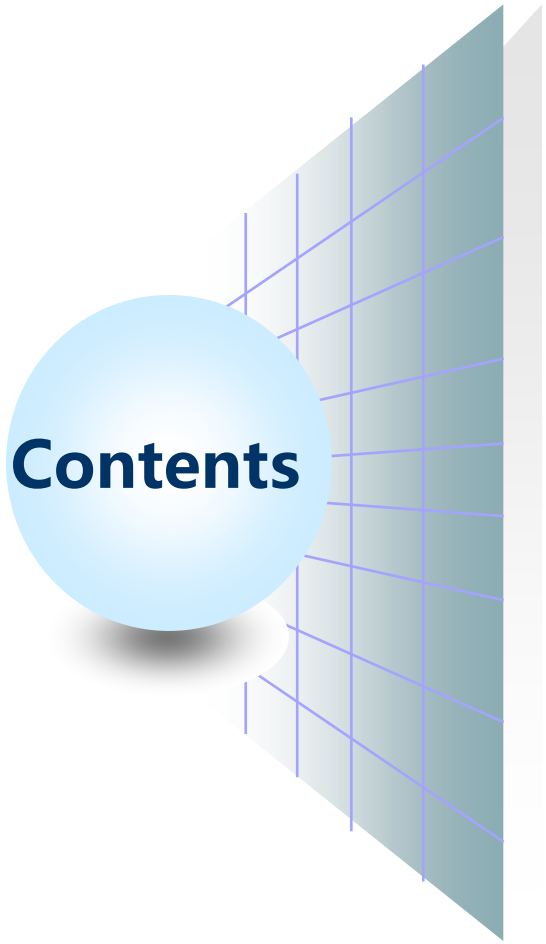
国家网络空间安全基础能力的搭建者
Pioneer of National Cyberspace Security

EVERSEC 恒安嘉新

Attack hunting with Threat Intelligence of DNS

Eversec Technology Co., Ltd.

Contents



Attack(Threat) Hunting

Concept

- ✓ **Attack hunting (Threat)** means to pro-actively search for malware or attackers that are lurking in your network — and **may have been there for some time**. They could be quietly siphoning off data, patiently listening in for confidential information, or working their way through the network looking for credentials powerful enough to steal key information.

Key Point:

- ✓ Basic security hygiene and properly implemented AV, firewalls, NDR and other automated security tools should stop the majority of threats from getting in. But once an attacker has sneaked into your network undetected, there's often not much to stop them from staying there.

3 Categories

1、**Hunt for Attacks within your Organization**

2、Hunt for Threat Pro-actively on the internet

3、Hunt for Attack with a Trap

DNS Resolving Precedure

DNS stands for “Domain Name System” and it is a mechanism to make the Internet a more human-friendly place.

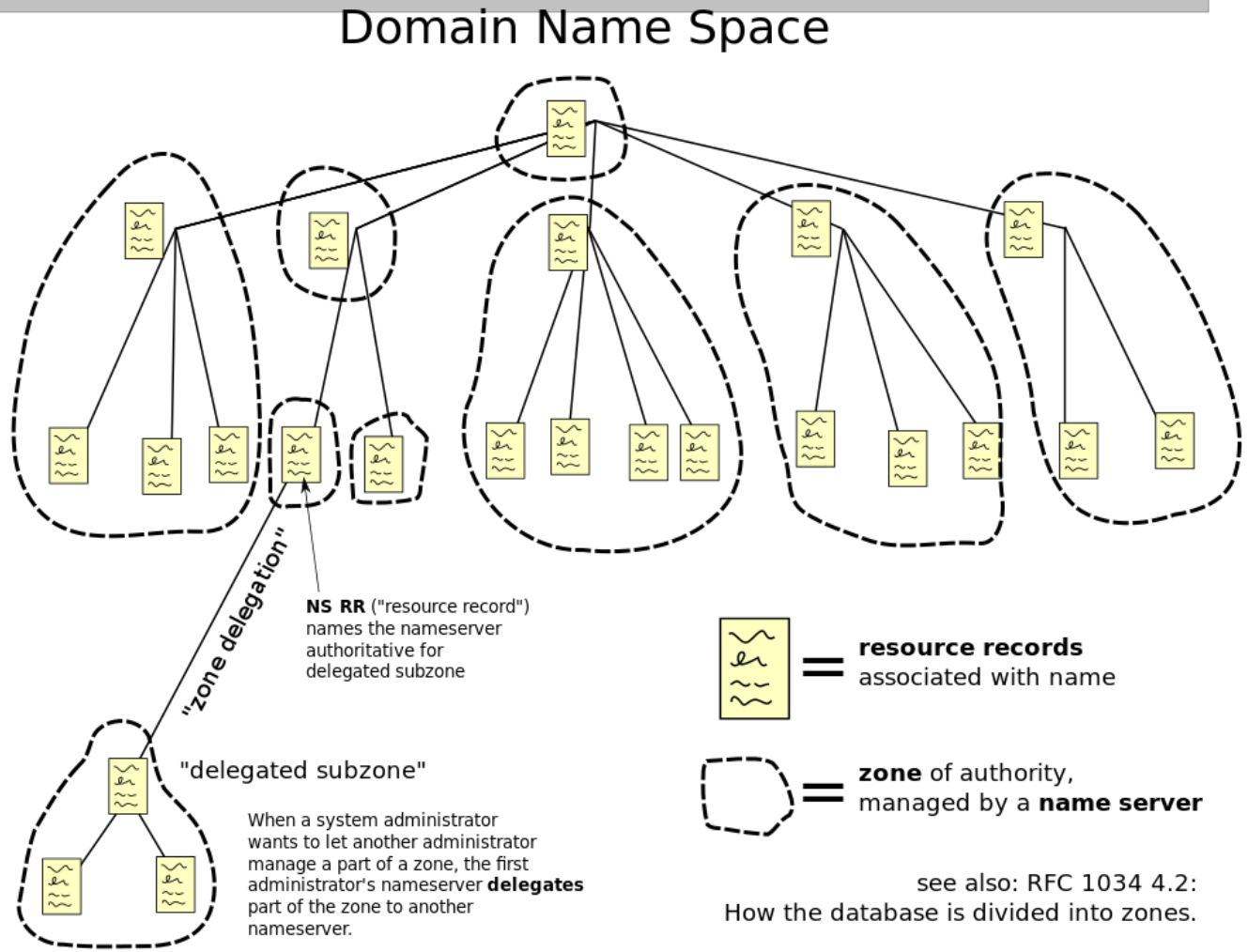
When type **www.google.com** on your browser;

1. If the DNS records are located in your **computer’s DNS cache**, you’ll be taken straight to **www.google.com** to avoid the remainder of your DNS quest.

2.If no data is detected, a query will be forwarded to your local DNS server.

3. If the data on the resolving nameserver are **not cached** then the request to find the DNS records is forwarded to a root nameserver.

4.When the DNS records are found, a link is opened to the server where the site is stored and **www.google.com** is seen on the computer.



Encrypted DNS: Mixed Blessing

- A big Trend of DNS encryption is impacting a vital analytics source : DNS query
- DNS over HTTPS(DoH) and DNS over TLS(DoT) are impacting the ability to monitor DNS queries.
- DoH uses HTTPS port 443 which is normal in internet perspective, while DoT uses 853 which may be blocked by FW.

DNS over TCP/UDP port 53(Do. 53) v.s. Encrypted DNS

For Convenience

- ✓ Easy for companies to monitoring
- ✓ Easy monetized for ISPs.

- ✓ Ultimately, encrypted DNS will be resolved with Do. 53 at somewhere upstream.
- ✓ Privacy protection
- ✓ Data Security

For Security

- ✓ Easy for DNS Channel Inspection
- ✓ Easy for DNS logs extraction

- ✓ Analyzing the content on the wire requires TLS **interception**
- ✓ Prevent from behavior reconnaissance
- ✓ Mitigate DNS spoofing

DNS Cyber Threat Intelligence(CTI)

- DNS CTI could be defined as 'all the Threat information that comes from the DNS system and the interactions of its users'.
- DNS serves as early warning and detection solution for **phishing, spam, malicious and suspicious behaviors**, and other attacks. DNS intelligence is considered the only source of "*ground truth*" information for the Internet.

who.is

FARSIGHT SECURITY

Infoblox

Kaspersky Threat Intelligence Portal

SOCRadar® Extension to Your SOC Team!

