ACM Winter School
NISER, Bhuvaneshwar

16th December 2019

Speaker: *Gopinath Palaniappan*

Part 1: MALWARE ANALYSIS

Part 2: DNS & ATTACKS USING THEM

Part 3: MALICIOUS DOMAIN DETECTION

Part 1:

MALWARE ANALYSIS

An Introduction

Outline

- What is Malware?
- Why Malware?
- Harmful effects of Malware
- Spreading of Malware
- Popular types of Malware
- Popular carriers of Malware
- Stages of Malware Exploit plan
- Malware Creators
- Dimensions of Malware Detection
- Techniques for Malware Analysis & Detection
- Case Study
- Demonstration

What is Malware?

Malware = **Mal**icious Soft**ware**

- **Exploit** - a software designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware, taking control, stealing data, etc.
- **Payload** - is that part of the exploit which actually performs the intended malicious action. e.g. Opening a backdoor, installing keyloggers, stealing or tampering data, etc.

Why Malware?

- **Money**
- **Fame/Defame**
- **Destruction**
- **Cyber warfare**
- **3352 Malware detected per minute i.e. 434 million in Q1 2019 (Quick Heal)**

Harmful effects of Malware

- Hamper availability of a service (DoS/DDoS)
- Compromise privacy (steal data)
- Undesirable results of software
- Financial or Infrastructural loss
- Prank
- Impacts: Health, Banking, Business, Politics, Social Media, etc.

Spreading of Malware

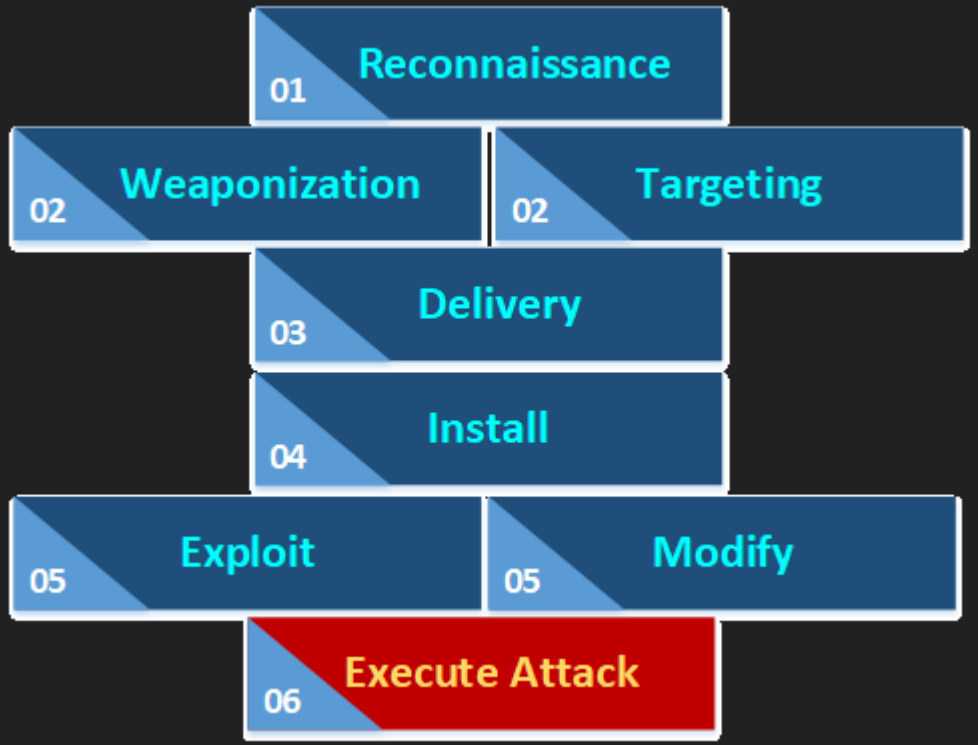
- **Websites** *(links, compromised websites)*
- **Email** *(attachments, links)*
- **Physical media** *(storage devices)*
- **Software download** *(trojan)*
- **File sharing**

