Detection of DNS Traffic Anomalies in Large Networks

Milan Čermák, Pavel Čeleda, Jan Vykopal

{cermak|celeda|vykopal}@ics.muni.cz

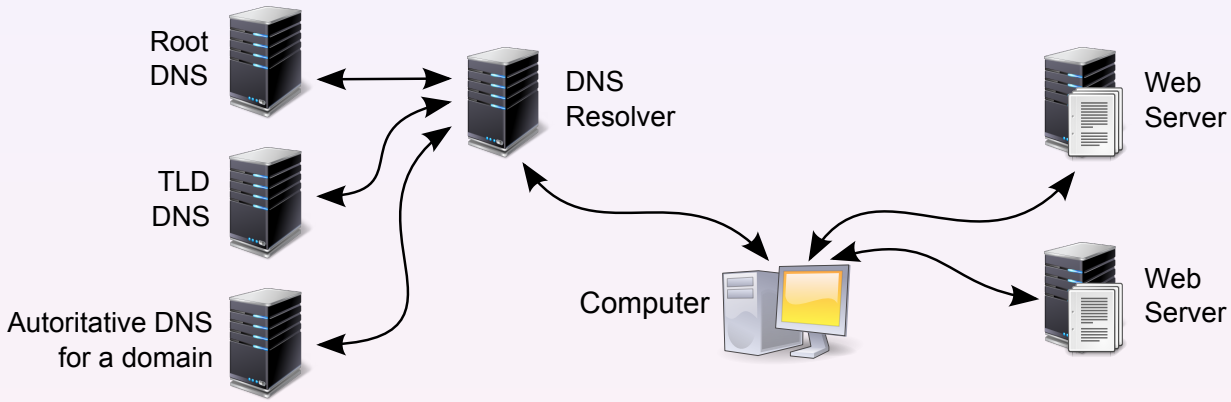
20th Eunice Open European Summer School and Conference 2014
1-5 September 2014, Rennes, France

Part I

Introduction

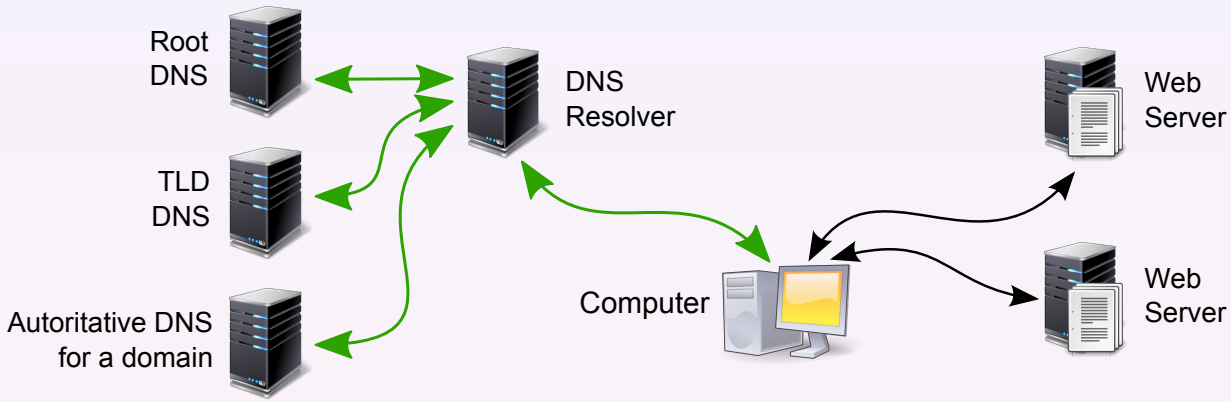
Motivation

Almost every Internet communication is preceded by a translation of a domain name to an IP address.



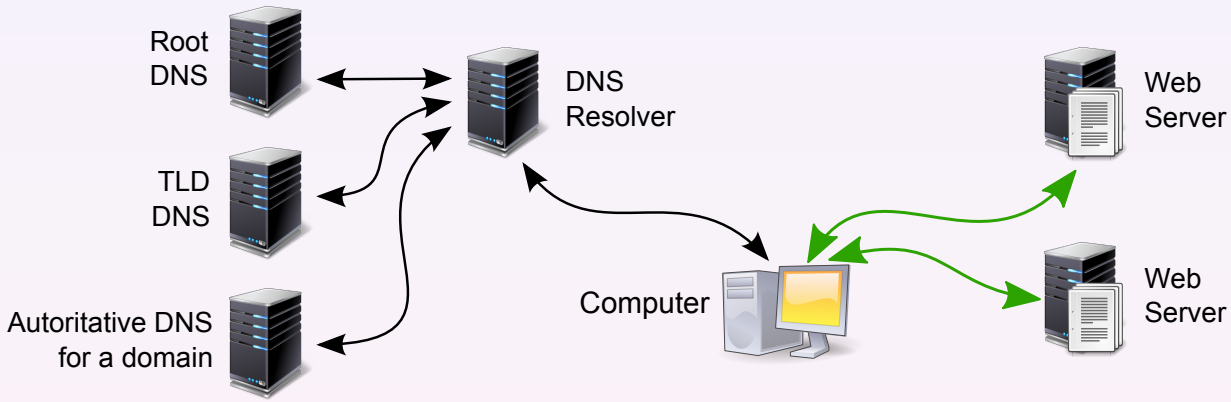
Motivation

Almost every Internet communication is preceded by a translation of a domain name to an IP address.



