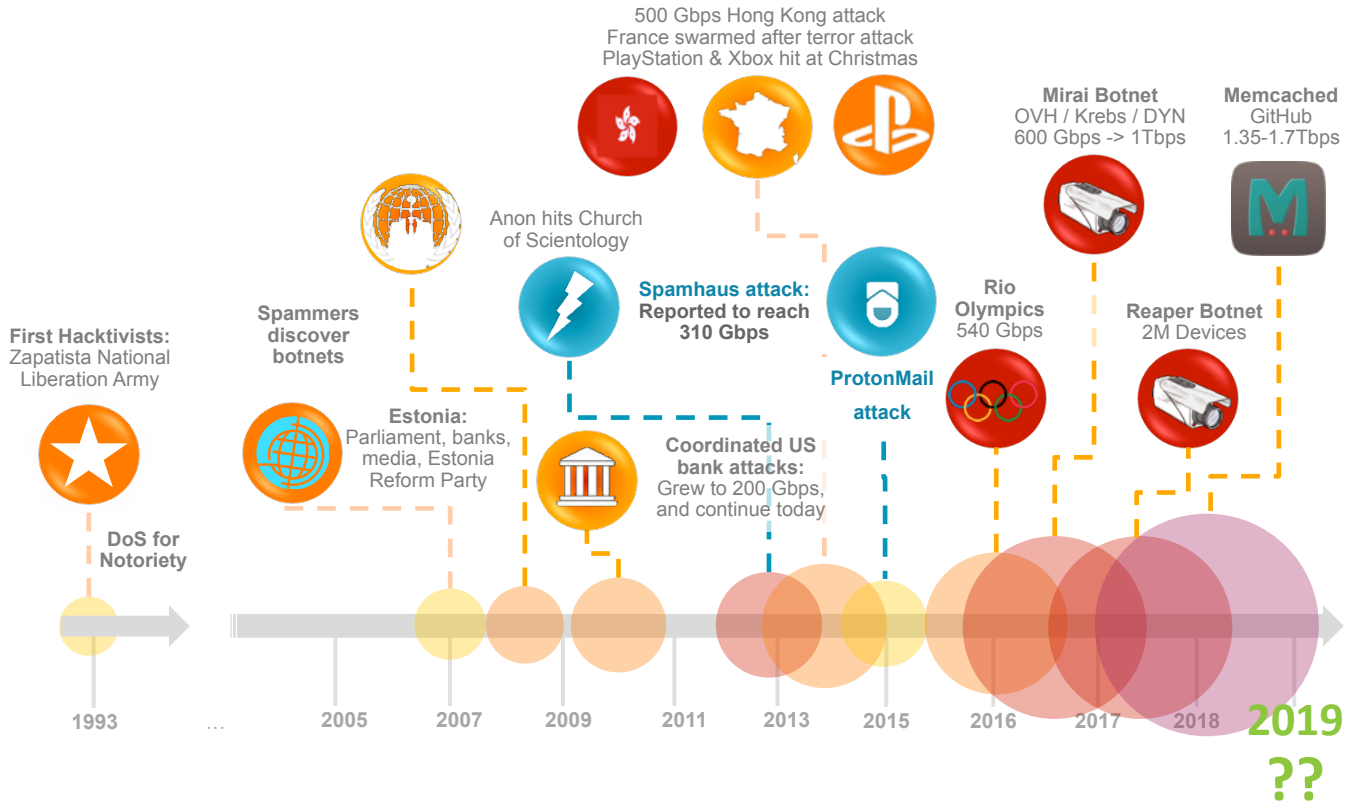
corero telent

Very Large-Scale Edge DDoS Protection

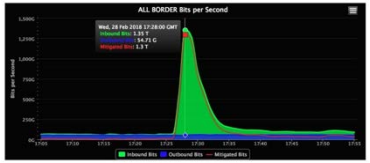
Sean Newman
Director Product Management

Is DDoS Still on the increase?

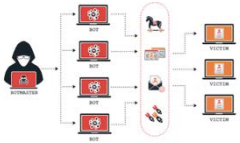


DDoS Evolution in 2018

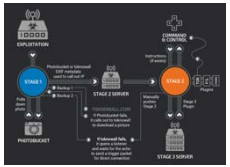
- **High Bandwidth**
  - memcached exceeds 1Tbps, routinely > 100Gbps



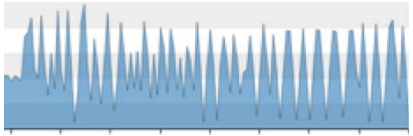
- **Botnets**
  - Mirai (and its many known variants)
  - IoT (100s of Millions of easy to recruit devices)