- **Darknet**
  Messages sent to non-public and hidden network addresses.
- **Spam-Select**
  Select fields from emails sent to global honeypot spamtraps
- **Phishing URL's**
  PhishLabs data for malicious sites involved in phishing campaigns
- **Processed DNS Data**
  Raw DNS data that has been de-duplicated, filtered and verified
- **Newly Active Domains**
  Domains that were active and went dormant for at least 10 days before the next observation
- **Newly Observed Domains**
  Base Domains considered 'New' when compared to historical database
- **DNS Changes**
  Domains and IP addresses that have changed compared to historical database

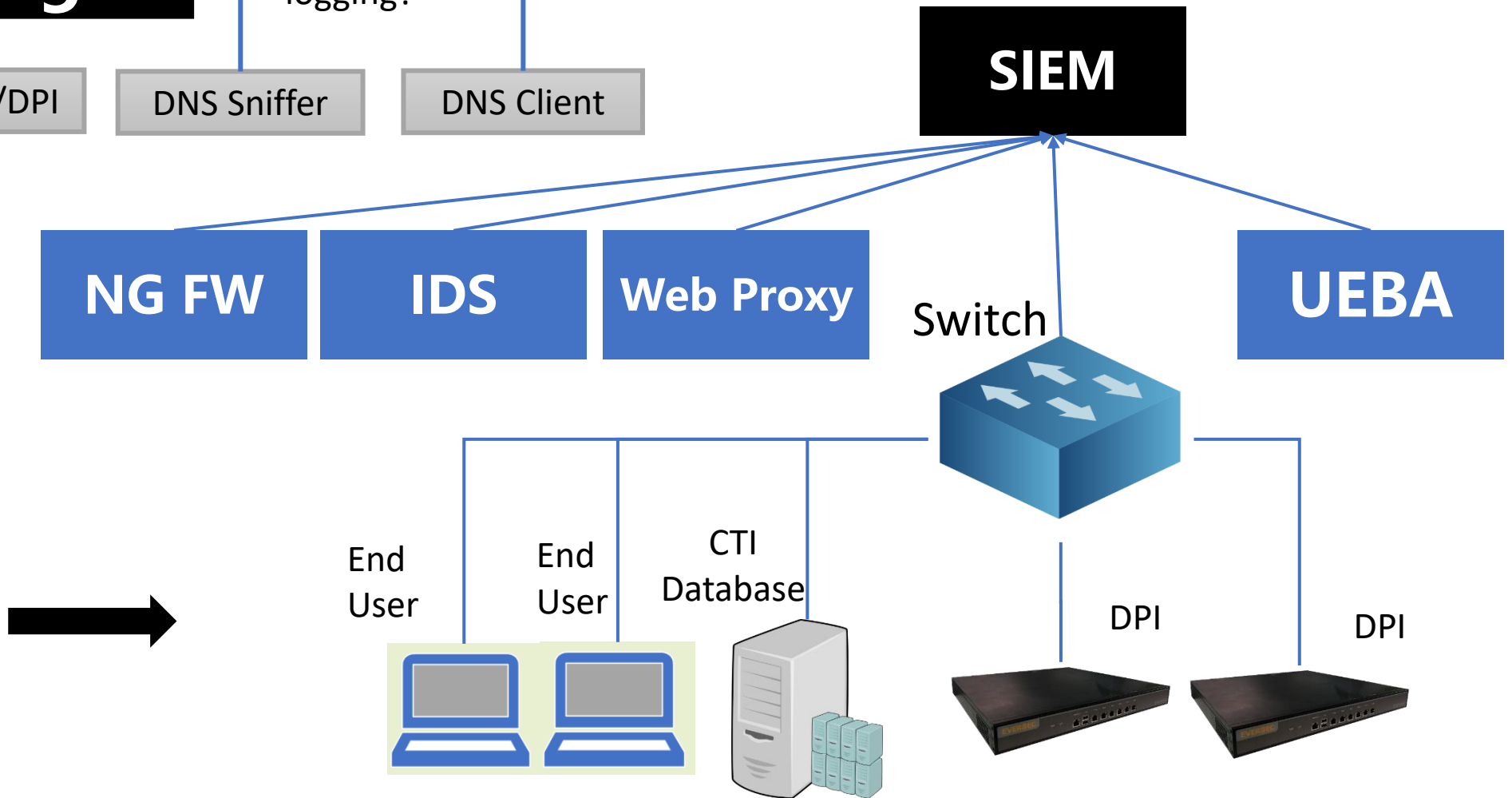
DNS CTI examples

- **Associated IPs:** In a similar manner, you can detect related IPs on the same network by looking into DNS information
- **Forward DNS records:** All present DNS records on the current website
- **DNS historical records:** Historical DNS records from days, months or years ago
- **Subdomain mapping:** By accessing all current DNS records, you can also perform subdomain enumeration for current and past subdomains over a period of time
- **Reverse DNS records:** Current rDNS records obtained by performing a reverse DNS lookup
- **Registrar name servers:** Current NS records at the domain registrar
- **Glue record history:** DNS records created at the domain registrar
- **Historical registrar name servers:** Past information about NS used on the registrar, going back by years
- **DNS software identification:** Software information for the DNS server you're running, including name and current version
- **Associated domain names:** DNS intelligence also provides the ability to detect associated domains hosted on the same networks as the main apex domain

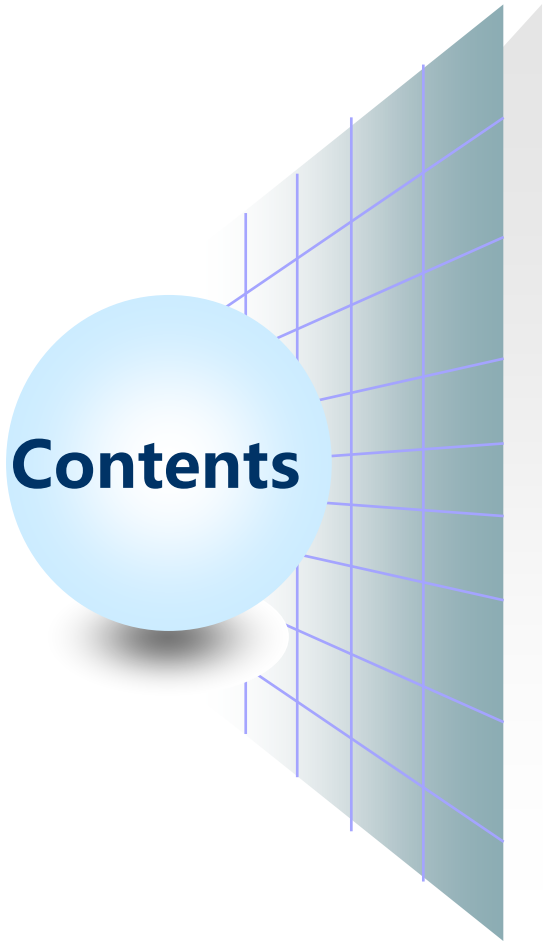
DNS as Data source of Attack Hunting

DNS query logging is effective to detect hostname lookups for knowing malicious domain.

- DNS cache is a good short-term investigative tool for Attack Hunting.
- DNS logs are one of the most actionable SOC/SIEM data source

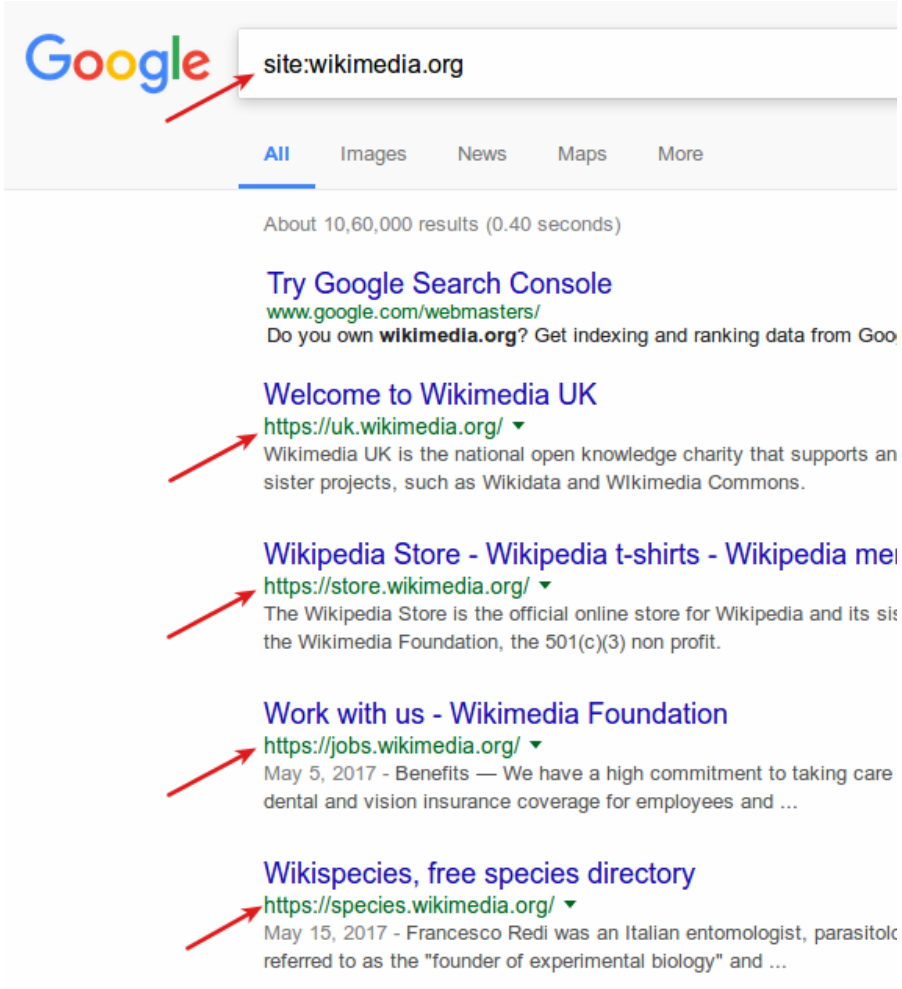


Contents



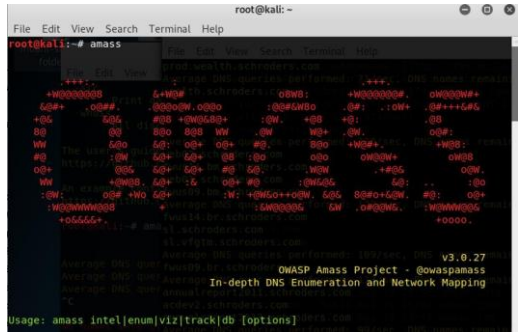
Subdomain Enumeration

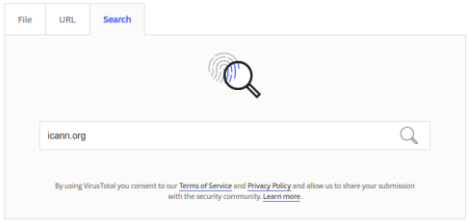
Subdomain enumeration is the process of finding sub-domains for one or more domain(s). It is an essential part of the reconnaissance phase. There are two types called active subdomain enumeration and Passive subdomain enumeration.

