  - To identify the infected hosts with high probability

Related Study

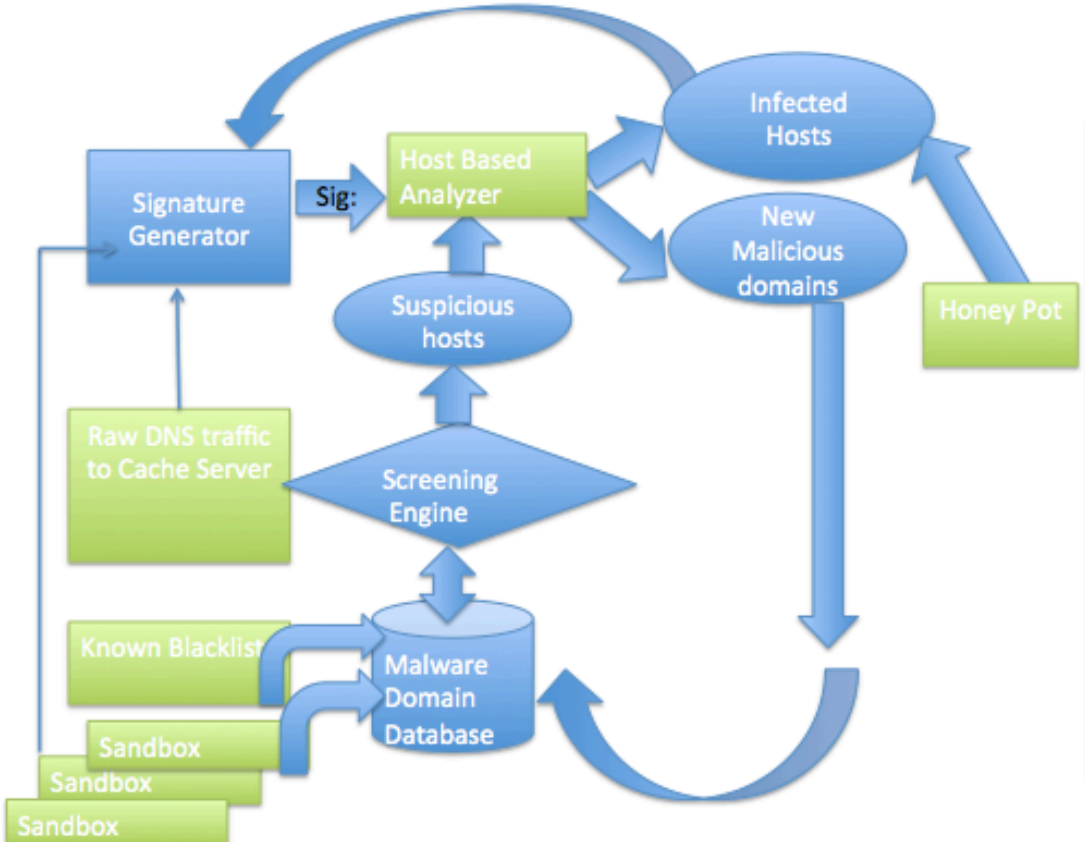
- Notos: [4]
  - Dynamically assigns reputation scores to domains before maliciousness has not been detected
- EXPOSURE: [5]
  - 15 Features of malicious DNS activities
  - Detection of Malware domains
- Kopis: [6]
  - Upper DNS Hierarchy traffic analysis
  - Detection of Malware domains

Our Study

- Host Based Analysis
- Malicious DNS features from Sandbox DNS traffic

• Current Studies(Analysis on DNS traffic)

- Design



- Screening
  - Matching with Known Blacklist
  - Behavioral Similarity
- Host Based Analysis
- Update Blacklist
- Update Behaviors
- Update Blacklists

3

• Current Studies(Analysis on DNS traffic-Packet)

- Results(Spybot)

- Spybot DNS traffic
  - Nature of DGA -> Third Level domains pattern
  - Eg-
    - *.hn.org 147
    - *.afraid.org 148
    - *.yi.org 147
    - *.dynserv.com 148
  - A Queries for Mail/Web?
    - Week 1->(3091/130491 uniq A? queries)(DGA generated domains)
    - Week2 ->(2284/173237 uniq A? queries)new domains= 1430
    - Week 3 ->(24/190314 uniq A? queries) new domains =10
    - Week 4 ->(31/137417 uniq A? queries)new domains= 8
    - Week 5 ->(19/148462 uniq A? queries) new domains=1
    - Week 6 ->(25/116968 uniq A? queries)no new domain
    - All unique domains for 6 week (A Queries for Web)(not MX related)= 4609

3

- Current Studies(Analysis on DNS traffic – Cache Log)
- Results(Domestic University/Domestic Research Center)

- Domestic University Log Data(29 to 1 July 2012)
  - Found malware related domains = 41
  - Suspicious IPs = 255

    (Matching with known malicious domains list)

- Domestic Research Center Log Data(July 10, 2012)
  - Found malware related domains=29
  - Suspicious IP = unknown IP information

3

• Current Studies(Analysis on DNS traffic-Packet)

- Project Overview (Myanmar ISP's DNS traffic)

- Collaborative Research with Ministry of Communications, Posts and Telegraphs and Research Center for Information and Physical Security by Asia Pacific Telecom Fund provided to Myanmar.