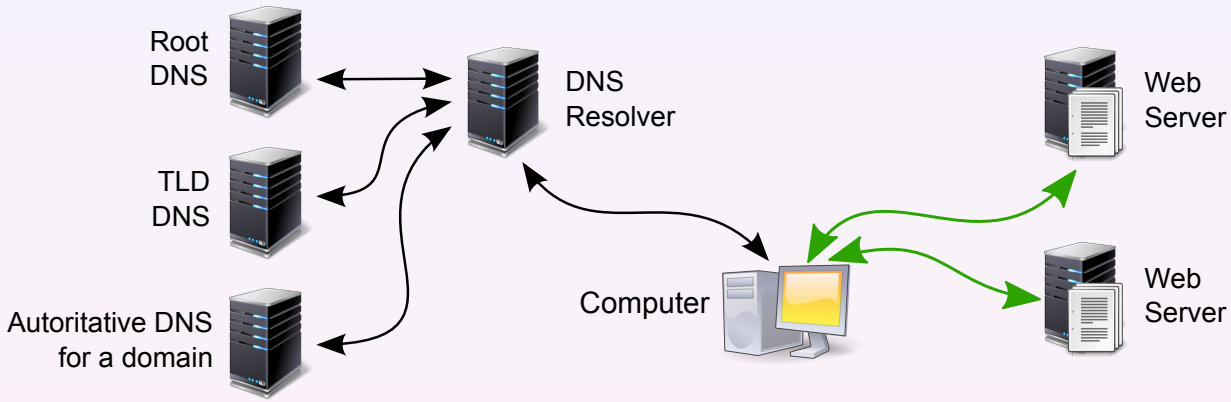
Motivation

Almost every Internet communication is preceded by a translation of a domain name to an IP address.



Motivation

Almost every Internet communication is preceded by a translation of a domain name to an IP address.



DNS Traffic Monitoring Benefits

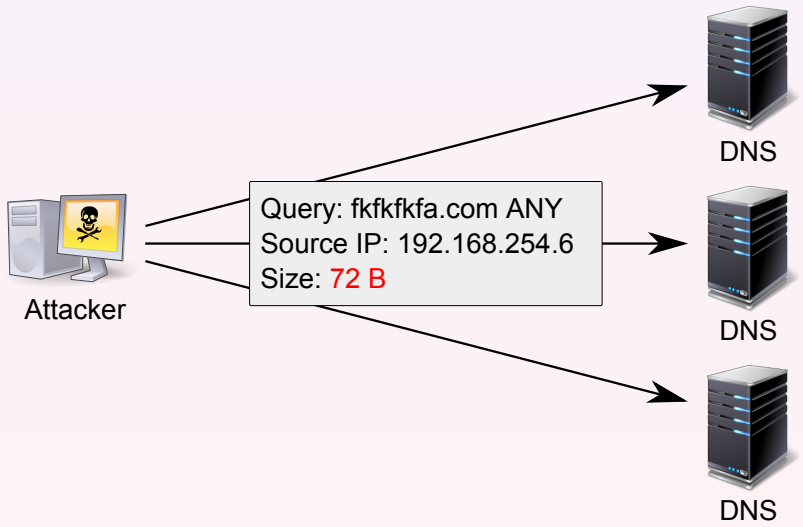
- DNS packets are not encrypted.
- Knowledge of a queried domain can extend capabilities of current anomaly detection methods.
- Possibility to detect anomalies in a DNS traffic itself.

DNS Traffic Attacks and Anomalies

- **Malicious domains queries**
  - Botnet C&C (domain-flux and fast-flux domains),
  - Malware spread,
  - ...
- **Amplification DDoS attacks**
- **And many others ...**

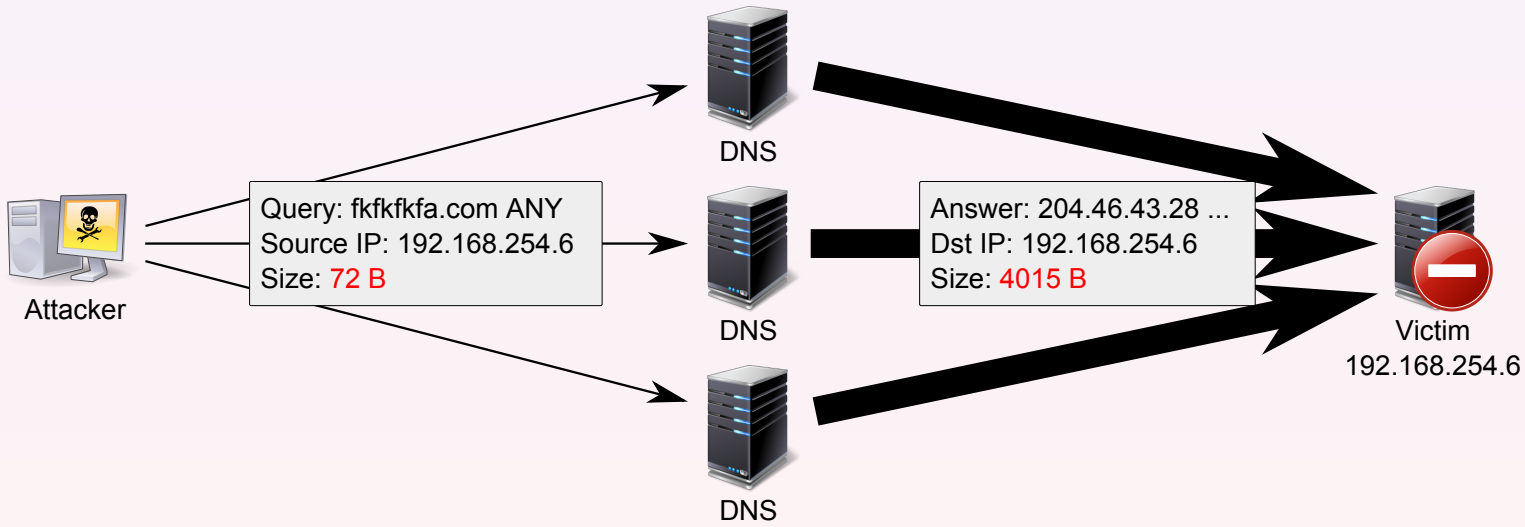
DNS Traffic Attacks and Anomalies

- **Malicious domains queries**
  - Botnet C&C (domain-flux and fast-flux domains),
  - Malware spread,
  - ...
- **Amplification DDoS attacks**
- **And many others ...**



DNS Traffic Attacks and Anomalies

- **Malicious domains queries**
  - Botnet C&C (domain-flux and fast-flux domains),
  - Malware spread,
  - ...
- **Amplification DDoS attacks**
- **And many others ...**