Popular types of Malware

- **Virus** *(infects a program)*
- **Worm** *(crawls through a network spreading infection)*
- **Trojan Horse** *(masquerades/misleads)*
- **Backdoor** *(command & control)*
- **Rootkit** *(super-user privileges)*
- **Adware** *(advertisements)*
- **Botnets** *(zombies)*
- **Ransomware** *(refuse access by encryption)*
- **Spyware** *(keylogging, online behaviour)*
- **Browser hijacker** *(crypto-miner)*

Popular carriers of Malware

Stages of a Malware Exploit Plan



Malware Creators

Naive Malware Creators

- Self conceptualized ideas

Sophisticated Malware Creators

- Self conceptualized ideas
- Common Vulnerabilities Exposure (CVE)
  - Stuxnet attacks on Iran's Natanz nuclear plant - Shell flaw (CVE-2010-2772, CVE-2010-2568) in Windows
  - Wannacry, Brambul Worm - Server Message Block (SMB) vulnerability (CVE-2017-0143/4/5/6/8)

Dimensions of Malware Detection

Techniques for Malware Analysis & Detection

Signature-based

- Similar or re-packaged malware detection only

Static Analysis

- Determine the functionalities without executing the software

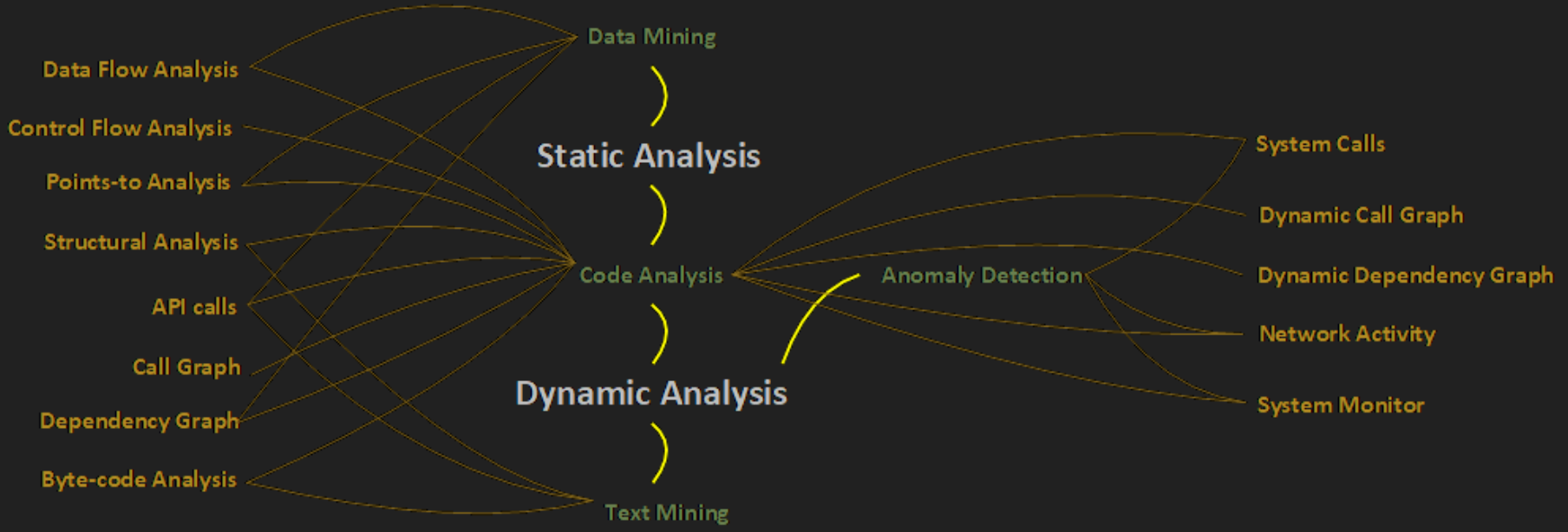
Dynamic Analysis

- Determining the functionalities by executing the software in a restricted environment

Supplementary Techniques

- Machine Learning
- Natural Language Processing
- Data/Text Mining

Techniques for Malware Analysis and Detection



Case Study

- **https://coednssecurity.in/pdf/An_Intrusion_using_Malware_and_DDNS.pdf**

Demonstration

Online Tools

https://www.virustotal.com/

http://www.hybrid-analysis.com

Desktop Tools

IDA pro

Part 2:

