A First Joint Look at DoS Attacks and BGP Blackholing in the Wild

Mattijs Jonker
Aiko Pras (UTwente)
Alberto Dainotti (CAIDA / UC San Diego)
Anna Sperotto (UTwente)

UNIVERSITY OF TWENTE.
Denial-of-Service attacks

● A conceptually simple, yet effective class of attacks
  ... that have gained a lot in popularity over the last years
  ... are also offered “as-a-Service” (Booters)

● Some well-known incidents stipulate threat/risks
  – e.g., attacks on Dyn & GitHub (memcached)

  New world record DDoS attack hits 1.7Tbps
days after landmark GitHub outage

Memcached denial-of-service attacks are getting bigger by the day, according to new analysis.

By Liam Tung | March 6, 2018 -- 12:34 GMT (04:34 PST) | Topic: Security

● DoS has become one of the biggest threats to Internet stability & reliability
BGP blackholing

- Is a technique that can be used to mitigate DoS attacks
- Leverages the BGP control plane to drop network traffic
- BGP communities are used to signal blackholing requests
  - by “tagging” prefix announcements with `<asn:value>`
  - 666 is a common value for blackholing
- Is very “coarse-grained”, meaning all network traffic destined to a prefix is indiscriminately dropped
A missing piece of the puzzle

Given its coarse-grained nature, we wonder if blackholing is used only in extreme cases.

A clear understanding of how blackholing is used in practice when DoS attacks occur is missing.

We use large-scale, longitudinal (3y) data sets on DoS attacks and blackholing to get more insights into operational practices.
Part 1: Blackholed Attacks
UCSD Network Telescope [data set 1/3]

- A large, /8 network telescope operated by UC San Diego
- Captures backscatter from DoS activity in which source IP addresses are *randomly and uniformly spoofed*
- We use the classification methodology by Moore et al. to infer DoS attacks [1]

Amplification Honeypots [data set 2/3]

- Honeypots
  - ... mimick reflectors abused in reflection attacks (e.g., NTP)
  - ... try to be appealing to attackers by offering large amplification
  - ... capture attempts at reflection
- We use logs from 24 honeypot instances that are geographically & logically distributed
  - From the AmpPot project (Christian Rossow, CISPA) [1]

Inferred blackholing events [data set 3/3]

- Scan BGP collector data for blackholing activity, using public BGP data: RIPE RIS and UO Route Views
- Use BGPStream framework for BGP data analysis [1]
- Match BGP updates against dictionary of known BH communities [2]


Measurement systems placement

A First Joint Look at DoS Attacks and BGP Blackholing in the Wild
Measurement systems placement

Attacking host(s) (e.g., botnet) randomly spoofed

SYN
Src: 123.4.5.6
Dst: victim-addr

provider AS
Interconnecting link

victim AS

Victim
IP: victim-addr

SYN | ACK
Src: victim-addr
Dst: 123.4.5.6

UCSD-NT
123.0.0.0/8

Network Telescope

A First Joint Look at DoS Attacks and BGP Blackholing in the Wild
Measurement systems placement

Attacking host(s) (e.g., botnet)

DNS query
Src: victim-addr
Dst: reflector-addr

DNS answer
Src: reflector-addr
Dst: victim-addr

Reflected & Amplification

Abused amplifiers

AmpPot

A First Joint Look at DoS Attacks and BGP Blackholing in the Wild
Measurement systems placement

**Attacking host(s)** (e.g., botnet)

**DNS query**
Src: victim-addr
Dst: reflector-addr

**DNS answer**
Src: reflector-addr
Dst: victim-addr

**SYN**
Src: 123.4.5.6
Dst: victim-addr

**SYN | ACK**
Src: victim-addr
Dst: 123.4.5.6

**Interconnecting link**

**UCSD-NT**
123.0.0.0/8

**Network Telescope**

**Abused amplifiers**

**AmpPot**
A First Joint Look at DoS Attacks and BGP Blackholing in the Wild
Attacks are mitigated within minutes

- More than half of attacks mitigated within minutes
  - 84.2% within ten minutes
  - takes longer than six hours for only 0.02%
- Suggest use of automated, rapid detection and mitigation
Blackholing endures after attacks end

- Deactivated within **three** hours following 74.8% of BH’d attacks
- For 3.9% it takes more than **24** hours
  - Suggests lack of automation in recovery
- Side effects of coarse-grained technique extend well beyond duration of attack
Less intense attacks are also BH’d