Research Questions

1. How can DNS traffic be **effectively analysed** in large networks?

Research Questions

1. How can DNS traffic be **effectively analysed** in large networks?

2. What are the **differences** in the analysis of DNS traffic using **standard and extended flow** records?

Research Questions

1. How can DNS traffic be **effectively analysed** in large networks?

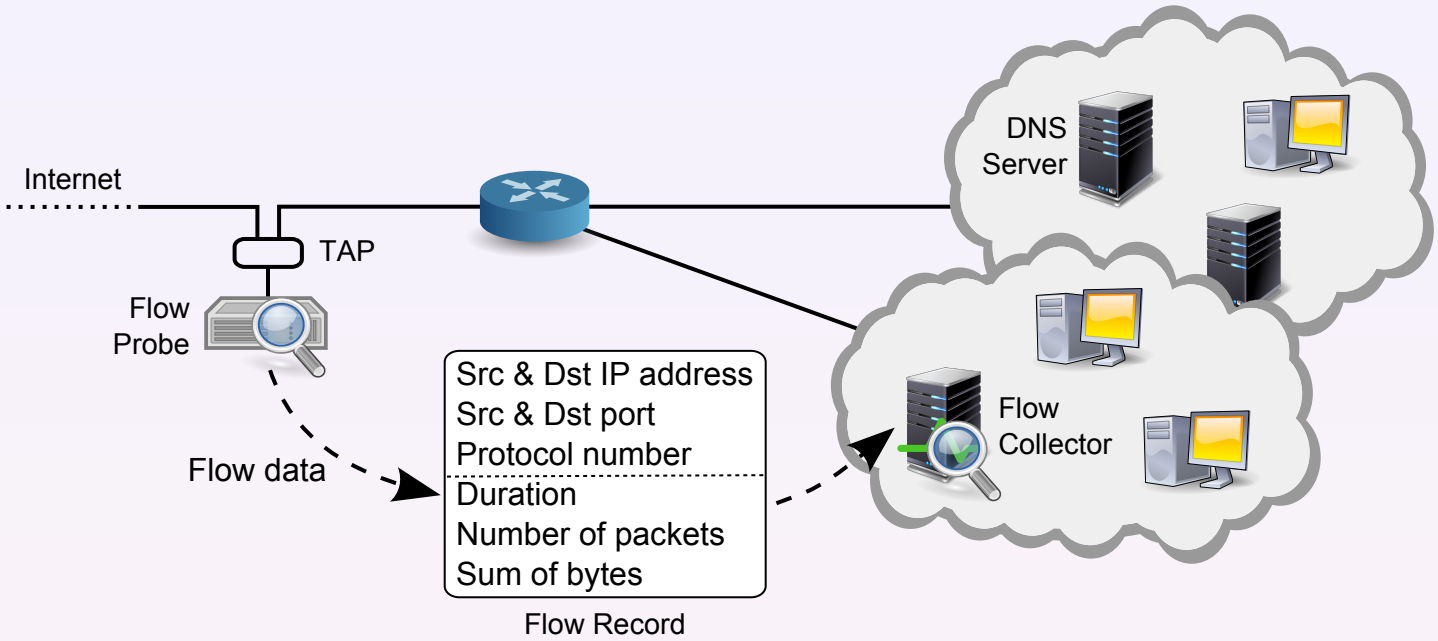
2. What are the **differences** in the analysis of DNS traffic using **standard and extended flow** records?

3. What are the advantages of **combinating DNS traffic** information **with flow** records for network anomaly detection?

Part II

DNS Traffic Monitoring

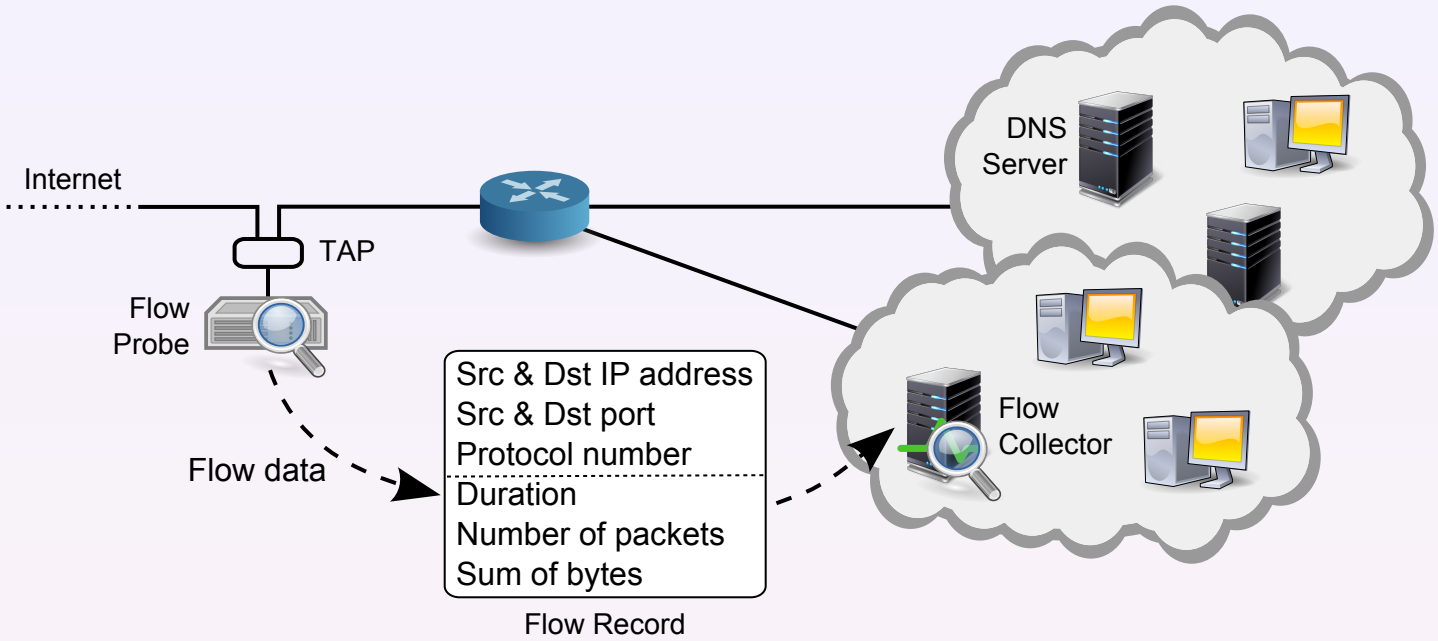
Flow Based DNS Traffic Monitoring



Standard Flow Record

$$F = (IP_{src}, IP_{dst}, P_{src}, P_{dst}, Prot, T_{start}, T_{dur}, Pckts, Octs, Flags)$$