DNS AND ATTACKS USING THEM

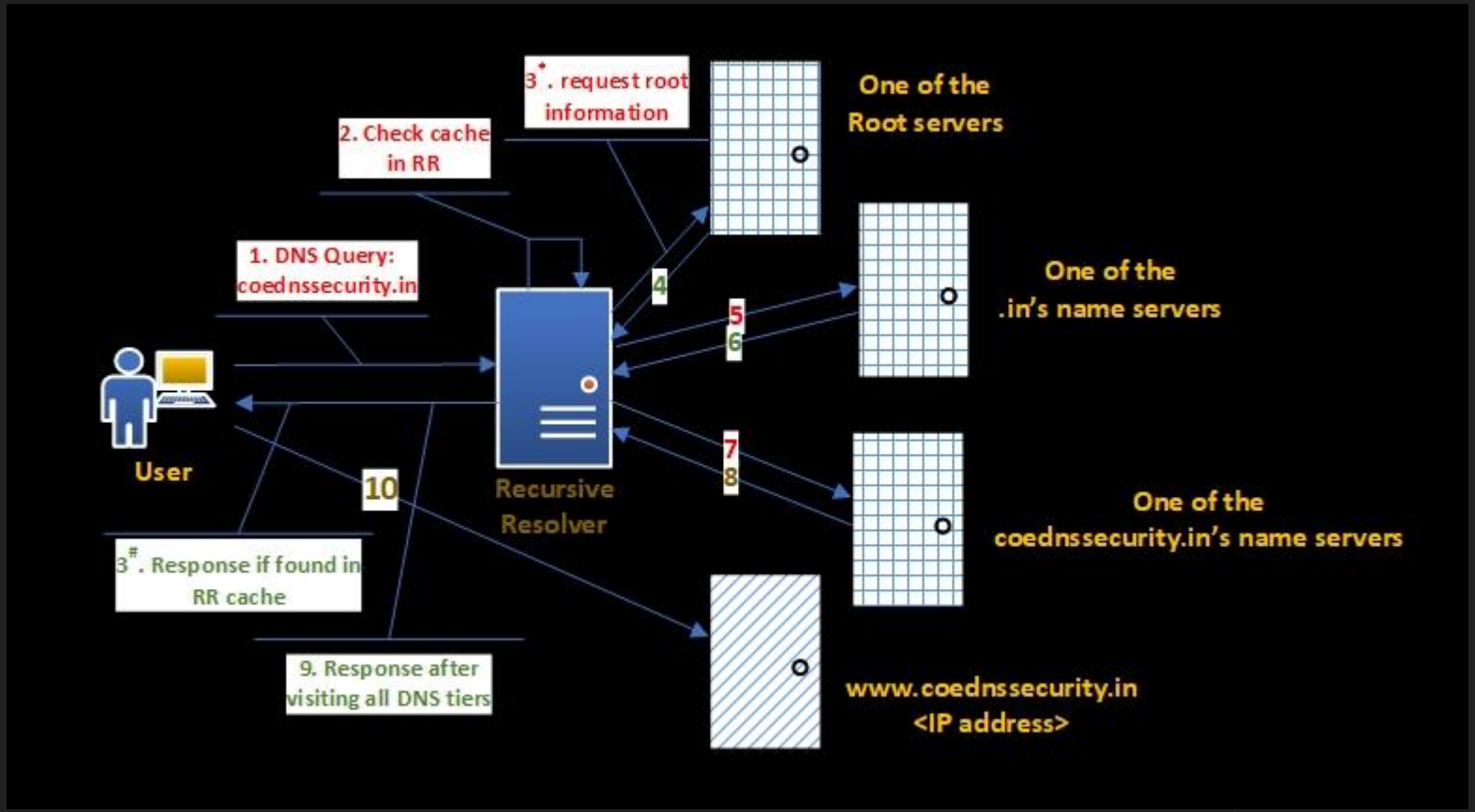
Outline

- What is DNS?
- How DNS works
- DNS Ecosystem
- Contractual relationships in DNS ecosystem
- Domain Name hierarchy
- Common DNS record types
- Popular Attacks using DNS
  - DNS Amplification Attack
  - DNS Changer
  - DNS Tunneling