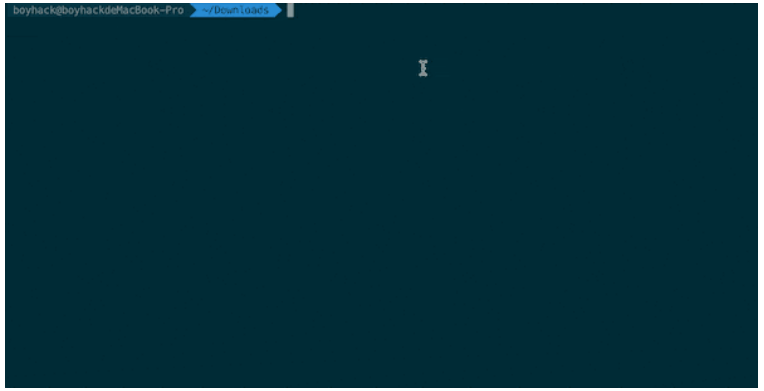


Subdomain enumeration is the beginning of most DNS attacks. It mainly uses violent enumeration of sub-domain information for DNS query.

- The attacker sends a large number of domain name requests to the DNS server within a unit time. One of the characteristics of such domain name requests It is because the subdomain name is different but the main domain name is the same.
- The attacker traverses the subdomain name to blast the subdomain name, which can facilitate in-depth attacks in the later stage.







https://github.com/boy-hack/ksubdomain

VirusTotal runs its own passive DNS replication service, built by storing DNS resolutions performed when visiting URLs submitted by users. In order to retrieve the information of a domain you just have to put domain name in the search bar.

Botnet with DGA Domain name

DGA is a specific algorithm used in malware to generate domain names in batches.

- Attackers can obtain same DGA domain name which may lead to coalition.
- Large amount of Generated domain names
- Seeds varies from a wide range.
- Complex generation methods

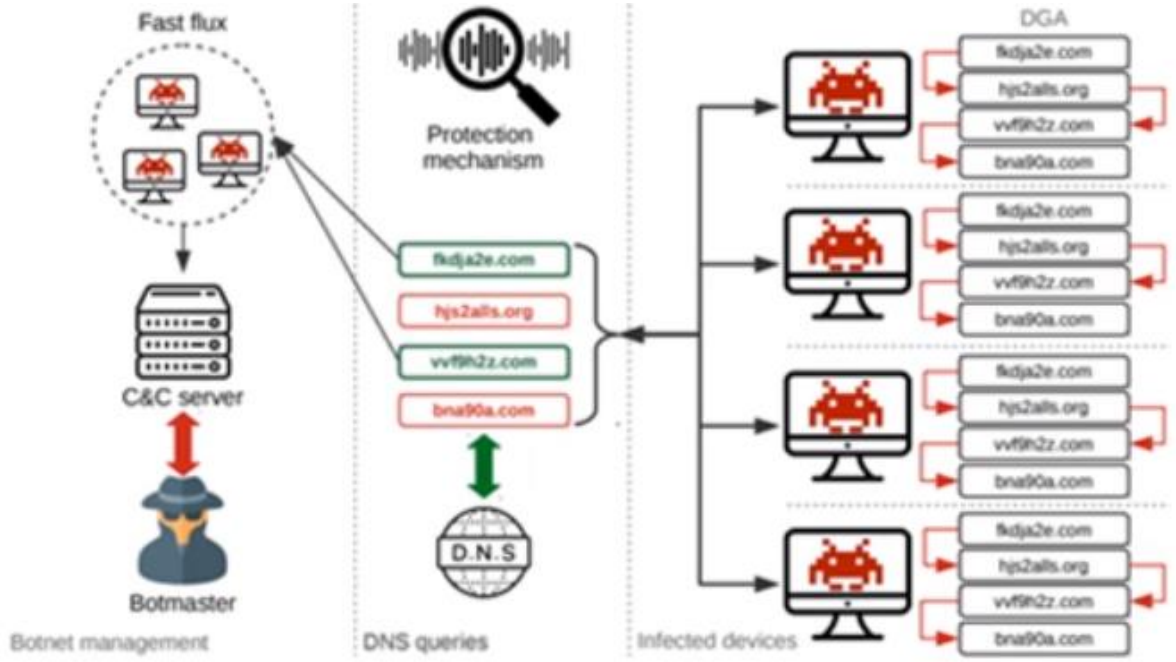
DGA seed: Seed refers to an input of the attacker in DGA, in order to control the process and result of DGA.

The **domain name** or IP of the C&C server in a botnet is static. If it is blocked by security personnel, the problem of node failure will easily occur, which will lead to the paralysis of the entire botnet, which is called "central node failure".

Domain Flux Protocol is proposed , of which algorithm is DGA, while C&C domain name is generated by certain algorithm. Mid-nodes between attackers and compromised hosts are changing, which could evade C&C detections .

DGA Methods

- Arithmetic Based: A series of ASCII numbers are generated to represent domain names, its main stream methods.
- Hash Based: DGA based on hexadecimal expression of digest number. MD5 and SHA256 are common used.
- Dictionary Based: Expression is randomly chosen from dictionary in order to deceive attack hunters. Dictionary is usually embedded in program or
- Permutation based: Permutation of characters of initial domain name string.



✓ DGA identification based on DNS

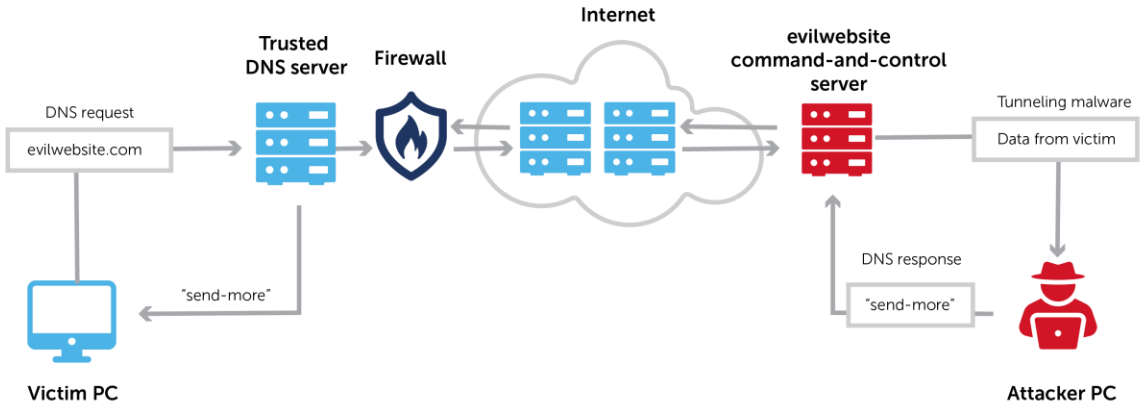
DNS Tunneling

DNS tunnel is ideal for C&C

- DNS tunneling transmits information through the **DNS protocol**.
- Normal DNS requests only contain the information necessary to communicate between a client and a server.
- DNS tunneling inserts an **additional string of data** into pathway. It establishes a form of communication that bypasses most filters, firewalls, and packet capture software.
- DNS tunneling can establish C&C. It can exfiltrate data. Information is often broken up into smaller pieces, moved throughout DNS, and reassembled on the other end.