Flow Based DNS Traffic Monitoring



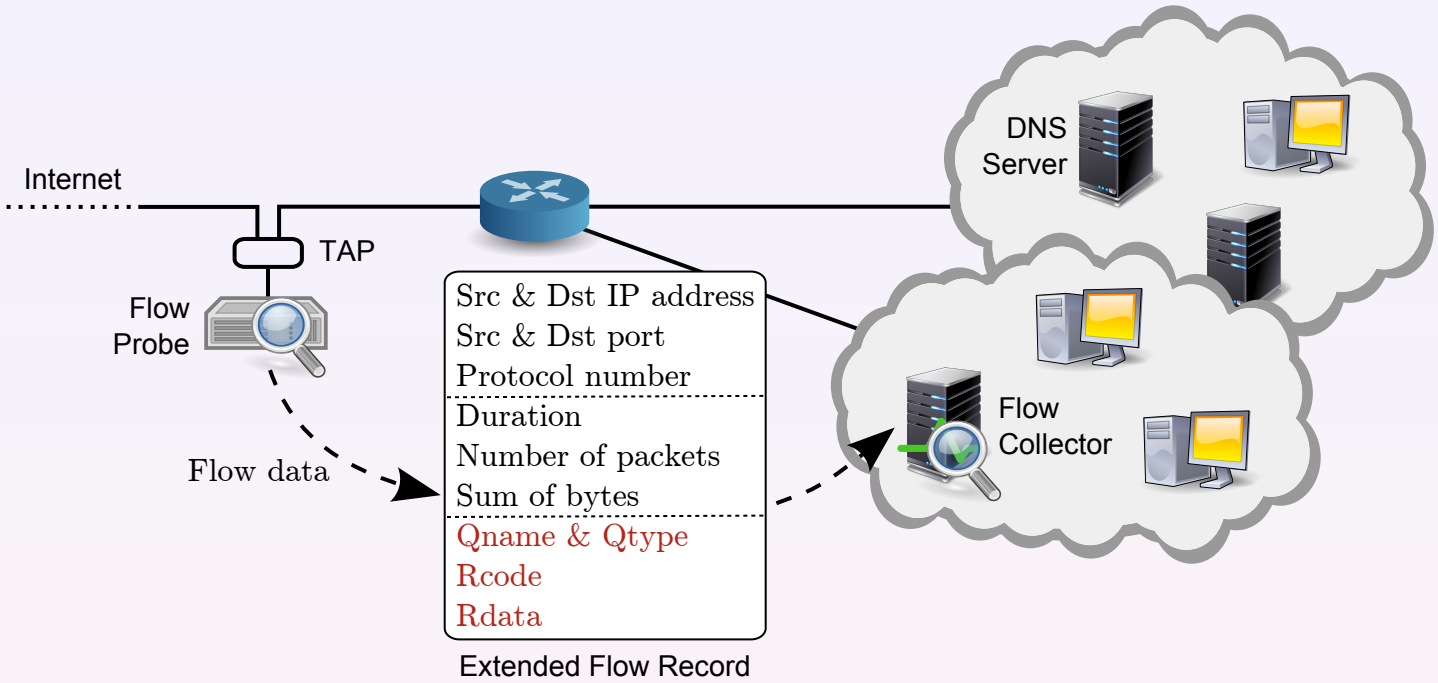
Standard Flow Record

$$F = (IP_{src}, IP_{dst}, P_{src}, P_{dst}, Prot, T_{start}, T_{dur}, Pckts, Octs, Flags)$$