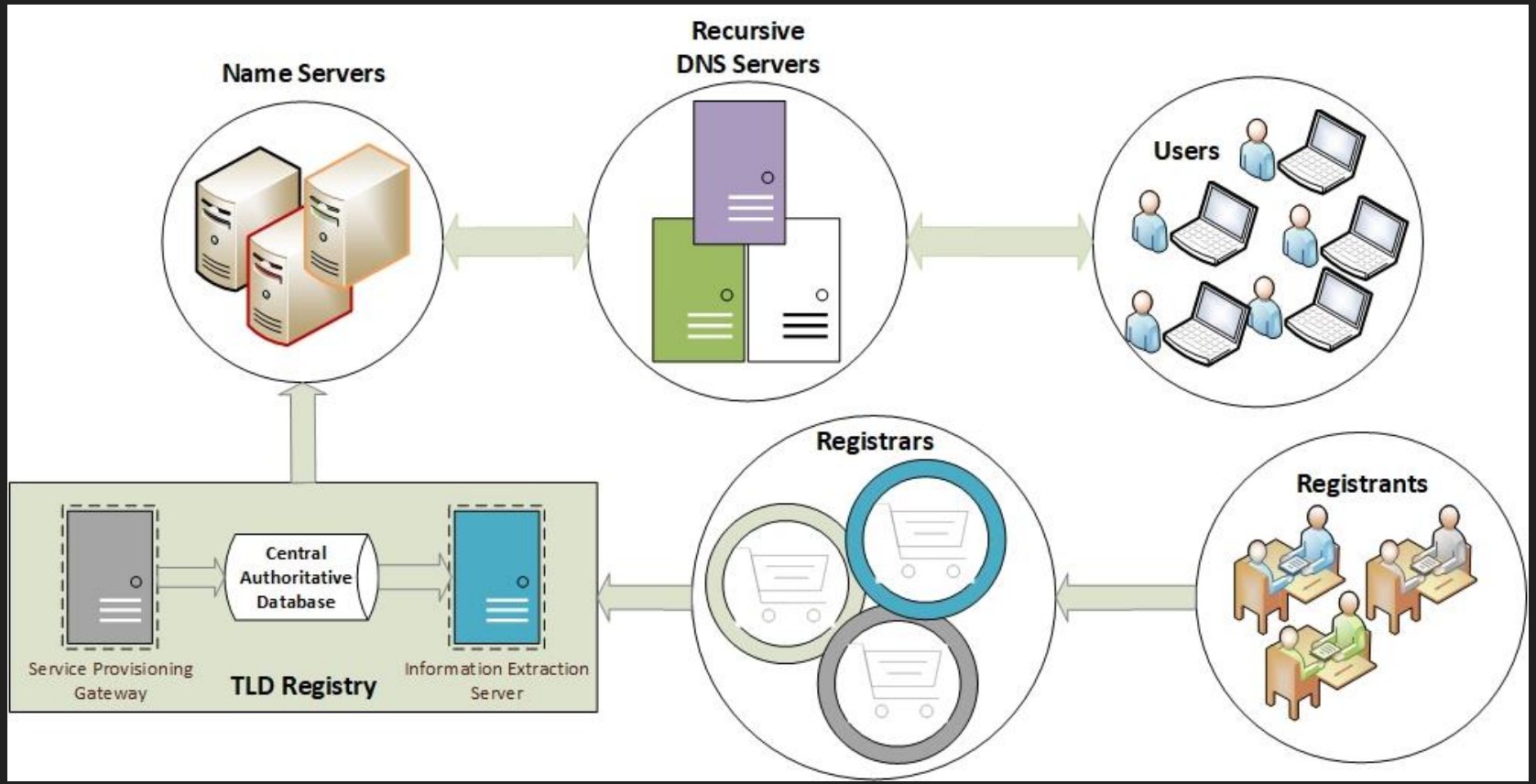
What is DNS ?