- ~2/3rd of BH’ed attacks (against ~9/10th of all attacks) have an intensity of up to ~300Mbps (100pps),
- 13.1% see at most 3Mbps (1pps), showing that operators take drastic measures for less intense attacks
- Similar findings for reflection attacks (see paper)
- Results confirm Moore et al. methodology at scale (USENIX ‘01)
- Corroborates our previous finding of ~30k attacks/day (IMC ‘17) [1]

Attacks we do not see

- Match blackholing events with preceding attacks

<table>
<thead>
<tr>
<th>source</th>
<th>#BH events</th>
<th>#BH’d prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSD-NT ⋃ AmpPot</td>
<td>363.0k / 1.3M (27.8%)</td>
<td>45.2k / 146.2k (30.9%)</td>
</tr>
</tbody>
</table>

- We match 27.8% of BH events with DoS attacks
- Results do not allow us to infer the fraction of other types of attacks (e.g., direct and unspoofed)
- However, highlights that reflection and randomly spoofed DoS represent a significant share of DoS that operators had to deal with
Part 2: Service Collateral
DNS Measurements [data set 1/2]

- Large dataset of active DNS measurements
- Provides mappings from IPv4 to:
  - *Websites* (www. → A RR)
  - *Mail exchangers* (MX → A)
  - *Authoritative nameservers* (NS → A)
- We use .com, .net & .org (~50% of global namespace)

<table>
<thead>
<tr>
<th>type</th>
<th>#prefixes</th>
<th>#names associated</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>overall</td>
<td>no-alt</td>
<td>ratio</td>
<td></td>
</tr>
<tr>
<td>Web</td>
<td>13.7k (9.3%)</td>
<td>782k</td>
<td>670k</td>
<td>0.86</td>
<td></td>
</tr>
<tr>
<td>Mail</td>
<td>2247 (1.5%)</td>
<td>180k</td>
<td>177k</td>
<td>0.98</td>
<td></td>
</tr>
<tr>
<td>NS</td>
<td>1176 (0.8%)</td>
<td>10k</td>
<td>10k</td>
<td>0.99</td>
<td></td>
</tr>
</tbody>
</table>
Reactive measurements [data set 2/2]

- Reactively measure blackholed /32s
  - Upon BH *activation* (i.e., announcement) and *deactivation* (i.e., withdrawal/re-announcement)
  - Subject to various heuristics (max 4 in /24, spacing, ...)
- Use RIPE Atlas to send traceroutes
  - From probes in *peer, customer & provider* networks
- Scan a handful of IANA-assigned ports
  - For Web, mail and DNS
  - From a single VP
Inferring blackhole (in)efficacy

**Port probes**
- Exclusively open state on *deactivation* → infer efficacy
- Open on *activation* → infer inefficacy
- Other cases → inconclusive

**Traceroutes**
- Exclusively last_hop_is_destination on *deactivation* → infer efficacy
- last_hop_is_destination on *activation* → infer inefficacy
Port probe inferences

<table>
<thead>
<tr>
<th>response</th>
<th>#service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Web</td>
</tr>
<tr>
<td>a ∪ d</td>
<td>2886</td>
</tr>
<tr>
<td>a ∩ d</td>
<td>6.98%</td>
</tr>
<tr>
<td>a \ d</td>
<td>0.38%</td>
</tr>
<tr>
<td>d \ a</td>
<td>92.64%</td>
</tr>
</tbody>
</table>

- Jointly, we infer efficacy in 95.25% of “coverable” cases
- The a \ d category is near-zero, which supports the chosen methodology
## Trace route inferences

<table>
<thead>
<tr>
<th>Probe network</th>
<th>#groups</th>
<th>inference</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Efficacy</td>
<td>Inefficacy</td>
<td>∩</td>
<td></td>
</tr>
<tr>
<td>peer</td>
<td>5.0k</td>
<td>29%</td>
<td>8%</td>
<td>1.0%</td>
<td></td>
</tr>
<tr>
<td>provider</td>
<td>5.4k</td>
<td>29%</td>
<td>6%</td>
<td>0.8%</td>
<td></td>
</tr>
<tr>
<td>customer</td>
<td>2.0k</td>
<td>17%</td>
<td>8%</td>
<td>2.1%</td>
<td></td>
</tr>
</tbody>
</table>

- Jointly, we infer efficacy significantly more often than inefficacy
- But our “coverage” is limited (i.e., last hops never respond)
Corroborated Service Collateral

<table>
<thead>
<tr>
<th>type</th>
<th>#prefixes</th>
<th>#corroborated names</th>
<th>#affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td>734</td>
<td>30916</td>
<td></td>
</tr>
<tr>
<td>Mail</td>
<td>107</td>
<td>3533</td>
<td>522</td>
</tr>
<tr>
<td>NS</td>
<td>46</td>
<td>323</td>
<td>708</td>
</tr>
</tbody>
</table>

