Very Large-Scale Edge DDoS Protection

Sean Newman
Director Product Management
Is DDoS Still on the increase?

First Hacktivists: Zapatista National Liberation Army

Spammers discover botnets

Estonia: Parliament, banks, media, Estonia Reform Party

Coordinated US bank attacks: Grew to 200 Gbps, and continue today

500 Gbps Hong Kong attack
France swarmed after terror attack
PlayStation & Xbox hit at Christmas

Anon hits Church of Scientology

Spamhaus attack: Reported to reach 310 Gbps

Rio Olympics 540 Gbps

ProtonMail attack

Reaper Botnet
2M Devices

Mirai Botnet
OVH / Krebs / DYN
600 Gbps -> 1Tbps

Memcached
GitHub
1.35-1.7Tbps

2013
2005
2007
2009
2011
2013
2015
2016
2017
2018
2019
??

Anon hits Church of Scientology

Spammers discover botnets

Estonia: Parliament, banks, media, Estonia Reform Party

Coordinated US bank attacks: Grew to 200 Gbps, and continue today

500 Gbps Hong Kong attack
France swarmed after terror attack
PlayStation & Xbox hit at Christmas

Anon hits Church of Scientology

Spamhaus attack: Reported to reach 310 Gbps

Rio Olympics 540 Gbps

ProtonMail attack

Reaper Botnet
2M Devices

Mirai Botnet
OVH / Krebs / DYN
600 Gbps -> 1Tbps

Memcached
GitHub
1.35-1.7Tbps

2013
2005
2007
2009
2011
2013
2015
2016
2017
2018
2019
??

Anon hits Church of Scientology

Spammers discover botnets

Estonia: Parliament, banks, media, Estonia Reform Party

Coordinated US bank attacks: Grew to 200 Gbps, and continue today

500 Gbps Hong Kong attack
France swarmed after terror attack
PlayStation & Xbox hit at Christmas

Anon hits Church of Scientology

Spamhaus attack: Reported to reach 310 Gbps

Rio Olympics 540 Gbps

ProtonMail attack

Reaper Botnet
2M Devices

Mirai Botnet
OVH / Krebs / DYN
600 Gbps -> 1Tbps

Memcached
GitHub
1.35-1.7Tbps

2013
2005
2007
2009
2011
2013
2015
2016
2017
2018
2019
??
DDoS Evolution in 2018

- **High Bandwidth**
  - memcached exceeds 1Tbps, routinely > 100Gbps

- **Botnets**
  - Mirai (and its many known variants)
  - IoT (100s of Millions of easy to recruit devices)

- **Multivector**
  - 10+ vectors, Additive + Variation + Spray/Subnet

- **Boofter/Stresser Services**
  - the “10 minute” attack and pulsed attacks
Frequent DDoS Trend Continues...

Low-volume, short-duration attacks dominate!

- 40% Increase in Attacks compared to a year ago
- 7 Attacks per Customer per Day
- 77% Attacks 10 Minutes or Less
- 94% Attacks 5Gbps or Less

However...

- x2 Attacks over 10Gbps has doubled

DDoS attacks arriving from transit/peering

Good traffic destined for subscribers

ingress from transit/peering

egress to subscribers

DDoS victims

DDoS victims

Netflow Detect (out-of-band)

Service Provider
SP/Telco DDoS Scrubbing Redirect

DDoS attacks arriving from transit/peering

Good traffic destined for subscribers

Good traffic tunneled to edge or cust

BGP redirect

Netflow Detect (out-of-band)

note: Some Providers will have multiple scrubbing centers for Geos, redundancy, backhaul reasons.

Scrubbing Capacity (<10% edge capacity)

Good traffic destined for subscribers

ingress from transit/peering

Service Provider

Good traffic tunneled to edge or cust

Good traffic destined for subscribers

Good traffic tunneled to edge or cust
Large DDoS attack from transit/peering

Good traffic blocked by blackhole

ingress from transit/peering

BGP RTBH

Netflow Detect (out-of-band)

note: Some Providers will have multiple scrubbing centers for Geos, redundancy, backhaul reasons.

Scrubbing Capacity (50% edge capacity)

Customer offline for attack Duration

Customer offline for attack Duration

Service Provider

Customer to offline for attack Duration

Subscriber
Scrubbing Approach Increasingly Challenged

- **Provider Edge Capacity**: 100s of Gbps to multiple Terabits/sec
- **Provider RTBH Mitigation**: Manual instantiation of blackholes with target offline for duration of attack
- **Provider Scrubbing Capacity**: More attacks mitigated with Blackhole Scrubbing capacity needs to increase

The diagram illustrates the increasing challenge of scrubbing approaches due to the size of attacks and the need for partial protection (needs to be > 10%).
Scrubbing Redirect Challenges

DDoS Attacks Over Scrubbing Capacity Succeed!

Flow Monitoring
- Aggregation delay
- Attack overload
- Header only

Sampled Mirror
- Immediate forwarding
- Scales with attack
- Header and payload

BGP/RTBH/FlowSpec
- BGP propagation
- Header only
- Limited visibility

ACL Filters
- Rapid configuration
- Header and payload
- Streaming telemetry
New Opportunity for Edge Mitigation

- Monitor
- Inspect
- Detect
- Report / Signal
- Mitigate

**NOC/SOC**
- Sampled Mirror (tuple + payload)
- Filter Generation (tuple + payload)

**Network Edge**
- Sampled Mirror (1:N)
- Streaming Telemetry
- Ingress Traffic
- Egress Traffic
- Dynamic Filter (tuple + payload)

**Detection**

**Mitigation**
Full Edge Capacity Mitigation

Provider Edge Capacity
100s of Gbps to multiple Terabits/sec
<1% of attacks need to be blackholed

Provider Edge Mitigation
Leverage real-time data and analytics
to deliver intelligent automation

Provider Scrubbing Capacity
>90% attacks mitigated at Provider Edge
<10% redirected to scrubbing

Blackhole Zone
<1% of attacks need to be blackholed

Provider Edge Mitigation Zone

Scrubbing Zone
>90% attacks mitigated at Provider Edge
<10% redirected to scrubbing

Number of Attacks

100% Edge Protection

Scales to Tens of Terabits of DDoS Protection
Provider Edge DDoS Protection

DDoS Attacks arriving from transit/peering

Internet

ingress from transit/peering

Service Provider

NETCONF

Good traffic to edge or customer

Good traffic to edge or customer
Example Edge Filtering with Juniper MX

• Matching Firewall-type rules with defined actions:

```plaintext
firewall {
  family inet {
    filter CORERO-MITIGATE {
      term b8b244d6c04e4ee11e79416cd9f426af {
        from {
          destination-address {
            172.27.33.0/24;
          }
          protocol udp;
          source-port 19;
        }
        then {
          count Corero-b8b244d6c04e4ee11e79416cd9f426af;
          port-mirror;
          discard;
        }
      }
    }
  }
}
```
Summary

• DDoS as a whole still on the Increase
  – Attack Methods/Vectors more Sophisticated
  – Emerging trend for increase in proportion of larger attacks

• Traditional Scrubbing/RTBH Protection is inadequate
  – Typically too slow to react to avoid damage, or completes attack
  – Wastes core network bandwidth backhauling junk DDoS traffic

• New Opportunity for Protection on Network Edge Devices
  – Leverage built-in power of latest infrastructure devices
  – No need to insert new devices at every ingress point
  – Deliver always-on protection at edge capacity up to unprecedented scale
  – Can operate as an overlay to existing scrubbing centers
  – Deploy filters automatically from DDoS protection solution
Questions?
Thank You!