Part 2 – Defending Against a Live DDoS Attack

Evan Uhl, CISSP CRISC CISA GSEC
Security Operations Center Manager, Neustar, Inc.
Defenses and Techniques
Current Defenses

Organizations maintain a line of defense behind traditional infrastructural components, however adoption of DDoS appliances, services, and hybrids models continue to rise. Hybrid is up from 18% over 2014 and reflects ongoing evolution to deal with continuous DDoS threats.
Countermeasure Examples: (L3-L7)

L3-L4
- Invalid packets
- Fragment Flood Detection
- Multicast Blocking
- Private Address Blocking
- ICMP Flood Detection
- Filter List
- Payload Regular Expression
- Rate-based Blocking
- TCP SYN Flood Detection
- TCP Connection Limiting/Reset
- Traffic Shaping

Web servers - HTTP
- Malformed HTTP Filtering
- Application Misbehavior
- HTTP Rate Limiting
- Botnet Prevention
- Includes AIF signatures
- Payload Regular Expression
- Spoofed SYN Flood Prevention
- HTTP Authentication option
- HTTP Header Regular Expression

DNS Servers
- DNS Authentication
- Malformed DNS Traffic
- DNS Rate Limiting
- DNS NXDomain Rate Limiting
- DNS Regular Expression

SIP Servers
- SIP Malformed
- SIP Request Rate Limiting

SSL Secured Services
- TLS Attack Prevention
Effective Configurations and Techniques

- DNS Redirect
- BGP Redirect
- CDN
- Hybrid
- Always-on Hybrid
SOC Alignment – Tiered Responsibilities

- Call Receipt and Routing
- Device Health Monitoring
- Event Validation
- Ticket Creation & Escalation
- Application restarts
- Complete Event Analysis
- Routine CM work (turn-ups)
- Vendor Escalation
- Customer reporting
- Initial Event Analysis & Response
- Device Management/Fault Isolation
- SOC Mentorship
- Emerging Threat Research
- Solution Design/Engineering
- Automation/Optimization
- Complex CM work (turn-ups)
- SOC Training
- Client Engagements

NOC Analyst

SOC Engineer

Sr. SOC Engineer
Mitigating the Attacks of Today and Tomorrow

- Predictive Threat Analysis
- Attack Drills
- Alert Thresholds
- Proactive Monitoring
Inside the Attacker’s Studio: The DDoS Attack

What you see during a DDoS attack

The page cannot be displayed

The page you are looking for is currently unavailable. The website might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
  1. Click the Tools menu, and then click Internet Options.
  2. On the Connections tab, click LAN Settings.
  3. Select Automatically detect settings, and then click OK.
- Some sites require 128-bit connection security. Click the Help menu and then click About Internet Explorer to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your...
What We See During a DDoS Attack

```
32.0.4.147.32770 > 46.37.170.2.53: 6816 A? www.maybe.net. (31)
32.0.3.208.32770 > 46.37.170.2.53: 6817 A? www.maybe.net. (31)
112.0.0.52.34129 > 46.37.170.2.53: 28421 A? id10t.com. (27)
112.0.0.35.34129 > 46.37.170.2.53: 28422 A? id10t.com. (27)
112.0.0.52.34130 > 46.37.170.2.53: 28423 A? redskins.suck.com. (35)
32.0.3.234.32770 > 46.37.170.2.53: 6818 A? www.maybe.net. (31)
```
We Look Closer and See More
Getting you back to your regularly scheduled web surfing – Mitigation Starts
Perform Deep Packet Inspection Techniques to Identify Attack Vectors
Implement Countermeasures to Drop Malicious Attack Vectors

```
Payload regular expression countermeasure set to:
"jklijklldfjkl\d91\jify9if|fakljsf\fkdlsdf.com|dfsdfsdfsdfjkljklklsdf|\x05\x69|\x64|\x31|\x30
\x74|\x03|\x63|\x6f|\x6d|\x00",
euhf on Wed Jan 8 11:39:42
```

---

```
Payload regular expression TCP Ports
Example: '25'
80

Payload regular expression UDP Ports
Example: '25'

Payload regular expressions are case-sensitive by default. To perform case-insensitive matching, preface the expression with "(?!)?"

Payload Regular Expression
Example: \"xff\xff\x00\x01\" for hex values, (uses a PCRE format)
```