- Unreachable for the duration of the blackhole
  - At least for part of the Internet
- However
  - MTA retries may simply incur a delay
  - Cache mechanism may mitigate NS issues
Conclusions

- We started addressing the lack of understanding in how blackholing is used in practice when DoS attacks occur
  - e.g., we wondered if blackholing is used only in extreme cases
- Although we only provide first insights, our findings show:
  - Rapid reaction times suggest frequent use of automation
  - Excessive retention times suggest lack of automated recovery
  - Less intense attacks are also mitigated
- Preliminary augmentation with complementary measurements
  - Enabled us to corroborate BH (in)efficacy
  - “coverage” is limited (e.g., due to observation delays, firewalls)
- Future work
  - We linked only 28% of blackholing to attacks!
  - Improve reactive measurements (e.g., path or last hop analyses)
Questions
?

Mattijs Jonker
m.jonker@utwente.nl
linkedin.com/in/mattijsj/
mattijsjonker.com

A First Joint Look at DoS Attacks and BGP Blackholing in the Wild
A First Joint Look at DoS Attacks and BGP Blackholing in the Wild
Previous study [1/2]

DoS characterization at scale

- Integrates data from a large darknet, honeypots and a platform for DNS measurements
- Finds macroscopic and detailed insights about DoS attacks
  - ~30k attacks daily, Internet-wide
  - Affecting many networks and /24 blocks
  - Various attack types are sometimes launched simultaneously against the same target
  - Migration to cloud-based protection occurs faster following more intense attacks

Previous study [2/2]

**Blackholing activity at scale**

- Systematically studies BGP blackholing at scale
  ... using large public and private BGP routing data sets
- Finds detailed insights that relate to, among others:
  ... the adoption of blackholing over time
  ... effects on the data plane
  ... operational practices

*Giotsas et al., “Inferring BGP blackholing activity in the internet”, in IMC 2017*
Data sets

Attacks: 28 million in total

<table>
<thead>
<tr>
<th>source</th>
<th>#events</th>
<th>#targets</th>
<th>#ASNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSD-NT $\cup$ AmpPot</td>
<td>28.1M</td>
<td>8.6M</td>
<td>36.9k</td>
</tr>
<tr>
<td>UCSD-NT $\cap$ AmpPot</td>
<td>447.6k</td>
<td>0.2M</td>
<td>9.2k</td>
</tr>
</tbody>
</table>

• Blackholing events: 1.3 million in total

<table>
<thead>
<tr>
<th>#BH events</th>
<th>#prefixes</th>
<th>#origins</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3M</td>
<td>146.2k</td>
<td>2.7k</td>
</tr>
</tbody>
</table>
Blackholed attacks [1/2]

- Match attacks with succeeding mitigation through BH
  ... by requiring BH prefix to “cover” attacked /32
  ... and cap at 24h

<table>
<thead>
<tr>
<th>source</th>
<th>#attacks</th>
<th>#targets</th>
<th>#ASNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSD-NT ⋃ AmpPot</td>
<td>456.0k / 28.1M (1.6%)</td>
<td>70k / 8.6M (0.8%)</td>
<td>2.5k</td>
</tr>
<tr>
<td>UCSD-NT ⋂ AmpPot</td>
<td>18.4k / 447.6k (4.1%)</td>
<td>5.7k / 6.0M (3.3%)</td>
<td>0.8k</td>
</tr>
</tbody>
</table>

- Small percentages suggest noise, but:
  - Small attack intensities trigger BH (later)
  - We can observe BH only for a subset of ASes/targets
  - 2.5k ASes involved significant, but BH use might not be largely widespread

- Joint attacks (⋂) appear more likely to be BH’d
Blackholed attacks [2/2]

- Match blackholing events with preceding attacks

<table>
<thead>
<tr>
<th>source</th>
<th>#BH events</th>
<th>#BH’d prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSD-NT U AmpPot</td>
<td>363.0k / 1.3M (27.8%)</td>
<td>45.2k / 146.2k (30.9%)</td>
</tr>
</tbody>
</table>

- We match 27.8% with attacks
- Results do not allow us to infer the fraction of other types of attacks (e.g., direct and unspoofed)
- However, highlights that reflection and randomly spoofed DoS represents a significant share of DoS that operators had to deal with
Observation delay

\[ \begin{align*}
\text{active} & \quad \delta_a \\
\text{inactive} & \quad t_a \quad \delta_d \\
\text{realtime} & \quad \text{observation} \\
\text{time} & \quad t_d 
\end{align*} \]