Hard to detect and to trace its origin

DNS tunneling



DNS Hidden Tunnel

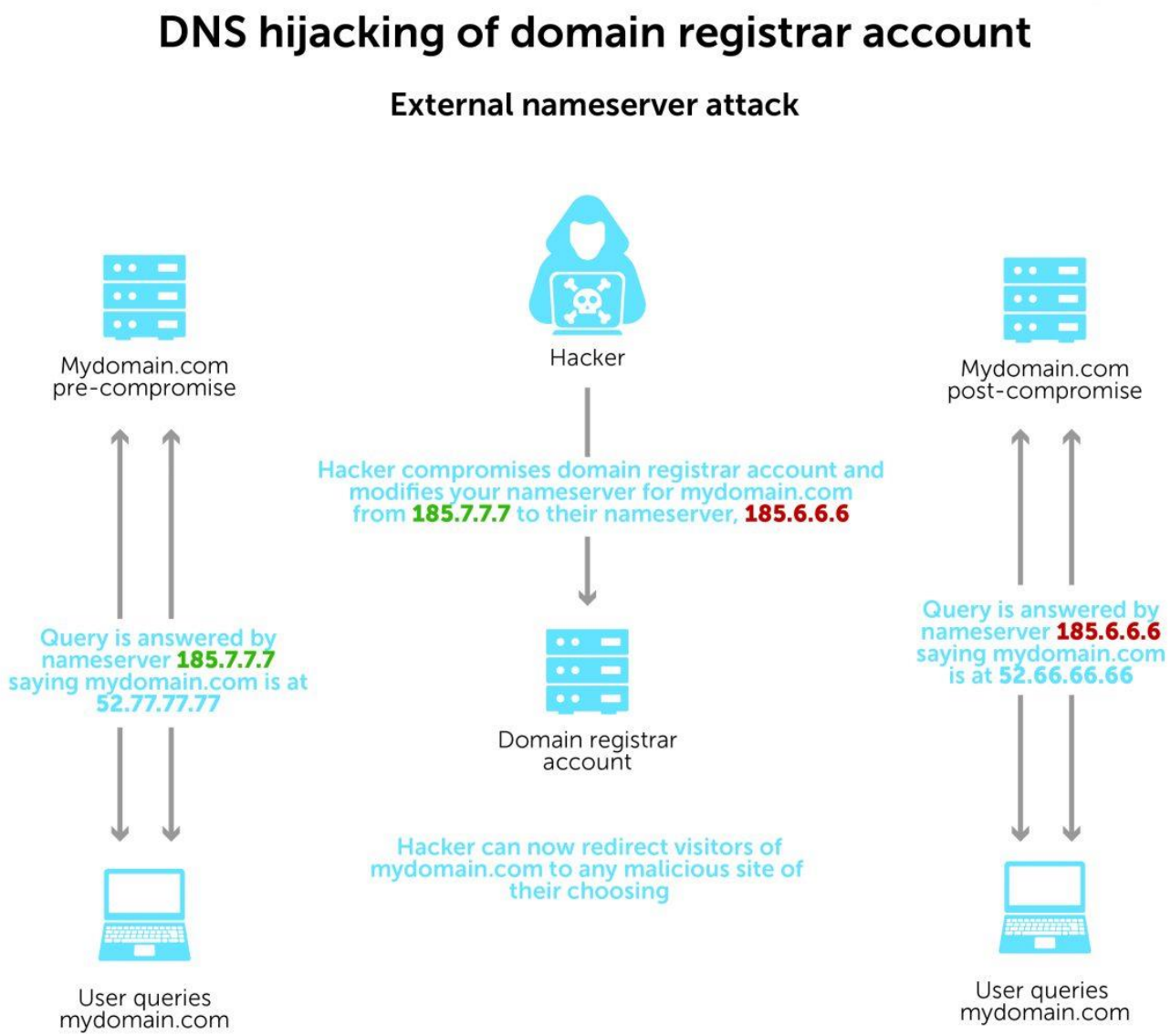
Domain Name based Covert Channel: An attacker compromises or registers a domain name and sets its Domain Name Server (NS) as a hidden tunnel server. The hidden channel client can communicate with the server by requesting the subdomain under the domain from any recursive DNS server.

Server based Covert Channel: An attacker runs a UDP-based service (such as OpenVPN) on port 53 and establishes a connection directly from the client, or uses UDP tunneling software to inject data into the spare space at the end of an existing DNS message, making the UDP partial payload a covert channel data.

DNS Hijacking

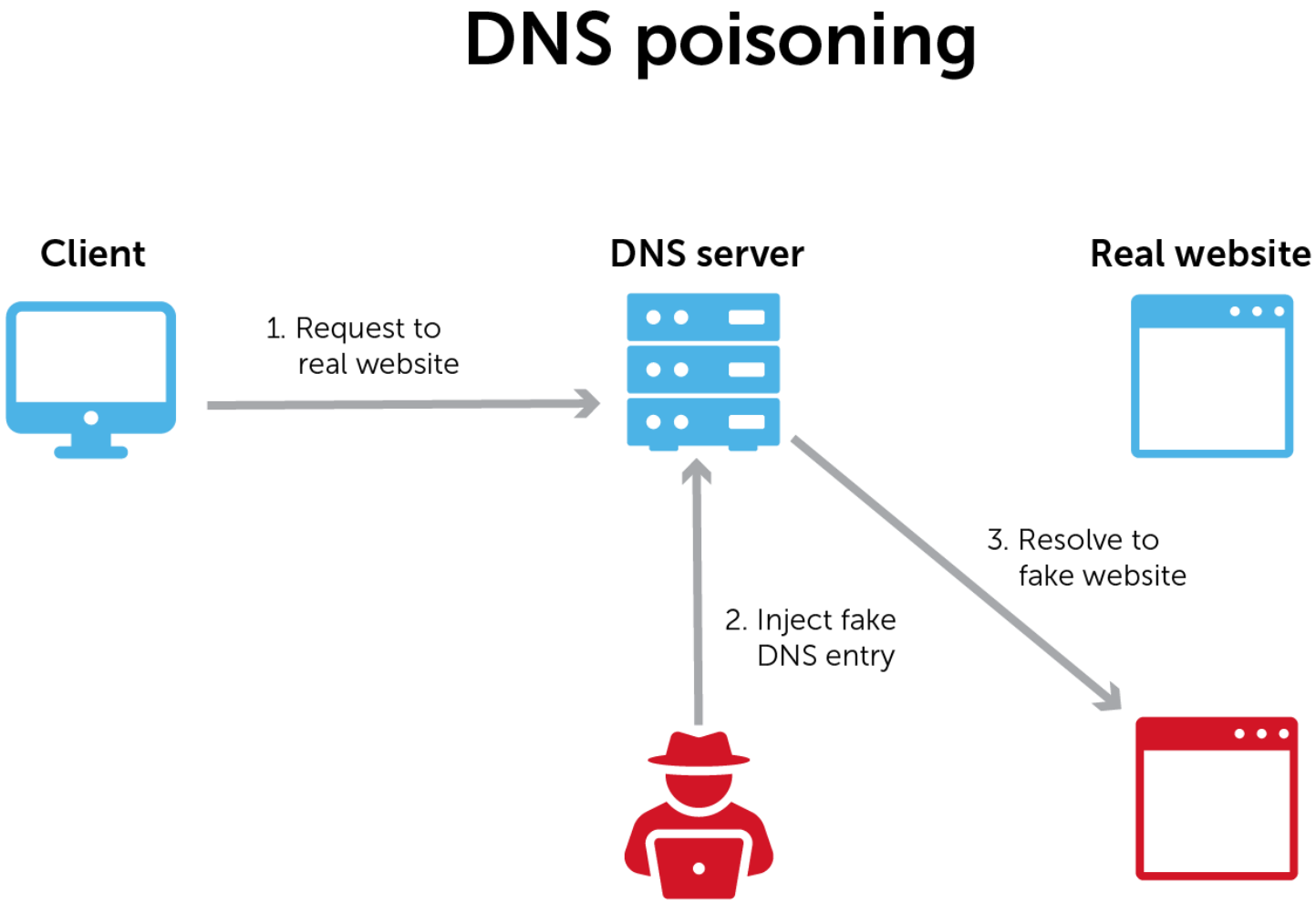
- Domain Name Server (DNS) hijacking, also named DNS redirection, is a type of DNS attack in which DNS queries are incorrectly resolved in order to unexpectedly redirect users to malicious sites.
- To perform the attack, perpetrators either install malware on computers, take over routers, or intercept or hack DNS communication.

1.Attackers can compromise a domain registrar account and modify your DNS nameserver to one that they control.
2.Hacker can change the record for your domain's IP address to point to their address instead.
3.Hackers can compromise an organization's router and change the DNS server that automatically gets pushed down to each device when users sign on to your network.



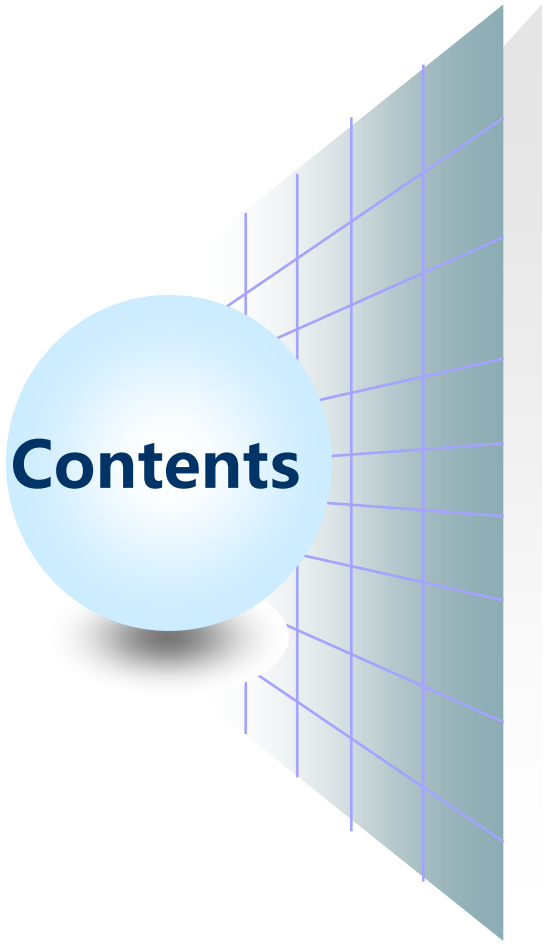
DNS Poisoning/Spoofing

- DNS poisoning and its cousin, DNS cache poisoning, use security gaps in the **DNS protocol to redirect internet traffic to malicious websites.**
- These are sometimes called man-in-the-middle attacks.
- DNS poisoning happens **when a hacker intervenes in that process and supplies the wrong answer.** Once it has tricked the browser into thinking that it received the right answer to its query, the hacker can divert traffic to whatever fake website it wants.

