Detection of DNS Traffic Anomalies in Large Networks

Milan Čermák, Pavel Čeleda, Jan Vykopal

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

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

![Diagram](image.png)
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 . . .**

---

![Diagram showing DNS traffic attacks and anomalies](image)
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?
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 combining DNS traffic information with flow records for network anomaly detection?
Part II

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

\[ F_{DNS} = (Qname, Qtype, Rcode, Rdata) \]
Extended Flow Record

\[ F_{\text{ext}} = F \cdot F_{\text{DNS}} = (IP_{\text{src}}, IP_{\text{dst}}, P_{\text{src}}, P_{\text{dst}}, Prot, T_{\text{start}}, T_{\text{dur}}, Pckts, Octs, Flags, Qname, Qtype, Rcode, Rdata) \]
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 $F_{\text{ext}} = F \cdot F_{\text{DNS}}$.
   4. Export a flow record $F_{\text{ext}}$ 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
The attack is characterised by a large amount of same queries with spoofed IP address.
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
**Detection Method**

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

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

⇒ 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 $F_{ext} \cdot Qname$ in the response by ANY query type.

2. Check if the result contains at least one IP address from a local network.
   - If yes, then add domain to a whitelist of local domains.
   - Otherwise report $F_{ext} \cdot IP_{src}$ as open DNS resolver.
Amplification DDoS Attack

DetectOpenDNSResolver (DNS response)

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

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

**Detection Results**

![Bar chart showing detection results for different months and typing errors](chart.png)

- **Total number of clients**
- **# Clients using external DNS**
- **Typing errors**

Milan Čermák et al.  Detection of DNS Traffic Anomalies in Large Networks
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.
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.

⇒ Testing all queried domains may be very time consuming.
Malware Domains Query Detection

GetMalwareAffectedDevices ()

1. Detect device querying the domain $F_{\text{ext}}.Qname = \text{dns.msftncsi.com}$.

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

<table>
<thead>
<tr>
<th>Domain</th>
<th>Number of blacklists</th>
</tr>
</thead>
<tbody>
<tr>
<td>habble.ru</td>
<td>6</td>
</tr>
<tr>
<td><a href="http://www.softosystem.com">www.softosystem.com</a></td>
<td>7</td>
</tr>
<tr>
<td>cybeitrapp.info</td>
<td>5</td>
</tr>
<tr>
<td>telemetry.tanzuki.net</td>
<td>5</td>
</tr>
<tr>
<td>cybermindtool.info</td>
<td>4</td>
</tr>
</tbody>
</table>
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.
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