DNS Flow Record

$$F_{DNS} = (Qname, Qtype, Rcode, Rdata)$$

Flow Based DNS Traffic Monitoring

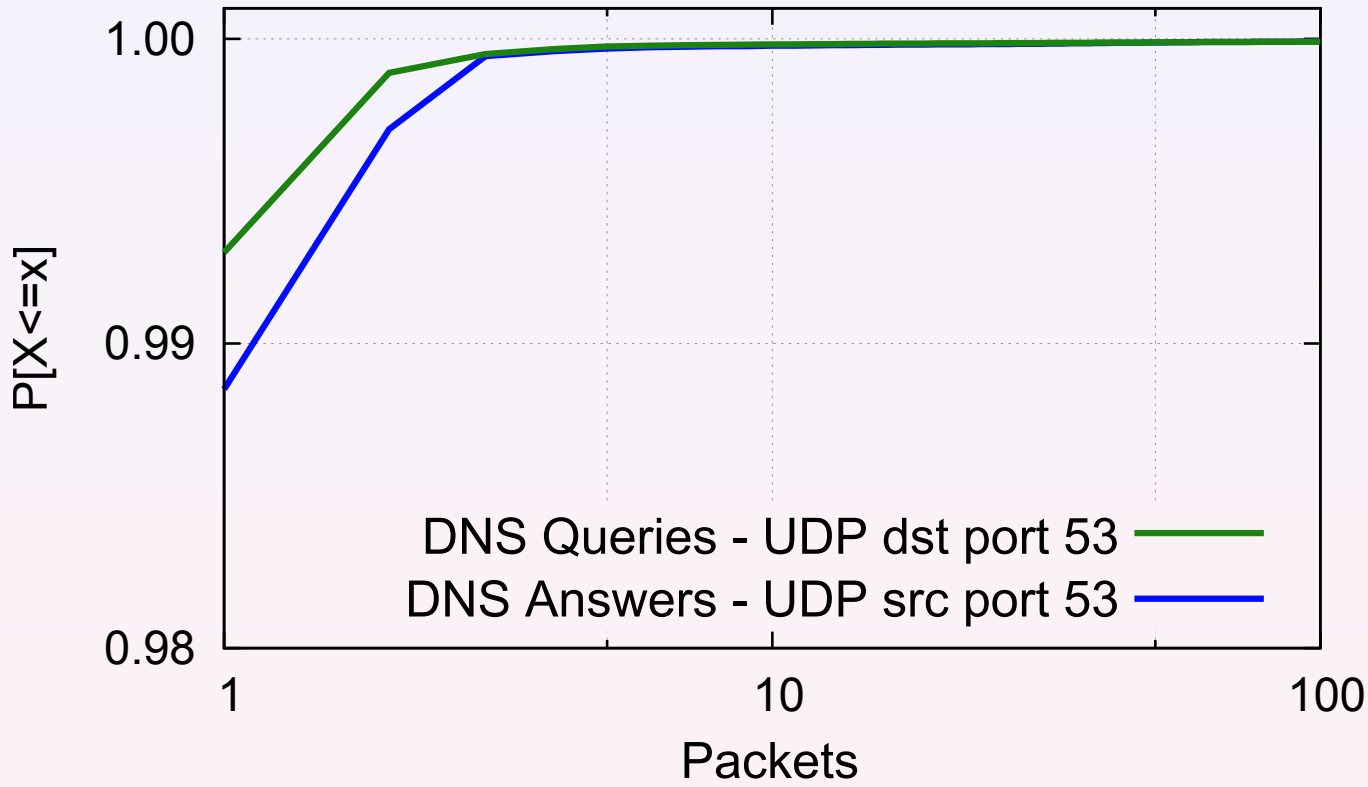


Extended Flow Record

$$F_{ext} = F \cdot F_{DNS} = (IP_{src}, IP_{dst}, P_{src}, P_{dst}, Prot, T_{start}, T_{dur}, Pckts, Octs, Flags, Qname, Qtype, Rcode, Rdata)$$

Flow Based DNS Traffic Monitoring

Cumulative Distribution Function of DNS Packets per Flow



Up to 99 % of flows with port 53 contain only one packet.

⇒ **Flow aggregation is not used.**

Extended Flow Expiration Algorithm

GenerateExtendedFlow (incoming packet)

1. Parse flow information F from incoming packet header.
2. Check if incoming packet contains a valid DNS header.
   3. Parse DNS packet and create a flow record $F_{ext} = F \cdot F_{DNS}$.
   4. Export a flow record F_{ext} without storing in a flow cache.
5. Otherwise update flow record F in a flow cache.

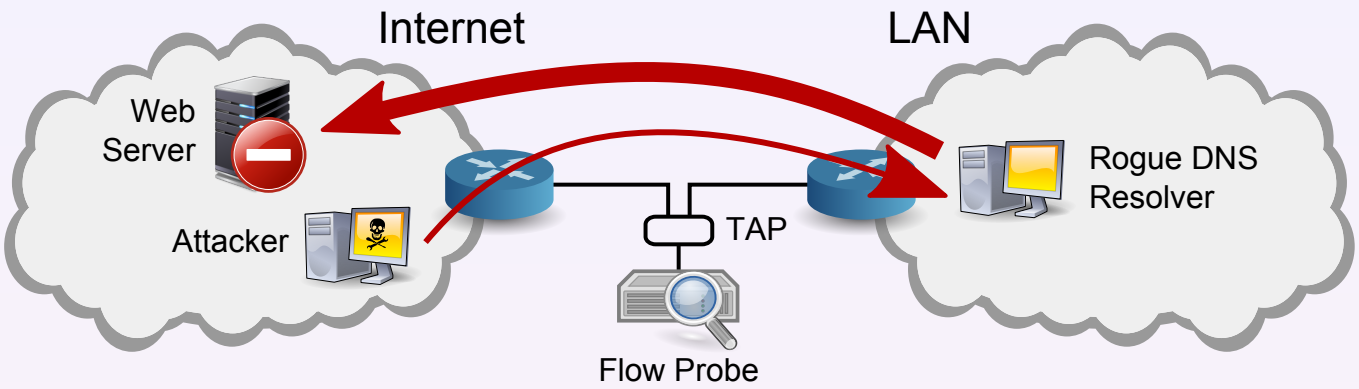
Main Contribution

- Significant **reduction of flow cache memory occupation** due to immediate export of a flow record.

Part III

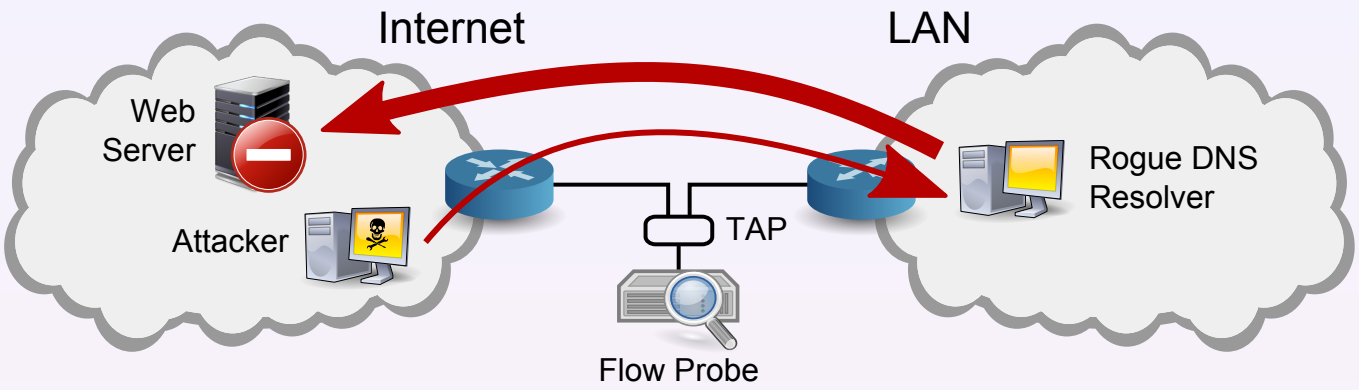
DNS Traffic Anomaly Detection Using Standard Flows

Amplification DDoS Attack



The attack is characterised by a large amount of same queries with spoofed IP address.

Amplification DDoS Attack



The attack is characterised by a large amount of same queries with spoofed IP address.