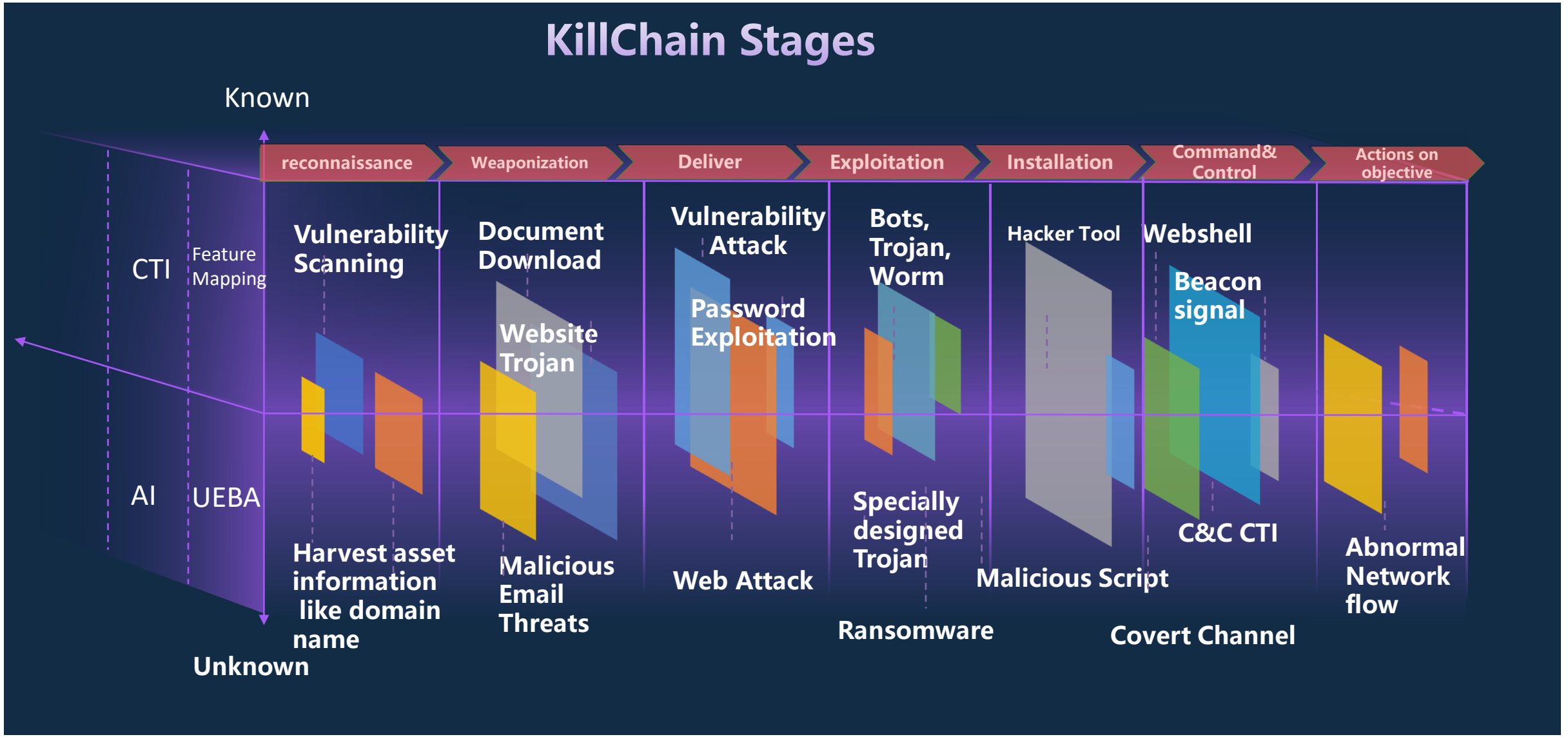


DNS Spoofing is a DNS attack that changes DNS records returned to a querier;

Contents

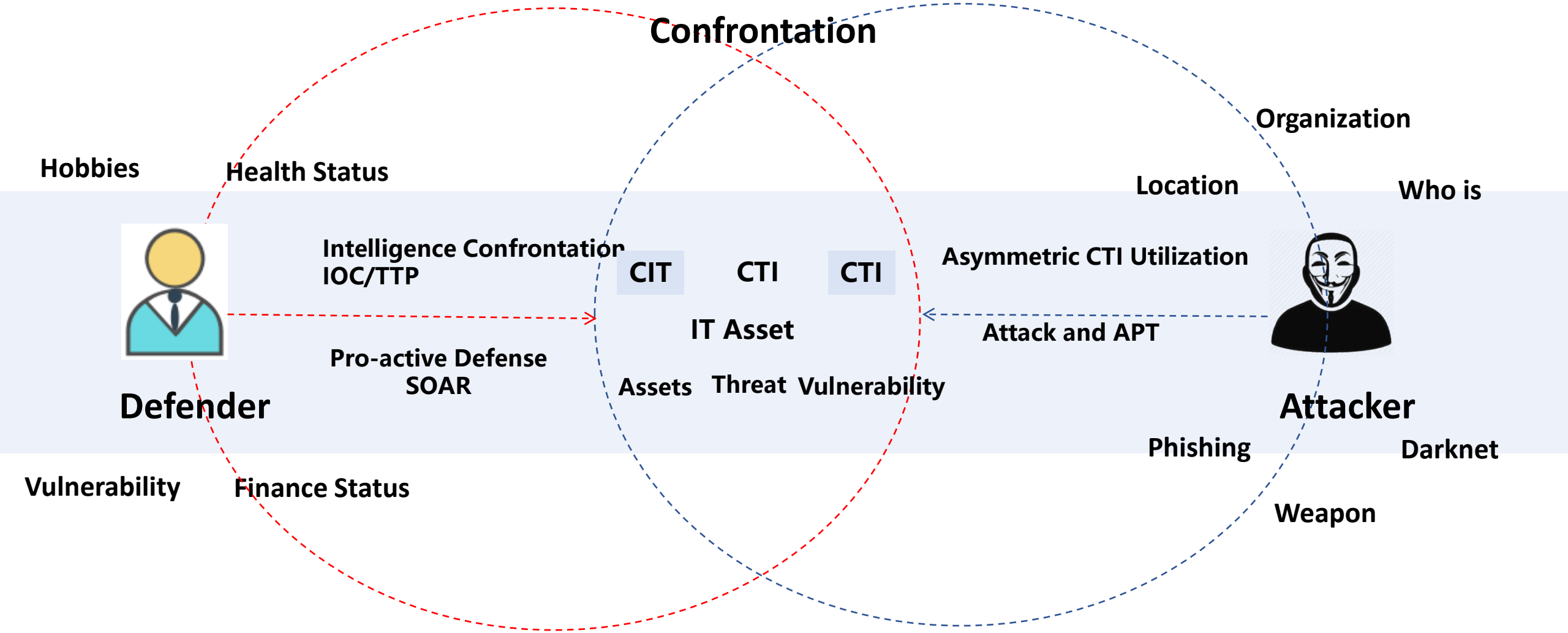


Attack Detection with DNS at any Stage



Entity Profiling with DNS Intelligence in Confrontation

Entity profiling is leveraged by both Attacker and Defender as an effective weapon.