- **The Domain Name System (DNS) is one the vital elements in the Internet. Due to the importance of DNS, it's been the target of attacks by attackers**

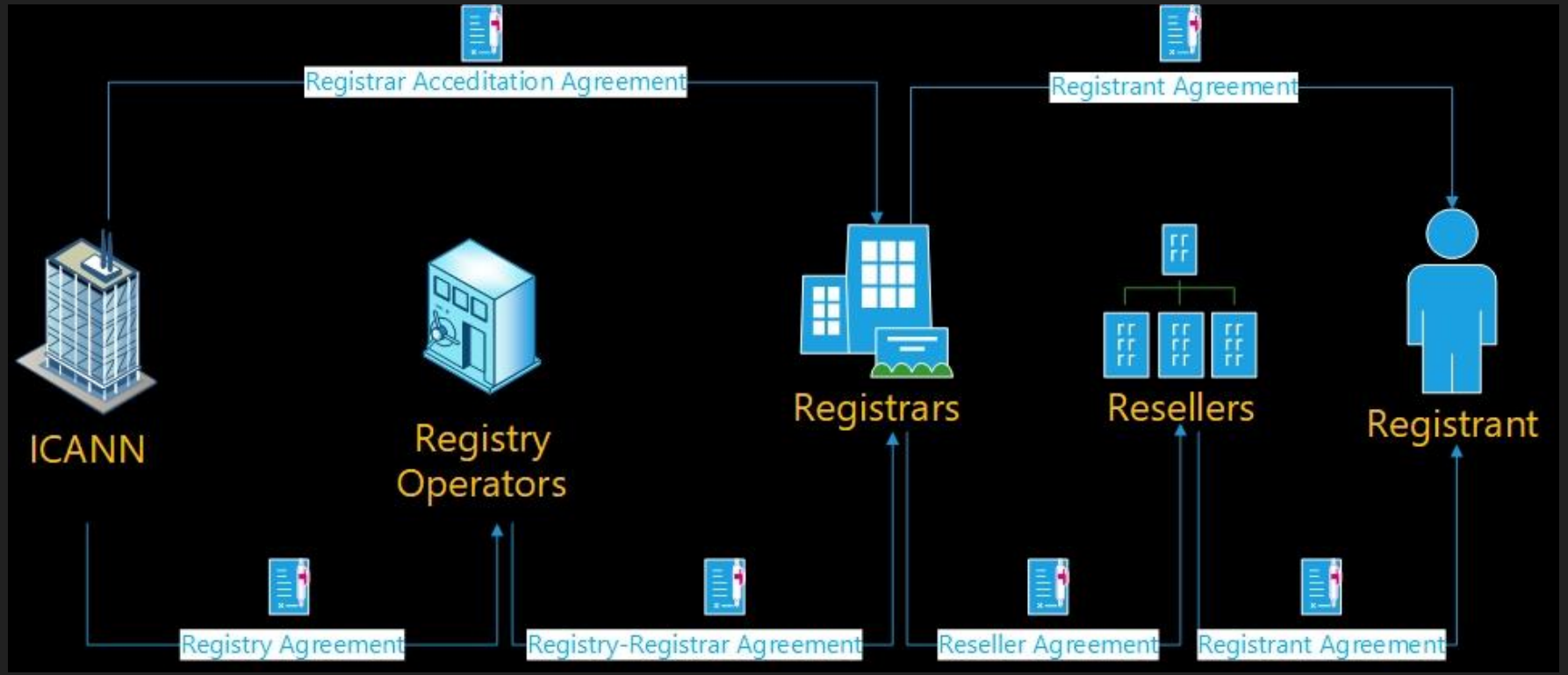
How DNS works



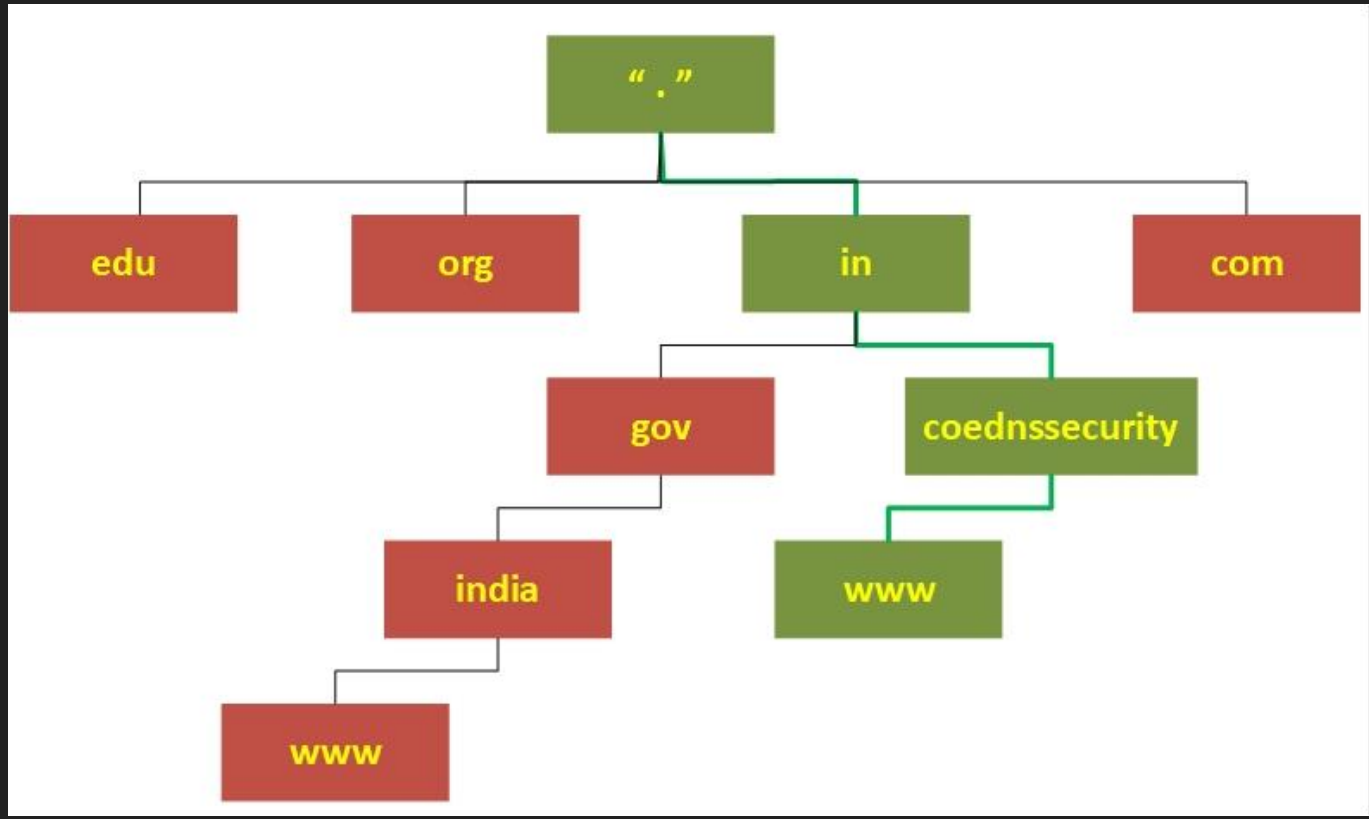
DNS Ecosystem



Contractual relationships in DNS Ecosystem



Domain Name hierarchy



The root

Top-Level Domains

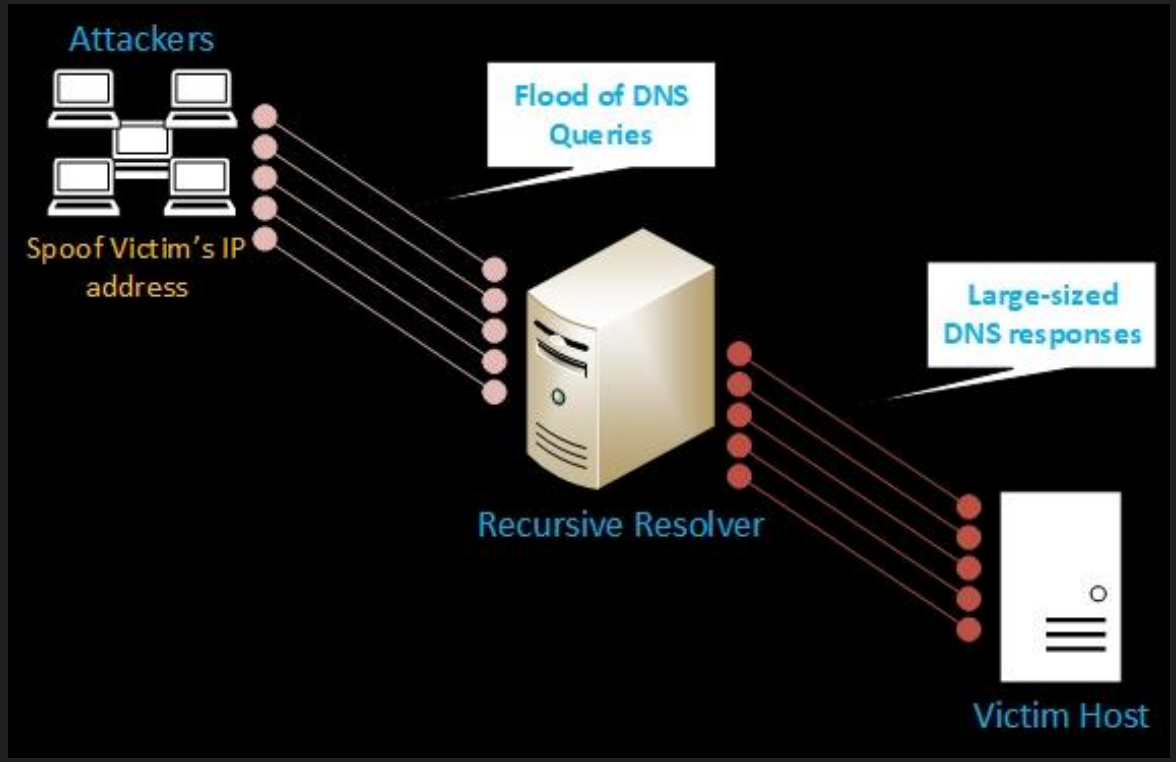
Second-Level Domains

Third-Level Domains

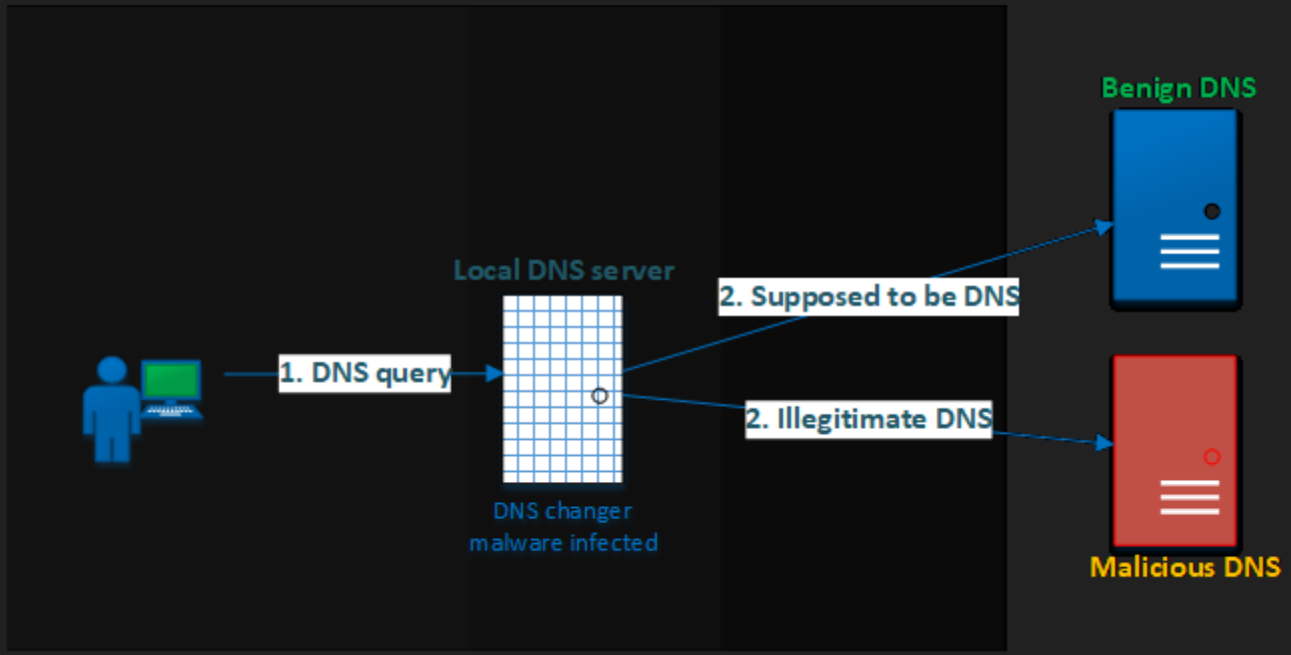
Common DNS record types

- A record: IPv4 address. A domain or sub-domain has single IP while one IP can have multiple domains pointing to it.