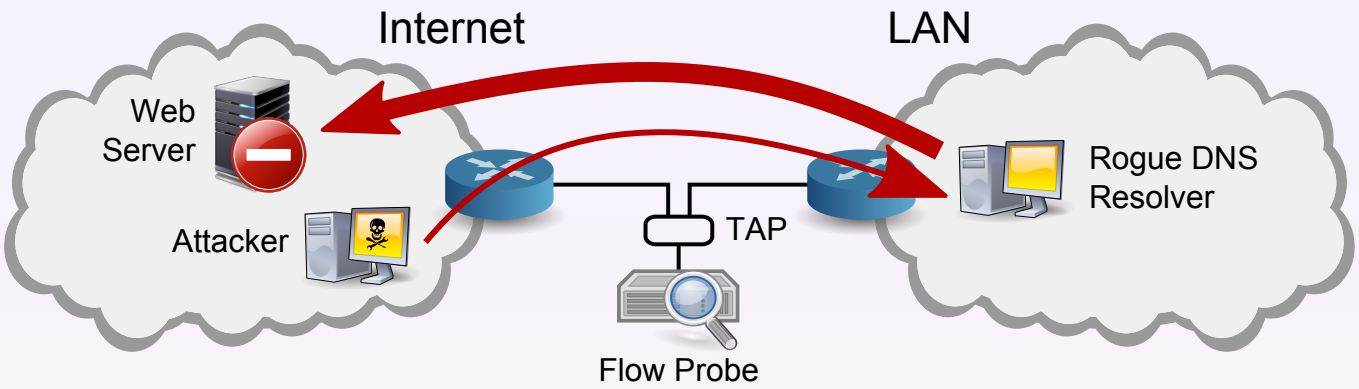
Detection Method

- Increasing count of flows, with high bytes-per-packet ratio and the source port 53.
- Access control lists reflecting network security policy.
- Usually **threshold** adjustment is **required**.

Part IV

DNS Traffic Anomaly Detection Using Extended Flows

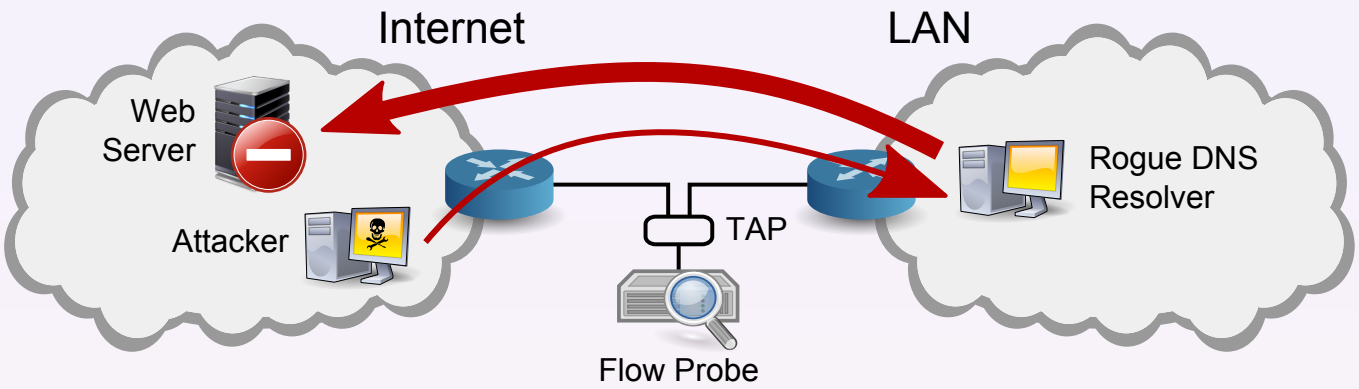
Amplification DDoS Attack



Detection Method

- Malware infected device or misconfigured DNS resolver recognition instead of using basic flow statistics.

Amplification DDoS Attack



Detection Method

- Malware infected device or misconfigured DNS resolver recognition instead of using basic flow statistics.

  $\Rightarrow$ **The problem is to distinguish a regular DNS server responding to a query containing a local domain.**

Amplification DDoS Attack

DetectOpenDNSResolver (DNS response)

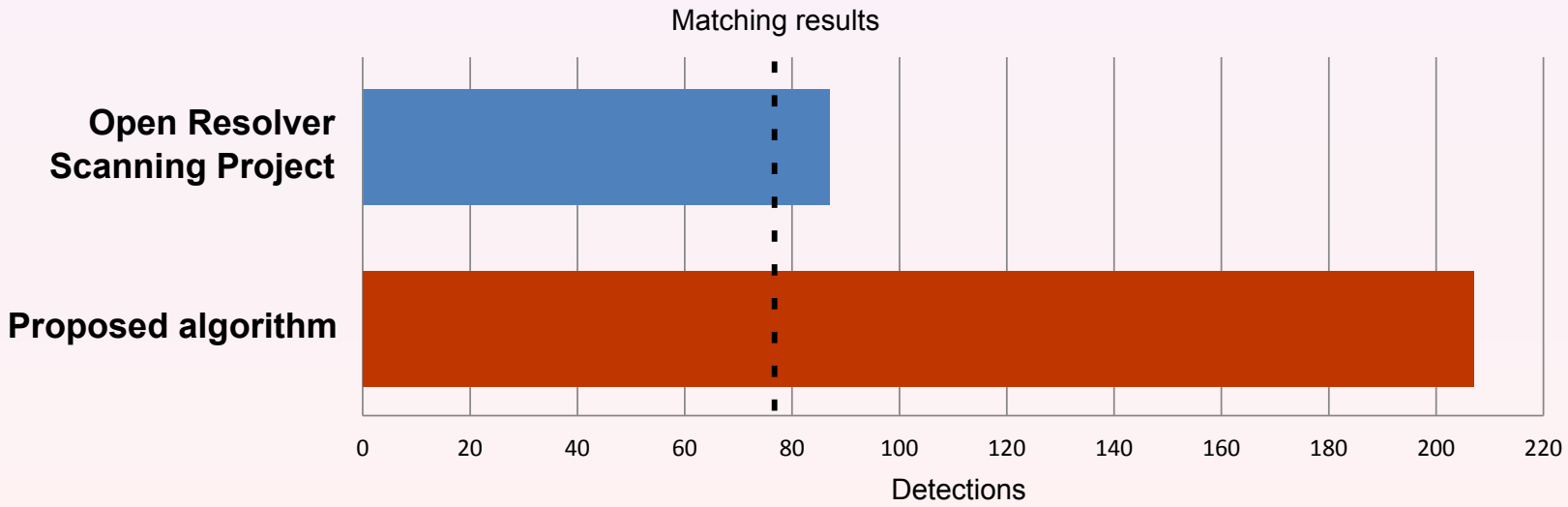
1. Request all information about a domain $F_{ext}.Qname$ in the response by `ANY` query type.
2. Check if the result contains at least one IP address from a local network.
    3. If yes, then add domain to a whitelist of local domains.
    4. Otherwise report $F_{ext}.IP_{src}$ as open DNS resolver.

