(D)OS DEMYSTIFIED

Tim Wagner – Security Specialist
Wes Stephens - Account Manager
Definitions

• **DOS Attack** - a perpetrator uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests—usually in an attempt to exhaust server resources (e.g., RAM and CPU). The goal is to make the resource unavailable. (Script based usually)

• **DDOS Attack** - launched from multiple connected devices that are distributed across the Internet. These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved. Unlike single-source DoS attacks, DDoS assaults tend to target the network infrastructure in an attempt to saturate it with huge volumes of traffic. (Botnet based usually)

• **Hybrid Protection** - The ability to use both on premises and off premises mechanisms to defend against a DOS and/or a DDOS attack
DD4BC claims ~400 Gbps

Extortion demands of 1-40 Bitcoin

Initially targeted Bitcoin, Payment providers, banks and now moving to other targets

UDP Amplification Attacks (NTP, SSDP, DNS); TCP SYN Floods; and Layer 7 attacks

April - May of 2015: emails sent to legitimate businesses with the threat of massive DDoS attacks

Sample from actual email:

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother. At least, don't expect cheap services like CloudFlare or Incapsula to help...but you can try. :(
Figure 2-2: The 10 most popular attack vectors have remained consistent since Q1 2015, with the exception of TCP Anomaly attacks, which first edged out ICMP attacks in Q4 2015.

Figure 2-1: Four of the 25 DDoS attack vectors tracked this quarter—UDP Fragment, DNS, NTP, and CHARGEN—comprised nearly 70% of the attacks.
The Hybrid Threat

Carphone Warehouse Breach with a DDOS Smoke Screen:
http://www.theregister.co.uk/2015/08/11/carphone_warehouse_ddos_before_giant_data_breach/

CyberCriminals Use DDOS to hide attacks:
Attack Size Realities

<table>
<thead>
<tr>
<th>Attack Size</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>500-999Mbps</td>
<td>1-10Gbps</td>
</tr>
<tr>
<td>Over 50Gbps</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

100+ Gbps Attacks 2016 YTD

- January: 100
- February: 130
- March: 240
- April: 1,000
- May: 1,000
- June: 2,675
- July: 2,050
- August: 2,675
- September: 401
- October: 448

Pie chart showing the distribution of attack sizes.

Legend:
- 500-999Mbps
- 1-10Gbps
- 10-50Gbps
- Over 50Gbps
- Unknown
448 Gbps Attack Breakdown

<table>
<thead>
<tr>
<th>Bandwidth (Gbps)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center 1</td>
<td>130.4</td>
</tr>
<tr>
<td>Data Center 2</td>
<td>154.3</td>
</tr>
<tr>
<td>Data Center 3</td>
<td>82.2</td>
</tr>
<tr>
<td>Data Center 4</td>
<td>80.8</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>447.7</strong></td>
</tr>
</tbody>
</table>
Denial of Service Solution Options
Current Volumetric DDoS Solution Market

Carriers Based
Generally they leverage thresholds and only work on the link that you purchase from the carrier
Example: Verizon/ATT

CDN Based
CDN technology is about absorbing and masking the effects of a DDOS attack, not removing it
Example: Akamai/Cloudflare

Enterprise Cloud Service
Generally based on 4-7 Scrubbing facilities, geographically dispersed, removes bad traffic and is priced on clean bandwidth
Example: F5 Silverline/Prolexic
Current Hybrid Options

Carriers Based
Generally they do not offer any on premises option to customers.

CDN Based
Generally no on premises option is offered to customers.

Enterprise Cloud Service
Certain solutions in this group do offer hybrid offerings. While not common, 3 vendors in this space offer something, implementation is the differentiator.
Important Decision Criteria

- Scale per Customer:
  - Limited Toolsets/Only DOS

- Hybrid Option:
  - False Positives

- Solution Side Effects:
  - Visibility into Attacks
24/7 SUPPORT
Ask your vendors where they have SOC locations, what layers of engineering support? Separate provisioning? Response time matters, make sure you understand this level of support. Is there more then one location?

GLOBAL COVERAGE
Where do you scrub traffic?
Explain how AnyCast works, if that is used
How is backend or private connectivity configured between centers
Replication time?

INDUSTRY-LEADING CAPACITY
- Scrubbing Capacity- Physical gear to clean traffic, this is the key!
- Bandwidth- Today and how does it change when you sign up customers
Physical Internet Cabling
Volumetric DDoS Protection - Service Options

Always on
Primary protection as the first line of defense
The Always On service stops bad traffic from ever reaching your network by continuously processing all traffic through the cloud-scrubbing service and returning only legitimate traffic through your website.