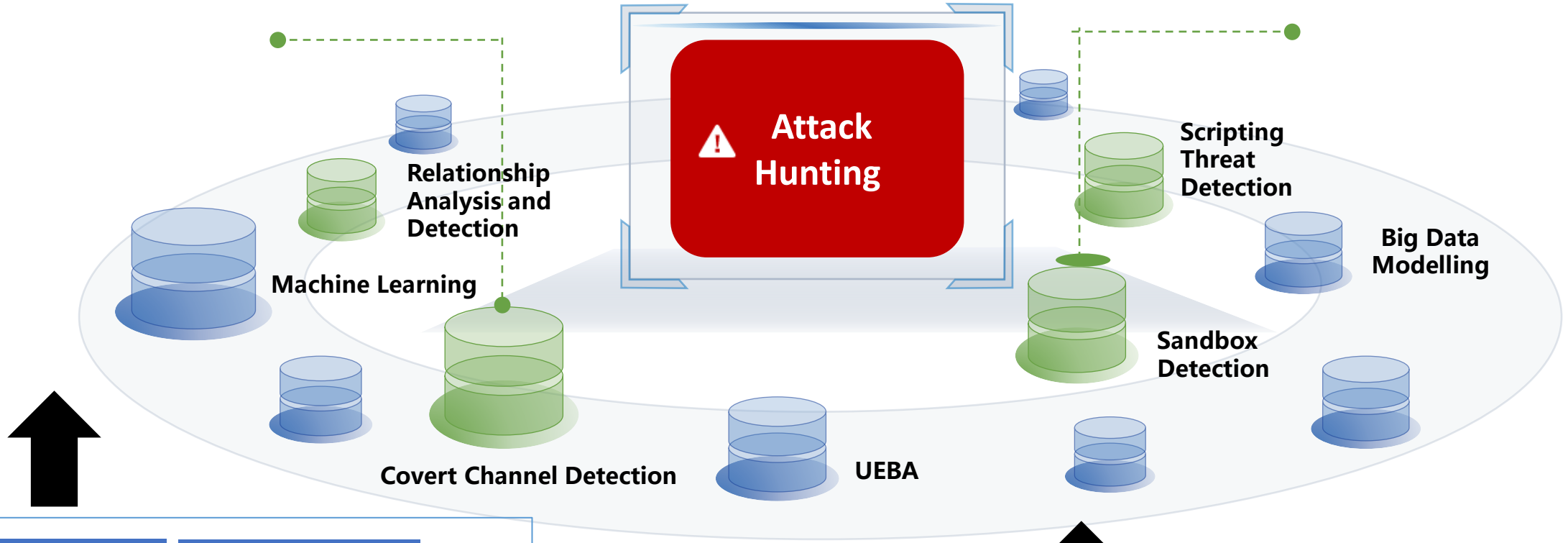


CTI Management Center

- **DNS CTI:** Darknet, Spam-Select, Raw DNS, Newly Active Domains, Malicious Domain names etc.
- **CNVD general-purpose vulnerabilities:** mainly the vulnerabilities corresponding to third-party software, applications, and systems. According to the general-purpose vulnerability data.
- **CNVD event-type vulnerabilities:** Different from general-purpose vulnerabilities, they are mainly vulnerabilities in Internet applications.
- **Virus Database:** The information on virus comes from.
- **Common IoC:** AV signature

CTI Distillation from DNS Logs

Cyber threat detection based on SIEM with DPI and DNS as data input



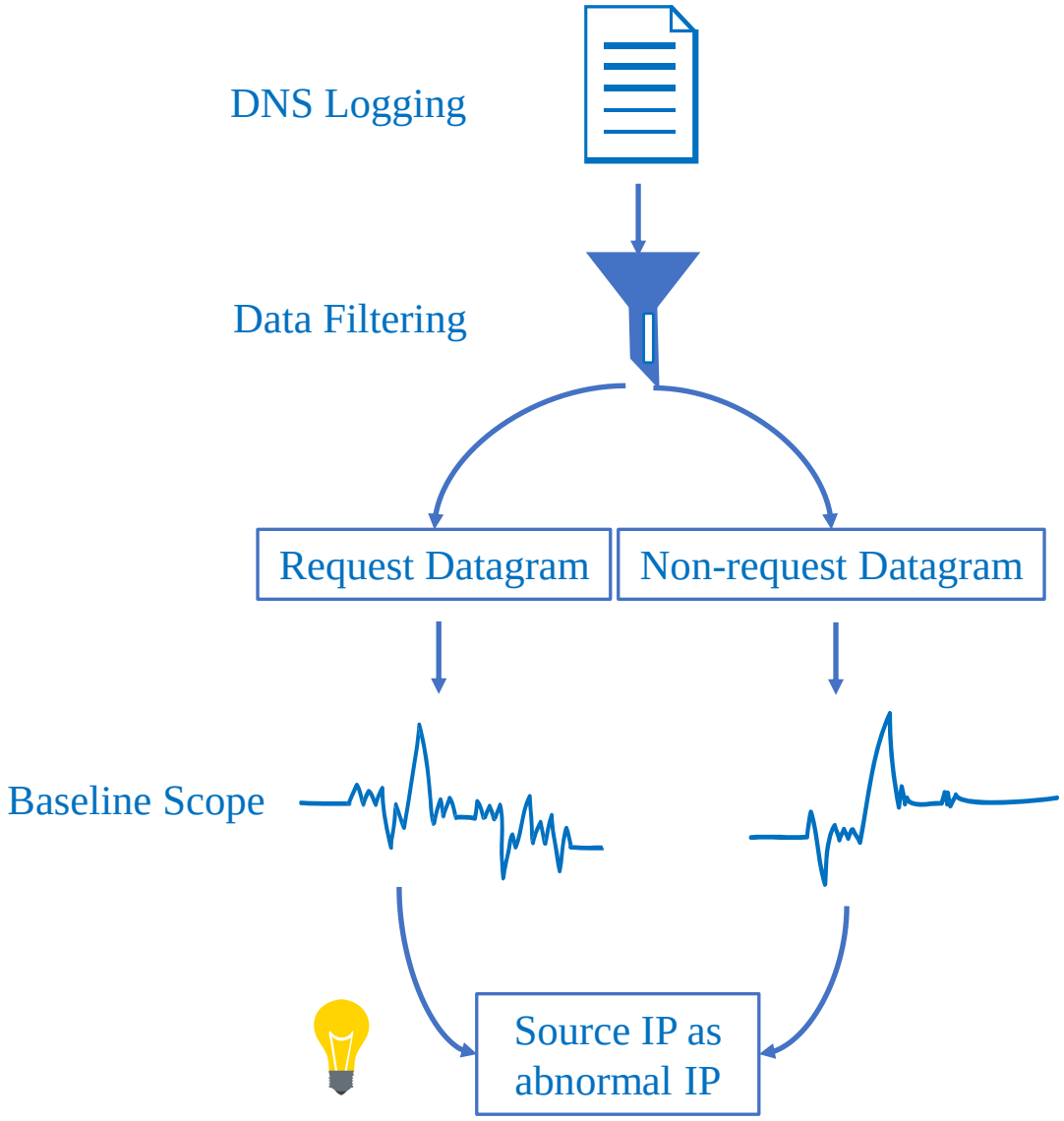
Darknet | Phishing URL
Spam-Select | Processed DNS Data
Newly Active Domains | DNS Changes

CTI

NG FW | IDS | NDR | Web Proxy

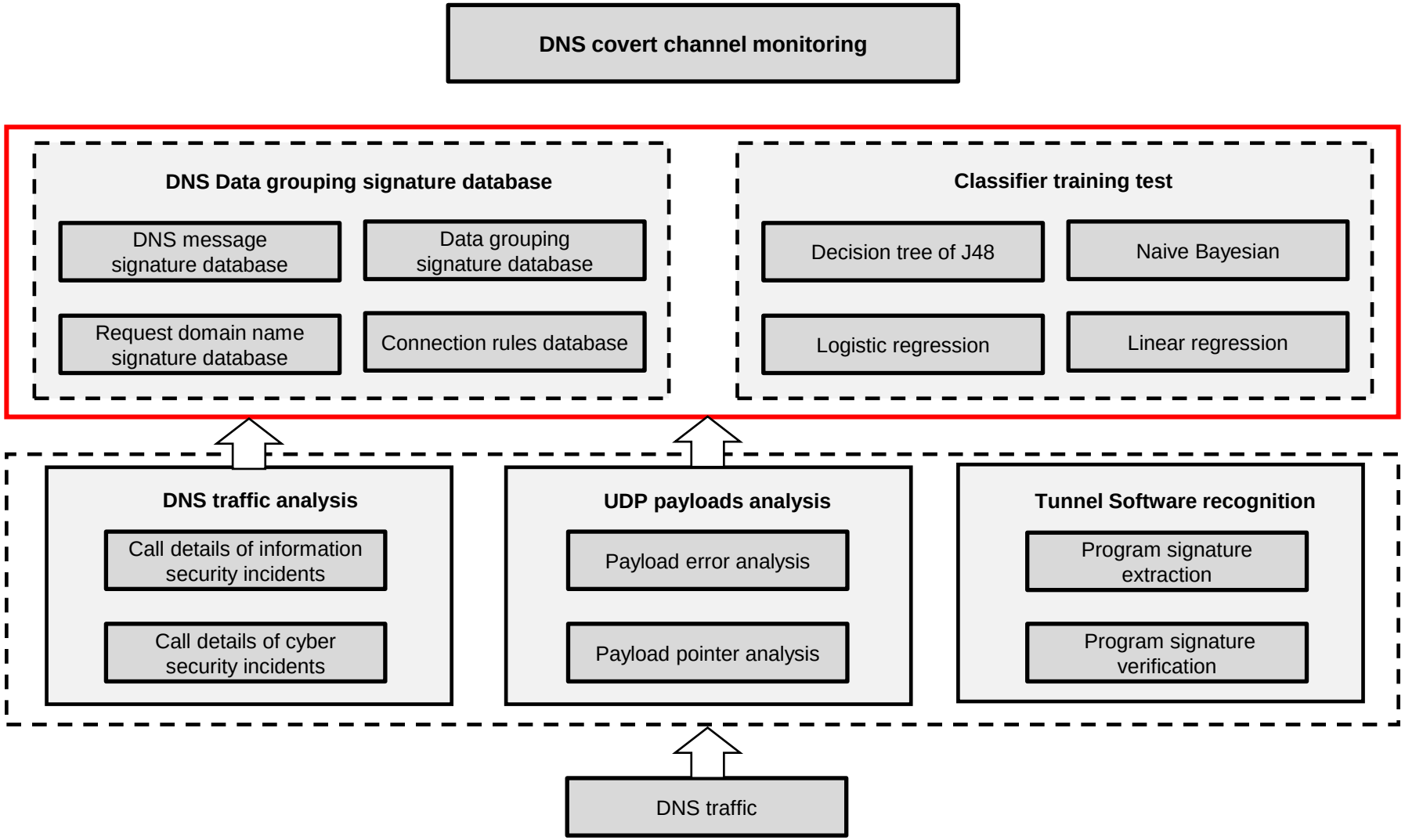
DNS Subdomain Enumeration Detection

- DNS Subdomain Enumeration detection model is proposed based on DNS CDR logs for DNS subdomain blasting attacks. By detecting the request packets and response packets of the DNS log, it can be judged whether there is a subdomain blasting attack.