Amplification DDoS Attack

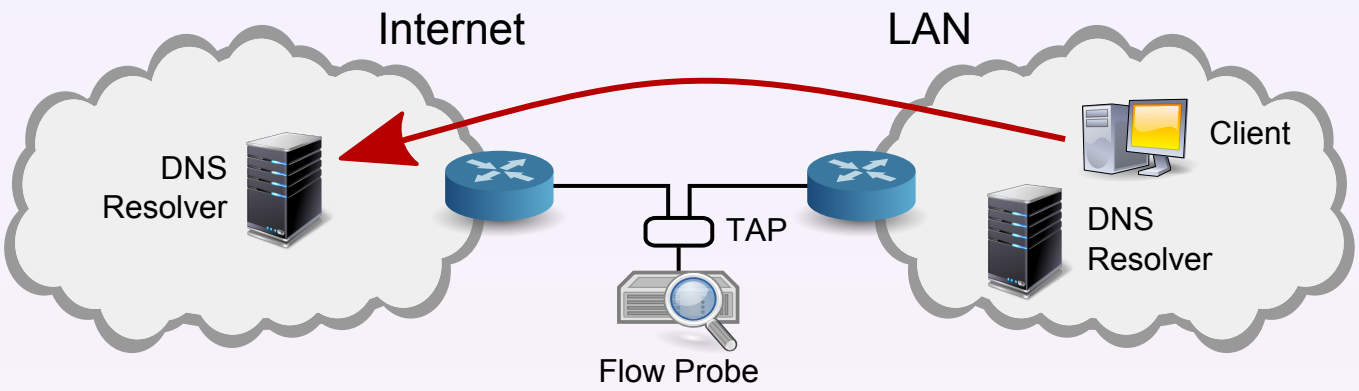
DetectOpenDNSResolver (DNS response)

1. Request all information about a domain $F_{ext}.Qname$ in the response by `ANY` query type.
2. Check if the result contains at least one IP address from a local network.
   3. If yes, then add domain to a whitelist of local domains.
   4. Otherwise report $F_{ext}.IP_{src}$ as open DNS resolver.

Detection Results



External DNS Resolver Usage Detection



Usage of an external DNS resolver may cause delay and also presents a security risk if the external DNS resolver responds with fraudulent IP addresses.

Detection Method

- In well-maintained networks is based on access control lists.
- In not well-maintained networks is a **problem to distinguish** between a **client** device and a local **DNS resolver**.

External DNS Resolver Usage Detection

DetectExternalDNS (DNS response)

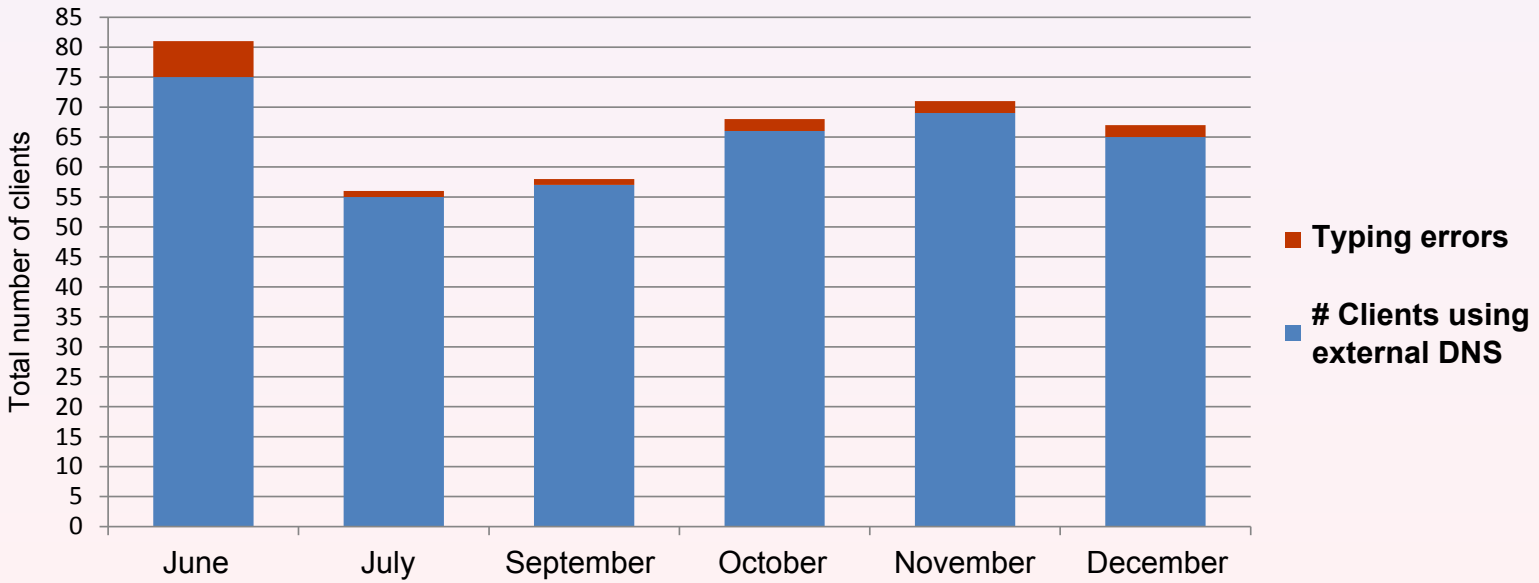
1. Get time of the response $F_{ext}.T_{start}$ and IP address of queried domain $F_{ext}.Rdata$.
2. Check if client $F_{ext}.IP_{dst}$ visits queried domain during $F_{ext}.T_{start} + 2\ sec$.
    3. If yes, then return client $F_{ext}.IP_{dst}$ as device using external DNS resolver.

