Botnet Detection Approaches Based on DNS Traffic Analysis: Critical Review

Presented by
Saif Al-Mashhadi,
Outlines

• INTRODUCTION
• BACKGROUND
• Critical Review
• Discussion
Botnet and botnet threats

Steal information “password, credit card” and bitcoin mining
DDOS Attacks Caused by botnet

Source Arbor

Source Akamai
Botnet Communication

- IRC
- HTTP
- P2P
- DNS
Botnet Life cycle

- The bot tries to locate and connect to the command and control server,
- Since the bots sending many discovery packets, bots will be vulnerable during this phase.
- Bot tries to perform a series of malicious activities based on the commands from its botmaster.
- The bot updates their behaviour and perform new malicious activities.

Initial infection and propagation phase.

Connection and rallying phase

The malicious and attack phase

Maintenance and upgrading phase
Botnet life cycle cont.
Botnet Based DNS Evasion Approaches

Fast-Flux
Botnet Based DNS Evasion Approaches cont.

User visit malicious site/email/software

C&C server IP resolved

C&C Server

Attacker generate and register AGD azanged.cn ,A record = C&C server IP

DGA
Botnet Detection Based on DNS Analysis

Botnet detection based-DNS

Honeypot

IDS

Anomaly based

Signature-based

Network-based

Host-based

Passive

Active
Honeybot
# BOTNET DOMAIN NAME FEATURES

<table>
<thead>
<tr>
<th>Future set</th>
<th>Feature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name based feature</strong></td>
<td>Meaningful length ratio</td>
</tr>
<tr>
<td></td>
<td>Domain character Entropy (Randomness)</td>
</tr>
<tr>
<td><strong>Message base features</strong></td>
<td>Number of source IPs</td>
</tr>
<tr>
<td></td>
<td>Numbers of A, AAAA, NS and MX querying</td>
</tr>
<tr>
<td><strong>Request features</strong></td>
<td>Total querying request per day</td>
</tr>
<tr>
<td></td>
<td>Querying request per hour</td>
</tr>
<tr>
<td></td>
<td>Number of NXDomain</td>
</tr>
<tr>
<td><strong>Time Based Future</strong></td>
<td>Domain Registration Date</td>
</tr>
<tr>
<td></td>
<td>TTL</td>
</tr>
<tr>
<td><strong>Reputation based</strong></td>
<td>IP reputation list</td>
</tr>
<tr>
<td></td>
<td>Domain reputation list</td>
</tr>
</tbody>
</table>
Critical Review

• The existing features of DNS query and response are not accurate enough to detect the presence of DNS botnet.
• Therefore, there are a need for more efficient features that can accurately detect DNS botnet.
• Entropy value as feature to calculate the randomness in the domain name of DNS query can significantly contribute to DNS based botnet.
• The randomness of the domain name is a result of DGA algorithm that employed to generate malicious domains.
• Others features such as the registration date, compare domain request with domain and IP address reputation database that can be used along with the entropy value might be lead to a better accuracy of DNS botnet detection.
Thank you