- AAAA record: IPv6 addresses.
- PTR record: finds a domain name in a reverse-lookup when the IP is already known.
- CNAME record: canonical name, forward a domain or sub-domain to another domain without providing an IP address. These can be used as aliases to domains.
- MX record: mail exchange record that directs mail to an email server.
- TXT record: domain administrator store text notes commonly used to gauge the trustworthiness and verify ownership of a domain.
- NS record: authoritative name servers.

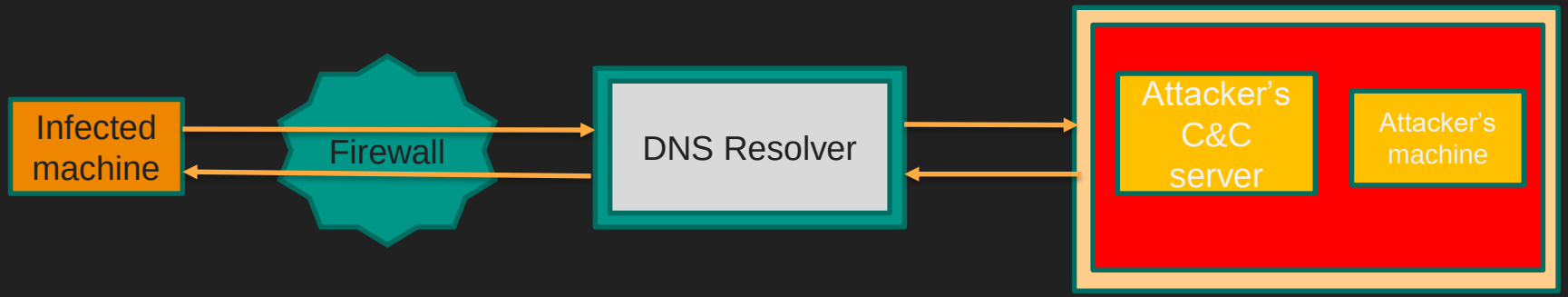
DNS Amplification Attack



DNS Changer


Benign DNS