---

```
Apply Regular Expression to Packet Headers
Action: Drop matched traffic
```
DDoS Mitigation Simulation
Weekly DDoS Attack Simulation

- Performed in a dedicated LAB environment
- Artifacts captured and audited as part of SSAE16
- Includes replaying of real production attacks seen in the wild
- Involves all stakeholders in a DDoS attack (not just SOC)
- Formal debrief held to discuss performance in the spirit of continuous improvement and skill development
Where there is one attack vector there is another…and another…and another…
Modify Countermeasures to Drop Additional Attack Vectors
But Wait…There’s More
Today’s DDoS Attack was brought to you by:
Working with A Service Provider

Embed the Service Provider Methods and Procedures into your operations
On-Demand DNS Redirect

Technical:
- Bi-directional traffic
- Source IP → XFF header
- SSL options
- Initiate with DNS change

Legitimate Users

Internet

156.33.10.104

Scrubbing Centers

Clean
Clean
Clean
Clean

The Security Operations Center (SOC) Manages mitigation

DNS Change
www.example.com 300 IN A 202.160.2.4
www.example.com 300 IN A 156.33.10.104

=Optional= Access Control List (ACL)
Whitelist IP Address ranges with upstream ISP

Cloud Failover
- Customer changes DNS record
- Enter IP in A record
- Cloud failover commences when DNS changes propagate, TTL expiration
- Scrubbing centers pass clean traffic to host
- Bi-directional traffic flow

The IP Address
Scrubbing Centers

www.example.com 202.160.2.4
On-Demand BGP Redirect

Technical:
- Inbound traffic only
- Source IP maintained
- No SSL option
- Must route to single destination per /24
- Requires /30 outside /24
CDN Flow Schematic

Cloud Failover
- Customer changes DNS record for Origin Server
- Enter IP in A record
- Cloud failover commences when DNS change propagates, TTL expiration
- Scrubbing centers pass clean traffic to Origin Server
- Bidirectional traffic flow

DNS Change

<table>
<thead>
<tr>
<th>Domain</th>
<th>Class</th>
<th>Type</th>
<th>TTL</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>IN</td>
<td>A</td>
<td>300</td>
<td>156.33.10.104</td>
</tr>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>IN</td>
<td>A</td>
<td>300</td>
<td>256.12.244.18</td>
</tr>
</tbody>
</table>

Security Operations Center (SOC)
- Manages mitigation
Always-On Hybrid DNS Redirect

- Scrubbing Centers
  - SNG
  - SJC
  - ASH
  - AMS

- Customer Router
- Ethernet Switch
- Neustar Security Operations Center (SOC)

- ISP 1
- ISP 2

- Network
- Internet

- Protection Groups

- Clean Traffic
- DNS change Neustar IP
- -Clean-Traffic
- -Legitimate-Traffic
- -Clean-Traffic
- -Legitimate-Traffic
- -Botnet

- Cloud Signal
- Security Operations Center (SOC)
Always-On Hybrid /24 BGP Redirect

- Internet
- Legitimate users
- Botnet
- Cloud Signal
- Security Operations Center (SOC)
- Neustar Scrubbing Centers
- /24 Prefix Announcement
- Ethernet Switch
- Protection Groups
- GRE endpoint
- DDoS Appliance
- Neustar Pravail APS
- Arbor packet capture
- MNGT0
- OOBM
- MNGT1
- ISP 1
- ISP 2
- Customer Router
- EXT0
- EXT1
- INT0
- INT1
- MNGT0
- SNG
- SJC
- ASH
- AMS
- Ethernet Switch
- GRE
- GRE
Case Studies
Law Enforcement Agency Attack

- Escalating attack on four customer hostnames with 12 distinct waves over a period of 11 days
- Required a combination of mitigation strategies and constant vigilance.
- Attack size averaged 2Gbps & 700Kpps across global nodes
Digital Media Attack

- Attack size reached 140Gbps / 13Mpps with wide distribution of sources – requiring versatile mitigation responses.
- DNS amplification is a weapon of choice
Questions?