DNS Covert Tunnel Detection

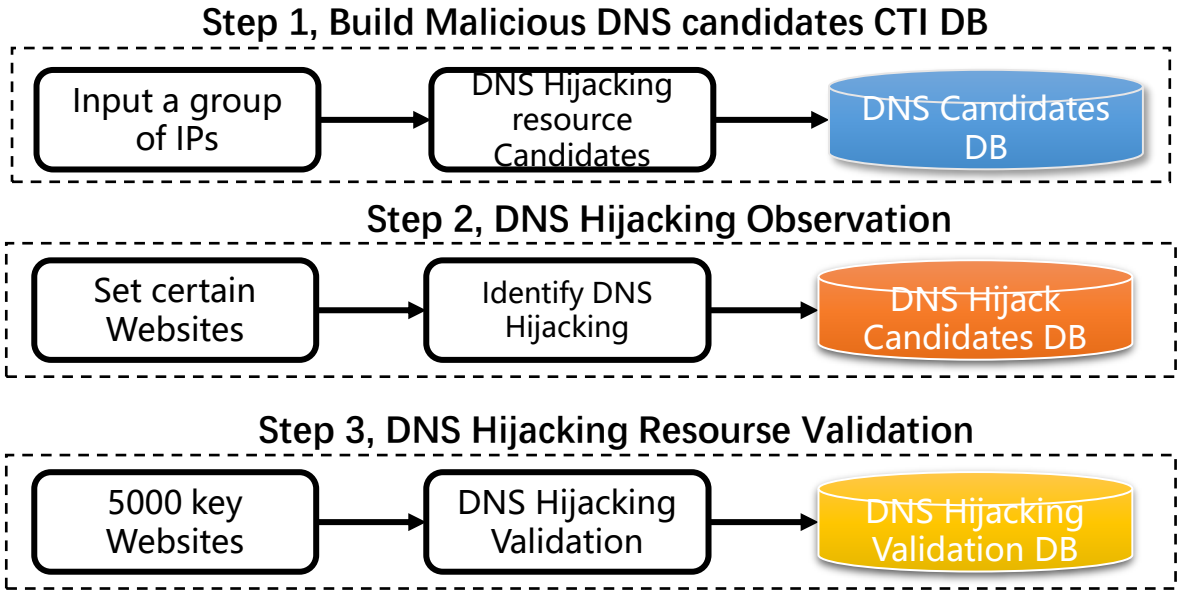
- **Data collection:** From the original DNS traffic, NDR is used to gather XDR, combined with UDP payload content analysis and tunnel program identification.
- **Feature Extraction:** DNS data packet characteristics, message features, domain name request behavior, and connection statics.
- **Machine learning:** A classifier with the monitoring capability of DNS covert channel.



DNS Hijacking Hunting with CTI

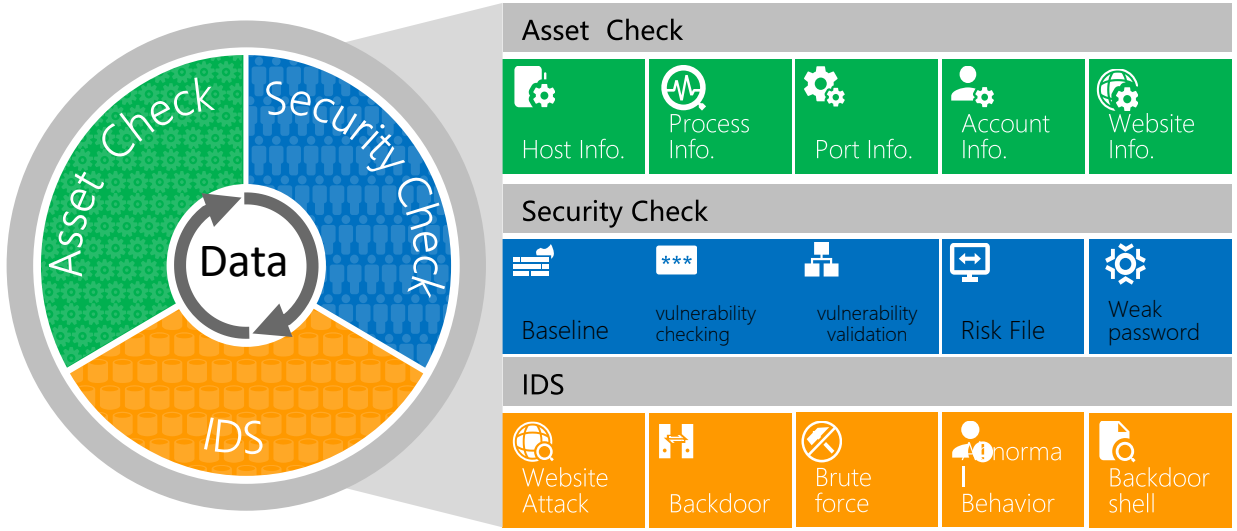
Solution—Hijacking Resource Intelligence Extraction and its Application

- Build DNS CTI DB– 3 steps to build a ultimate DNS Hijacking CTI DB. We should confirm the accuracy of Hijacked DNS labeling.



- Leverage machine learning – It takes automation to beat automated attacks. We need to take measures to analyze, detect and even predict DNS Hijacking related behavior before they happen.

Host Hijacking Prevention Solution



DNS Spoofing Detection with Threat Intelligence

The following example illustrates a DNS cache poisoning attack, in which an attacker (IP 192.168.3.300) intercepts a communication channel between a client (IP 192.168.1.100) and a server computer belonging to the website www.estores.com (IP 192.168.2.200).
In this scenario, a tool is used to dupe the client into thinking that the server IP is 192.168.3.300. At the same time, the server is made to think that the client's IP is also 192.168.3.300.
Such a scenario would proceed as follows:

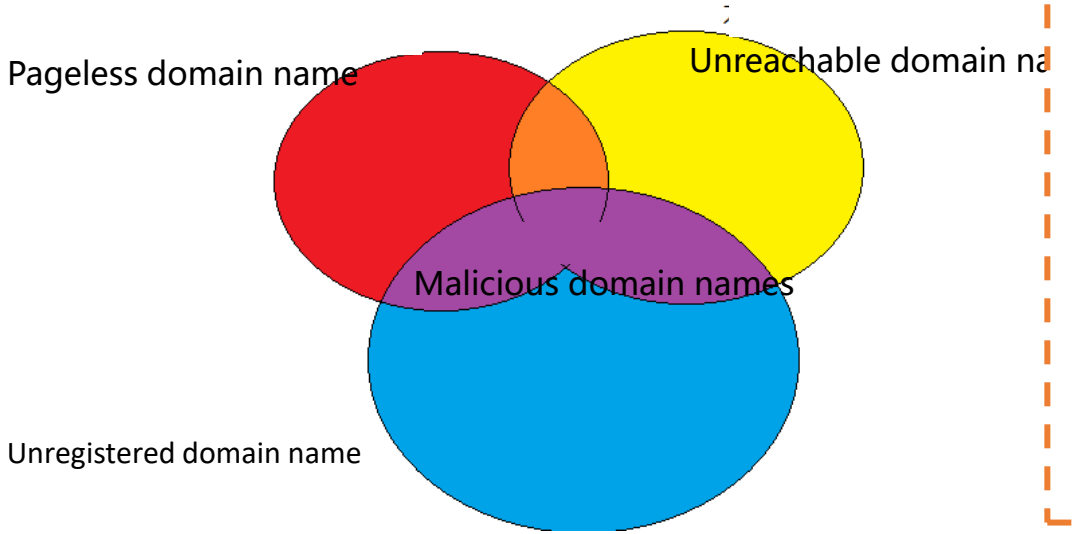
a) The attacker uses arpspoof to issue the command: arpspoof 192.168.1.100 192.168.2.200. This modifies the MAC addresses in the server's ARP table, causing it to think that the attacker's computer belongs to the client.
b) The attacker once again uses arpspoof to issue the command: arpspoof 192.168.2.200 192.168.1.100, which tells the client that the perpetrator's computer is the server.
c) The attacker issues the Linux command: echo 1> /proc/sys/net/ipv4/ip_forward. As a result, IP packets sent between the client and server are forwarded to the perpetrator's computer.
d) The host file, 192.168.3.300 estores.com is created on the attacker's local computer, which maps the website www.estores.com to their local IP.
e) The perpetrator sets up a web server on the local computer's IP and creates a fake website made to resemble www.estores.com.
f) Finally, a tool (e.g., dnsspoof) is used to direct all DNS requests to the perpetrator's local host file. The fake website is displayed to users as a result and, only by interacting with the site, malware is installed on their computers.

