DOTS extension for Attack type and bandwidth

1. Draft-chen-dots-attack-type-expansion-00
2. draft-chen-dots-attack-bandwidth-expansion-01

Meiling Chen, Li Su, Jin Peng
China Mobile Research Institute
March 2019
China Mobile's mitigation architecture of DDoS
Attack-bandwidth expansion
Draft-chen-dots-attack-bandwidth-expansion-00
Requirements

USE CASE 1
Optimal clean device selection

USE CASE 2
Optimum BGP redirect path for mitigation
Threshold: 70%

USE CASE 3
Offload the extreme large flow
Example: Ensure 10% success rate
Target-Attack-Type expansion

Draft-chen-dots-attack-type-expansion-00
Current status

- Different vendors are good at handling different types of DDoS attack.

**USE CASE 1**

- Mixed traffic attack
- Mitigator A for connectionless Flood, Mitigator B for CC attack
- Mitigation coordination

**Benefits**

- Mitigators can coordinate to mitigate attack flow.
- Shorten mitigation time.

**Fig. 1 Mixed attack**

**Fig. 2 direct mitigation**
Functions

- Verification the attack type
- Adjust detection strategy for different vendors
- Analysis of malicious reporting nodes
- Convenient management

Requirements for Unified naming format

- Equipment of different vendors cooperates each other easy to appear interactive chaos
Standard attack type definition (syntax)

[protocol level] [protocol name] [message name/operation name/port]
[attack methods feature description field 1] [attack methods feature description field 2] [attack methods describe the standard field]

<table>
<thead>
<tr>
<th>Protocol level (mandatory)</th>
<th>Protocol name (mandatory)</th>
<th>message name/operation name/port (optional)</th>
<th>attack methods feature description field 1 (optional)</th>
<th>attack methods feature description field 2 (optional)</th>
<th>attack methods described the standard field (mandatory)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network_Layer</td>
<td>ICMP</td>
<td>——</td>
<td>——</td>
<td>——</td>
<td>Flood</td>
</tr>
<tr>
<td>Transport_Layer</td>
<td>TCP</td>
<td>SYN</td>
<td>——</td>
<td>——</td>
<td>Flood</td>
</tr>
<tr>
<td>Transport_Layer</td>
<td>UDP</td>
<td>Memcached</td>
<td>Reflection</td>
<td>Amplification</td>
<td>Flood</td>
</tr>
<tr>
<td>Application_Layer</td>
<td>HTTP</td>
<td>GET</td>
<td>——</td>
<td>——</td>
<td>Flood</td>
</tr>
</tbody>
</table>

DDoS attack name complete definition and abbreviation definition example

<table>
<thead>
<tr>
<th>Attack name (complete)</th>
<th>Attack name (abbreviation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network_Layer ICMP Flood</td>
<td>ICMP Flood</td>
</tr>
<tr>
<td>Transport_Layer TCP SYN Flood</td>
<td>TCP SYN Flood</td>
</tr>
<tr>
<td>Transport_Layer UDP Memcached Reflection Amplification Flood</td>
<td>UDP Memcached Flood</td>
</tr>
<tr>
<td>Application_Layer HTTP GET Flood</td>
<td>HTTP GET Flood</td>
</tr>
</tbody>
</table>
Next steps:
1. Comments
2. Use case valuable?
3. Questions?