Always available
Primary protection available on-demand
The Always Available service runs on standby and can be initiated when under a DDoS attack.
Single Tier DDoS mitigation for all attacks

- Sits in front of the Firewall for L3/4 Protection
- Deploy inline or out of band?
- Does it do Layer 7 as well?
- Signaling to of premises solution
Two tier DDoS Protections

- Basic Layer 3/4 deployment inline in front of Firewall to protect against volumetric DDoS attacks
- Layer 7 DDoS mitigation on the inside tier. Requires SSL termination on the DDoS appliance
Two Ways to Direct Traffic to Silverline Scrubbing Centers

- BGP (BORDER GATEWAY PROTOCOL) ROUTED MODE
- DNS PROXY MODE

Multiple Ways to Return Clean Traffic

- GRE TUNNELS
- L2VPN / VIRTUAL ETHERNET SERVICE
- IP REFLECTION™
- EQUINIX CLOUD EXCHANGE
- PROXY
Data Center
TCP Connection: SYN
SRC: 86.75.30.9:27182
DST: 1.2.3.4:80

86.75.30.9
F5 Silverline DDoS Protection
DDoS Protection

ISP Router
Customer/ISP Transit Network
Network
F5 Router
Internet

69.86.73.76
TCP Connection: SYN
SRC: 69.86.73.76:4243
DST: 1.2.3.4:80

Customer Router

1.2.3.4
Customer

BGP Configuration Change:
withdraw advertisement for 1.2.3.0/24

BGP Route Advertisement:
F5 route for 1.2.3.0/24 becomes preferred

TCP Connection: SYN-ACK
SRC: 1.2.3.4:80
DST: 86.75.30.9:27182

TCP Connection: SYN
SRC: 86.75.30.9:27182
DST: 1.2.3.4:80

TCP Connection:
SRC: 69.86.73.76:4243
DST: 1.2.3.4:80

Clean traffic is returned via GRE Tunnel to customer’s data center

Routed Configuration
DDoS Protection Engaged
Proxy Configuration
DDoS Protection Engaged

Data Center
DNS Query: www.abc.com
DNS Query: www.abc.com
DNS Query: www.abc.com
DNS Response: www.abc.com 5.6.7.8
DNS Response: www.abc.com 5.6.7.8
Local DNS
Public DNS Servers
DNS Configuration Change
#www.abc.com 1.2.3.4
www.abc.com 5.6.7.8
Authoritative DNS
TCP Connection:
SRC: 86.75.30.9:27182
DST: 5.6.7.8:80
86.75.30.9
TCP Connection:
SRC: 9.9.9.18:31415
DST: 1.2.3.4:80
9.9.9.0/24
NAT Pool
F5 Silverline
DDoS Protection
TCP Connection:
SRC: 69.86.73.76:4242
DST: 5.6.7.8:80
69.86.73.76
TCP Connection:
SRC: 69.86.73.76:4243
DST: 5.6.7.8:80
ISP Router
ACL
permit: 9.9.9.0/24 1.2.3.4/32
deny: any 1.2.3.4/32
Customer
Admin
1.2.3.4
Customer Router
ISP Router
Proxy Configuration
DDoS Protection Engaged
What does traffic flow look like in a Scrubbing Center?
F5 Scrubbing Center Architecture - Routed Traffic

- Inspection Tools provide input on attacks for Traffic Actioner & SOC
- Traffic Actioner injects routes and steers traffic
- Scrubbing Center aggregates attack data from all sources
- Portal provides near real-time reporting and configuration

**Data Plane**
- Switching mirrors traffic to Inspection Toolsets and Routing layer
- Ingress Router applies ACLs and filters traffic
- Cloud Firewall Rules
- Network Mitigation removes advanced L4 attacks
- Egress Routing returns good traffic back to customer

**Network Mitigation**
- GRE Tunnel
- IP Reflection
- L2VPN

**Cloud**
- Volumetric DDoS protection, Managed Application firewall service, zero-day threat mitigation with iRules

**Signaling**
- BGP signaling
- Visibility Management

**Flow Collection**
- Aggregates attack data from all sources

**Ingress Router**
- Applies ACLs and filters traffic

**Routing/ACL**
- Traffic Actioner

**Traffic Actioner**
- Injects routes and steers traffic

**Scrubbing Center**
- Inspection Plane

**Portals**
- Provides near real-time reporting and configuration

**CustomerId**
- Silverline DDoS Cloud

**Traffic**
- Legitimate Users
- DDoS Attackers
F5 Scrubbing Center Architecture - Routed + Proxy

- **Traffic Actioner** injects routes and steers traffic.
- **Flow collection** aggregates attack data from all sources.
- **Portal** provides near real-time reporting and configuration.

**Inspection Tools** provide input on attacks for Traffic Actioner & SOC.

- **Traffic Actioner** injects routes and steers traffic.
- **Flow collection** aggregates attack data from all sources.
- **Portal** provides near real-time reporting and configuration.

**Switching mirrors traffic to Inspection Toolsets and Routing layer**

- **Ingress Router** applies ACLs and filters traffic, deny all except for proxy listeners.
- **Cloud Firewall Rules**
- **Network Mitigation** removes advanced L4 attacks.
- **Proxy Mitigation** to Remove L7 Attacks, SNAT translation occurs.

Volumetric DDoS protection, Managed Application firewall service, zero-day threat mitigation with iRules.

- **Egress Routing**
- **Customer**

- **Ingress Router** applies ACLs and filters traffic, deny all except for proxy listeners.
Key Considerations

- DDOS is about economics, both for the attacker and the victim
- DOS or DDOS is not a hack, but rather an attack
- Is DDOS/DOS protection a market or a feature of broader solutions?
- DDOS protection needs to become “baked in” to bandwidth considerations
- SSL DDOS is not common today, but it is growing
- Protection levels depend on Risk assessment
- Is it as a Service or Managed Service, it does matter

Solutions for an application world.