Local DNS server
2. Supposed to be DNS
1. DNS query
2. Illegitimate DNS
DNS changer
malware infected
Malicious DNS

DNS Tunneling



- Tools: dns2tcp, Iodine, OzymanDNS, NSTX, psUDP, DnsCat, TUNS, DNScapy, squeeza, DeNISe, Heyoka
- Mitigation: DNS payload inspection, DNS Traffic Analysis, Host monitoring for tunneling software

Part 3:

MALICIOUS DOMAIN DETECTION

Outline

- Common uses of maliciously registered domains
- Approaches to detect malicious domains
- Datasets for research
- Demonstration

Common uses of maliciously registered domains

1.

- Manipulate to webpage similar to a reputed website

2.

- Data Exflitration

3.

- Download malware

4.

- Redirect to other malware hosts

5.

- Remote control your network resources

6.

- Crash infrastructures

Approaches to detect malicious domains

Blacklist

- Reputation based on history

Lexical Features

- Length
- Characters ratio, continuity rate
- Phrases

Global ranking

- Alexa
- Domcop
- Majestic

Registration data

- RDAP
- IPWhois
- DomainWhois

Web Traffic

- Visitors count
- Stay time
- Web referrals

Category & Content

- Type of website
- Number of pages
- Broken links

Datasets for research

- Spamhaus DBL
- SURBL
- IANA
- ICANN

Thank You

gopinath@cdac.in