External DNS Resolver Usage Detection

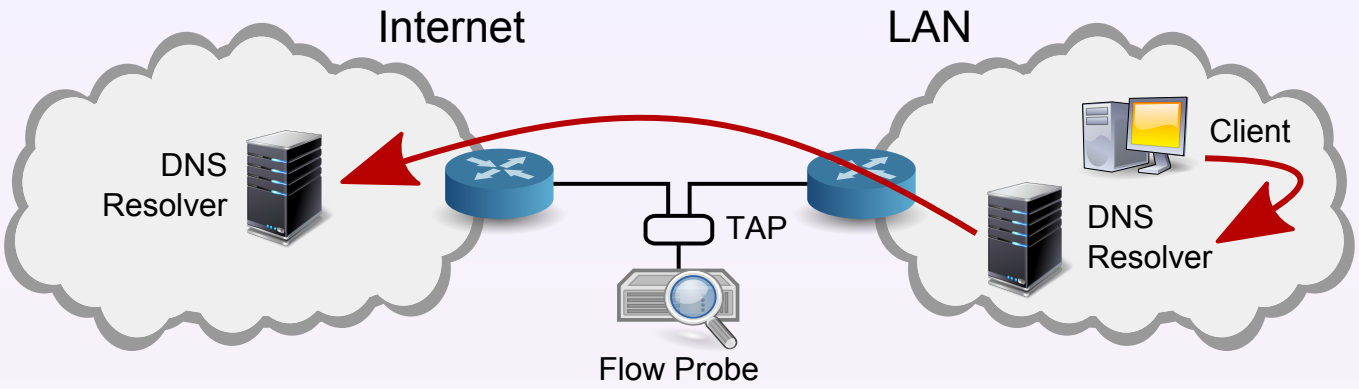
DetectExternalDNS (DNS response)

1. Get time of the response $F_{ext}.T_{start}$ and IP address of queried domain $F_{ext}.Rdata$.
2. Check if client $F_{ext}.IP_{dst}$ visits queried domain during $F_{ext}.T_{start} + 2\ sec$.
    3. If yes, then return client $F_{ext}.IP_{dst}$ as device using external DNS resolver.

Detection Results



Malware Domains Query Detection

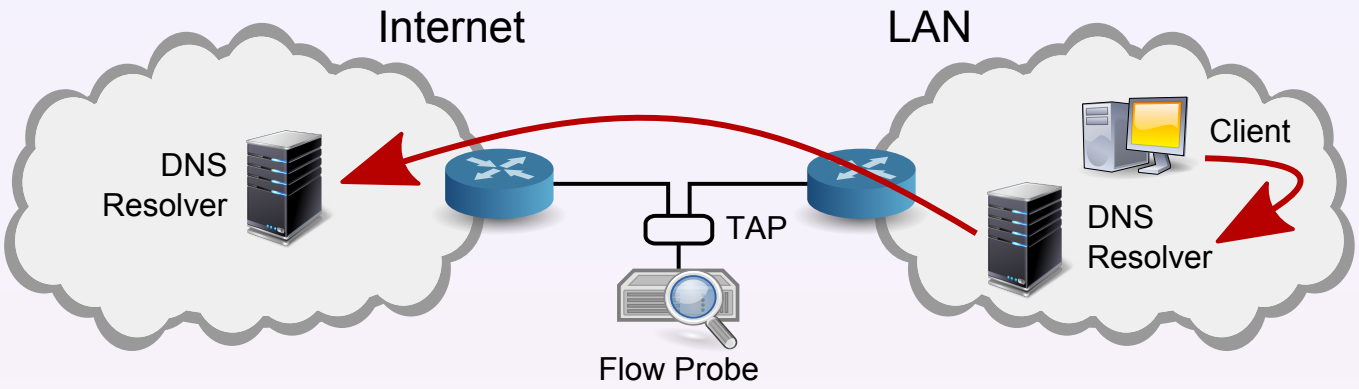


DNS queries generated by botnets (command and control center) or domains used for a malware spreading.

Detection Method

- Check all queried domains whether they are occurred in any malware domains blacklist.

Malware Domains Query Detection



DNS queries generated by botnets (command and control center) or domains used for a malware spreading.

Detection Method

- Check all queried domains whether they are occurred in any malware domains blacklist.

  $\Rightarrow$ **Testing all queried domains may be very time consuming.**

Malware Domains Query Detection

GetMalwareAffectedDevices ()

1. Detect device querying the domain $F_{ext}.Qname = dns.msftncsi.com$.
2. Select next `N` queried domains.
3. Exclude domains occurring in the Alexa top domains list.
4. Check the rest of domains if they are in blacklists.

Malware Domains Query Detection

GetMalwareAffectedDevices ()

1. Detect device querying the domain $F_{ext}.Qname = dns.msftncsi.com$.
2. Select next `N` queried domains.
3. Exclude domains occurring in the Alexa top domains list.
4. Check the rest of domains if they are in blacklists.

Detection Results

Domain	Number of blacklists
habble.ru	6
www.softosystem.com	7
cybeitrapp.info	5
telemetry.tanzuki.net	5
cybermindtool.info	4

Part V

Conclusion

Conclusion

- DNS information does **not affect the privacy** of users.
- **IP flows** represents optimal choice for a **large scale network monitoring**.
- Proposed updated DNS flow **exporting algorithm saving a flow cache** and exporting only necessary DNS packet fields.
- **New** network **anomaly detection algorithms** using DNS extended flows.
  - `https://is.muni.cz/publication/1131184?lang=en`

Thank You For Your Attention!

Detection of DNS Traffic Anomalies in Large Networks

Milan Čermák
cermak@ics.muni.cz

Pavel Čeleda
celeda@ics.muni.cz

Jan Vykopal
vykopal@ics.muni.cz