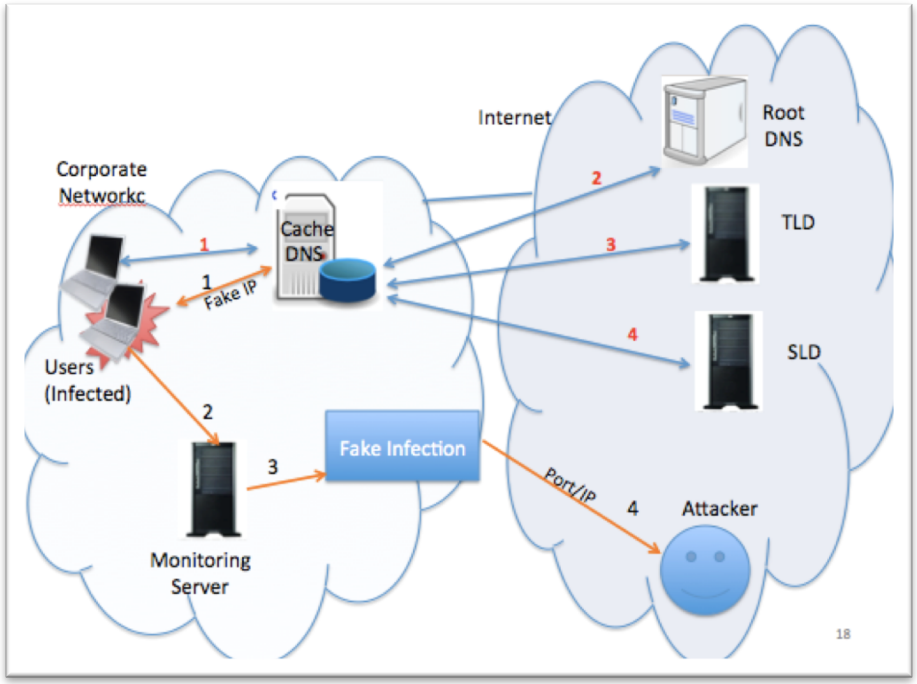
- Objectives
  - To identify malware infected hosts
  - To reduce the damage penetrated by malicious online activities
  - To improve quality of Services on Internet Security

- Purpose
  - To deploy a monitoring system in Myanmar's environment based on the research experience
  - To improve Human Resource Development
  - To get collaboration experience with a developed country

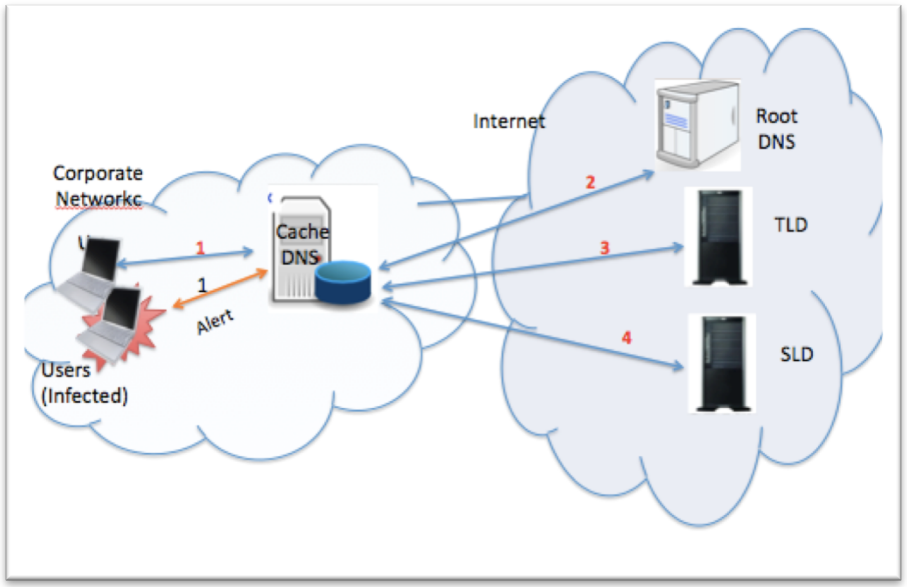
4

- Future Studies

Developing Countermeasures for the infected hosts



Counter Measure Design 1



Counter Measure Design 2

5

• Expected Contributions from Future Studies

- Novel DNS based Counter Measure System for the Infected Hosts

- New DNS firewall for the cooperate Network

6

• References

[1] A. J. Kalafut, C. A. Shue, and M. Gupta, “Touring DNS open houses for trend and and configurations,” *IEEE ACM Transactions on Networking*, vol. 19, no. 6, p. 1666, 2011

[2] W. van Wanrooij and A. Pras, “DNS zones revisited,” in Open European Summer School and IFIP WG6.4/6.6/6.9 Workshop (EUNICE), 2005

[3] The Measurement Factory, “DNS survey: October 2007,” http://dns.measurement-factory.com/surveys/200710.html.

[4] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster, “Building a dynamic reputation system for DNS,” in *19th Usenix Security Symposium*, 2010.{NOTOS}

[5] S. Hao, N. Feamster, and R. Pandrani, “Monitoring the Initial DNS Behavior of Malicious Domains,”2011”{EXPOSURE}

[6] M. Antonakakis, R. Perdisci, W. Lee, N. Vasiloglou II, and D. Dagon, “Detecting malware domains at the upper dns hierarchy,” in *Proceedings of the 20th USENIX Security Symposium, USENIX Security*, 2011, vol. 11, pp. 27–27.{Kopis}

Paper submission Plan to CSS2012 :

Title - Search Engine Based Investigation on Misconfiguration of Zone Transfer