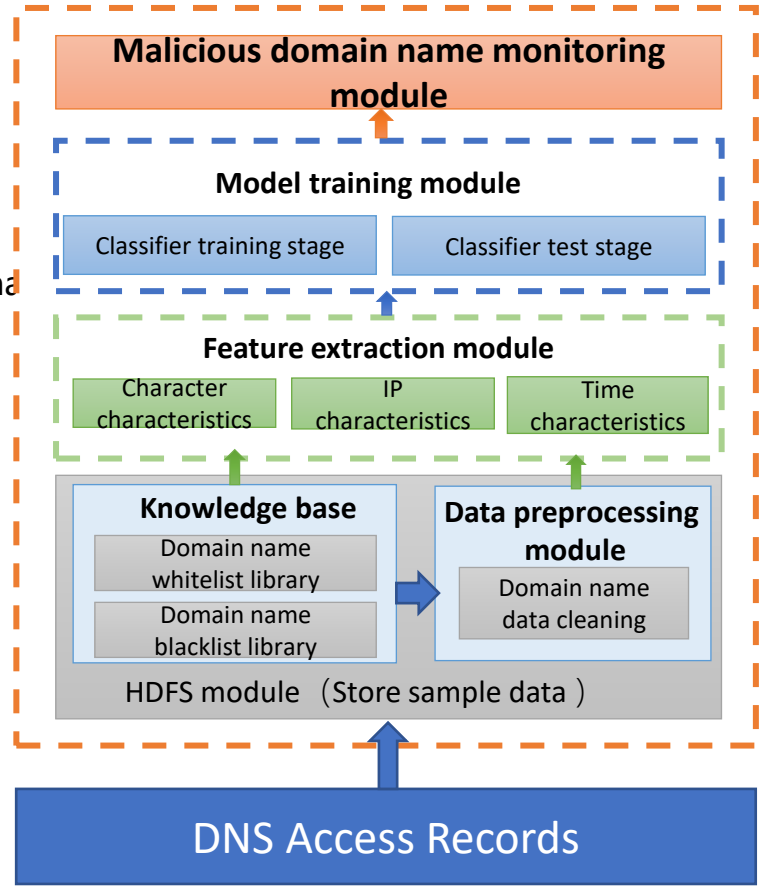
Threat Hunting with DGA detection

Criteria for malicious domain names:

When the domain name meets the following two criteria at the same time, it is judged as a suspected malicious domain name:

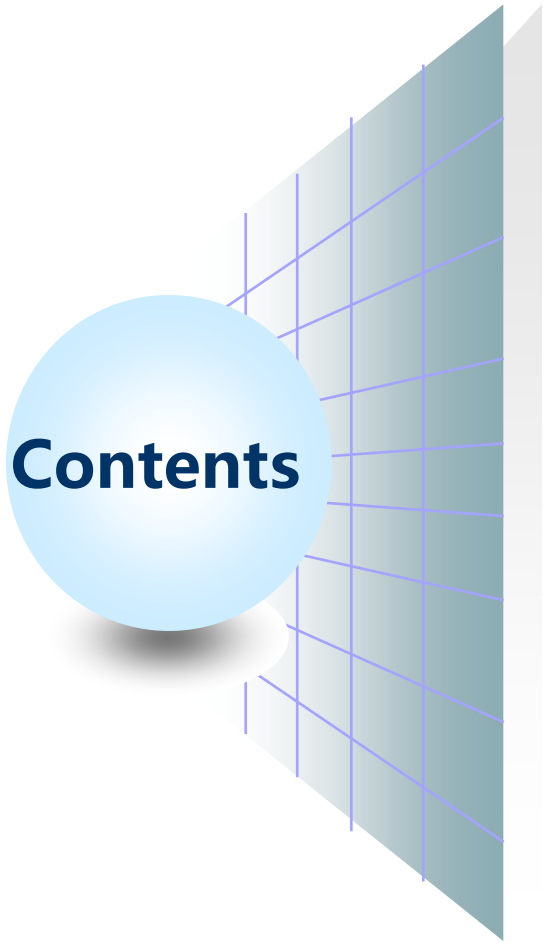
1. The domain name belongs to an unreachable domain name
2. The domain name has not been registered on the website





malicious domain name type	Number of IP	IP conversion frequency	Domain name readability	Access traffic stability
IP Fast-Flux	More	Quite fast	Normal	Relatively low
Domain-Flux	Normal	Quite slow	Relatively low	Relatively low

Contents



EVERSEC TECHNOLOGY CO .,LTD- An Overview

SEC：Science&Technology Engineering. Eversec strives to build a protection system based on Telecommunication and Security.

Solutions and Products

Comprehensive protection of cyberspace security

Cyberspace Security Situation Awareness, Mobile Internet Malware Monitoring and Protection, Internet Monitoring and Protection, Industrial Internet Security Protection

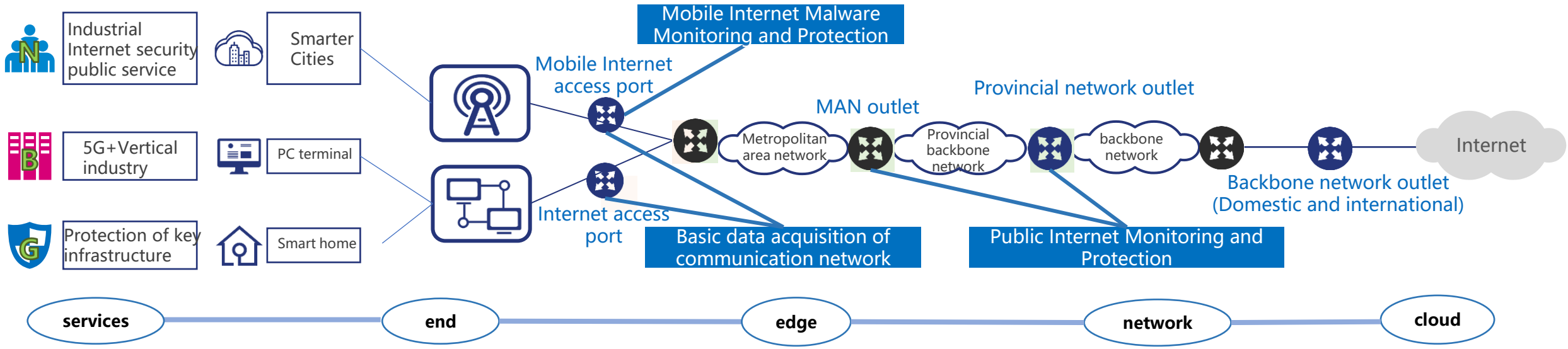
Smart big data analysis of network

Basic data acquisition of communication network, Big data signaling optimization of communication network, Big data value-added service of communication network

Service and Operation

Operation and maintenance services

System SaaS service, Operational Services, Operation and maintenance services, Practical training service



AI+Network security products driven by knowledge

EVERSEC 恒安嘉新

AI + knowledge graph + 「Network security」

Malicious program detection

Malicious APP , PC side malicious sample

Botnet detection

Botnet distribution

Malicious domain name detection

Phishing website , DGA domain name

Intrusion detection

Webshell , Intrusion tampering , Dark chain

Malicious traffic detection

Flow Baseline , Encrypted traffic , DDOS intelligent prediction

Smart intelligence detection

Profile of hackers and hacker organizations

Security log excavate

Association analysis

APT detection

New generation APT traffic comprehensive detection based on IOC+TTP, introducing threat intelligence association mining and prediction technology, and in-depth analysis of session oriented TTP model

Traceability analysis

Intelligence clue expansion ,Traceability of attack chain

Knowledge Application and Insight Analysis Based on Knowledge Graph Technology

EVERSEC 恒安嘉新

Data → (Objective Data) → knowledge Project → (Domain Knowledge) → knowledge graph Database → (Business Scenario) → Business map → (Capacity Output) → industry Application

Data
- Object
- File & Mail
- Log
- sensor

knowledge Project
- Establish Ontology
- Information Extraction
- Knowledge Mapping
- Knowledge Fusion
- Map Construction

knowledge graph Database
- AI Service
- Knowledge Representation
- Knowledge Index
- Knowledge Storage
- Domain Knowledge Map

Business map
- Graph Algorithm + Machine Learning
- APT Organization Business
- Network Security Service

industry Application
- Threat Intelligence
- Network Security
- Situation Awareness
- Industrial Internet
- ……

Knowledge insight: insight into data and the outline of things; Insight into information and logic behind it; Insight into knowledge and draw a network map.

让通信值得信赖

让安全创造价值