Stemming the tide on DDoS: Protecting today’s critical businesses

Peter Brecl

October 2019
The digital business must maintain availability by detecting and deflecting malicious activity 24/7.
What is a DDoS Attack?
DDoS Attacks

DDoS attack type breakdown:

Of the top 100 attacks, the majority employed three or four vectors within a single attack:
- **89%** multivector
- **11%** single vector

The percentages represent the dominant vector in the attacks mitigated.

- **25%** DNS reflection
- **18%** ICMP flood
- **17%** SYN flood
- **12%** NTP reflection
- **9%** Chargen reflection
- **19%** Miscellaneous*

*HTTP, layer 7, UDP non-standard ports, etc.

CenturyLink global SOCs mitigated **14,000+** customer DDoS attacks during 1H19

DDoS attack size, duration and type – 1H19

- **Median attack size** = 4 Gbps
- **Average size of peak daily attack** = 25 Gbps
- **Largest attack seen** = 430 Gbps

- **Daily** = ~120
- **1H19** = ~14K
- **Median attack duration** = 44 Minutes
- **Average attack duration** = 1 Hour, 51 Minutes
- **Longest DDoS attack** = 9 Days, 4 Hours, 40 Minutes
The Impact of Denial of Service Attacks

Cost of attacks outweigh investments in security controls and threat intelligence.

- Understand the impact of down time to your organization
- Develop the on-line presence strategy as a part of the disaster recovery plan
- Use pricing model that best matches your risk tolerance
DDoS Mitigation Provider Options

- Cloud-based DDoS mitigation
- Facilities based and Clean-pipes solutions
- CDN-based DDoS mitigation
- IaaS-based DDoS mitigation
Selecting the DDoS Mitigation Service

Options to Consider

• **Assets protected**
  - Web site
  - Data center
  - Corporate offices
  - Public or private cloud environment

• **Type of mitigation**
  - Always-on
  - On-demand

• **Methods of clean traffic return delivery**
  - Over the top
  - Integrated with the internet circuit
  - Via private connectivity

• **Attack monitoring**
  - Provider-monitored
  - Customer-monitored

• **Mitigation control**
  - Customer-initiated
  - Automated
  - SOC-assisted
Layered Approach for Mitigation of Large-scale DDoS Attacks
Internet Backbone as a Layer of Defense

BGP Flowspec Capability

- Uses BGP Flowspec announcements for an automated ACL rules delivery to Flowspec capable routers across the backbone and edges

- Highly scalable global solution

- Facilitates emergency mitigation.

- **Key Benefit:** Rapid deployment of rules globally
  - Provides an additional layer of mitigation against large scale volumetric layers 3 and 4 attacks
Tiered Scrubbing Architecture

• Super Scrubbing Centers
  • Handle super large attacks
  • Close to major Internet traffic peering points

• Regional Scrubbing Centers
  • Deal with larger attacks originating within the regions

• Many Local Scrubbing Centers
  • Minimize the latency
  • Reduce collateral impact
  • Escalated to Super or Regional centers when thresholds exceeded
Permanent Rules on the Network Edge

- **Facilities based Internet services providers**, have the ability to add permanent network defense rules on the provider edge routers.
- Basic layer in a multi-layered approach to DDoS mitigation. It helps reduce the attack surface.
- Complements traditional DDoS mitigation service

Key Attributes

- Always-on security control
- Layers 3-4 volumetric attack mitigation
- IPv4 or IPv6 filters, rate limiters, null routes and permanent ACLs
- Additional ACLs on upstream internet backbone routers
- Flow-based monitoring for advanced reporting
Hybrid Deployment Models

- Customer deploys on-premises DDoS mitigation appliance
- Customer controls and manages the certificates on the appliance for encrypted traffic mitigation
- Customer utilizes network-based DDoS mitigation service
- DDoS mitigation appliance signals the network-based DDoS when needing help with volumetric attacks
- Security Operations Center or automated controls engage the volumetric attack mitigation using the scrubbing centers.
Creating a safer internet through global visibility

We track ~1.2M threats per day for a comprehensive understanding of the global threat landscape.

We feed over 139B NetFlow sessions into our machine learning models daily.

We keep tabs on bad actors, actively monitoring ~18,000 C2s per day.

We act on what we see, identifying 680+ & removing ~63 new C2s per month.

We respond to and mitigate ~120 DDoS attacks per day.

We collect ~771M DNS queries per day for continuous learning.
DDoS Command & Control (C2) and Bot Discovery

- Use network as a sensor to identify C2 traffic
- Categorize the botnet
- Validate the C2
- Reverse trace the compromised bot’s communication with the validated C2
DDoS C2 Takedown

• Utilize the C2 information discovered from the network

• Disrupt communication between the C2 and compromised machines

• Track and disrupt communication of reemerging or backup C2 controls trying to regain control of the bots

• CenturyLink tracks over 18,000 botnets and takes down ~63 per month
Hunting and disrupting threats.

@BlackLotusLabs  www.centurylink.com/BlackLotusLabs
Mass Malware

Breakdown of validated C2s by family - 1H19.

<table>
<thead>
<tr>
<th>Family</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirai</td>
<td>1,438</td>
</tr>
<tr>
<td>Emotet</td>
<td>1,394</td>
</tr>
<tr>
<td>Gafgyt</td>
<td>1,240</td>
</tr>
<tr>
<td>Xor/DDoS</td>
<td>39</td>
</tr>
<tr>
<td>Necurs</td>
<td>9</td>
</tr>
</tbody>
</table>

Black Lotus Labs IoT malware family visibility — 1H19

<table>
<thead>
<tr>
<th></th>
<th>Gafgyt</th>
<th>Mirai</th>
<th>Xor/DDoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique C2s tracked</td>
<td>676</td>
<td>989</td>
<td>20</td>
</tr>
<tr>
<td>Unique victims targeted</td>
<td>61,911</td>
<td>88,114</td>
<td>9,575</td>
</tr>
<tr>
<td>Average uptime (days)</td>
<td>12</td>
<td>14</td>
<td>32</td>
</tr>
</tbody>
</table>