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



- **Booter/Stresser Services**
  - the “10 minute” attack and pulsed attacks



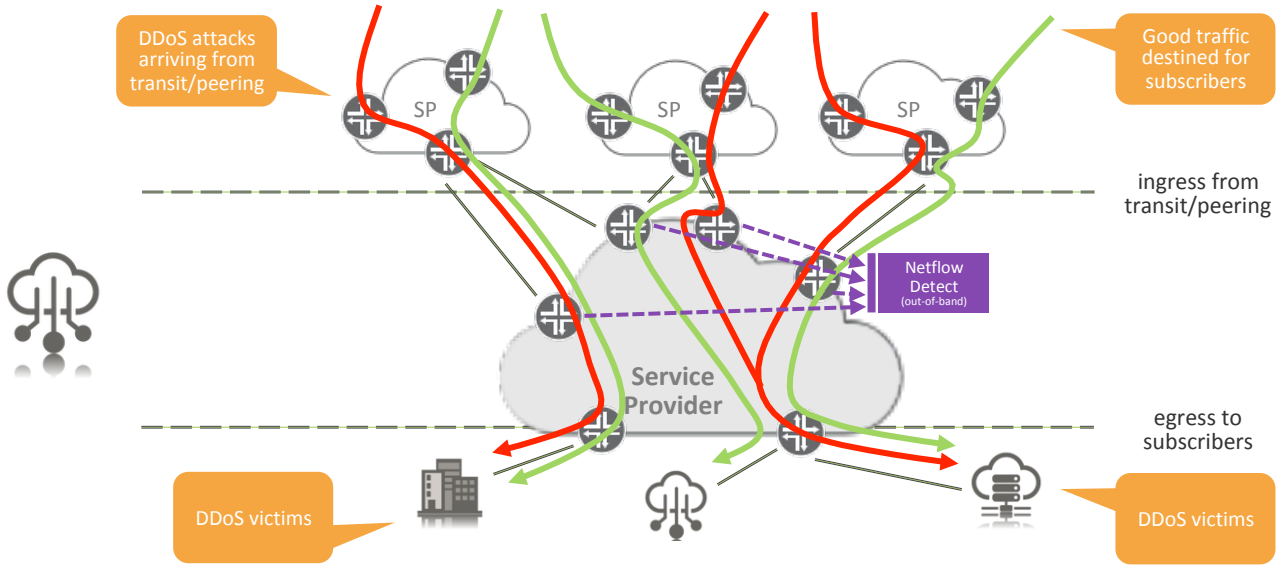
Frequent DDoS Trend Continues…

Low-volume, short-duration attacks dominate!

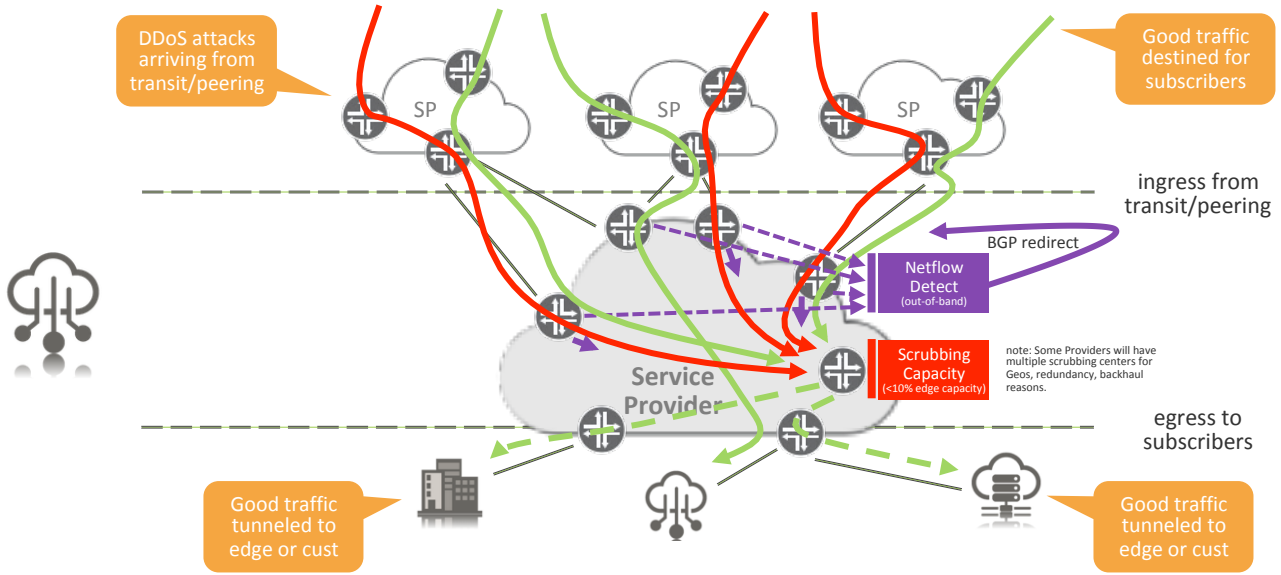
However…

Corero H1 2018 Trend Report: https://www.corero.com/resources/reports/h1-ddos-trends-report/

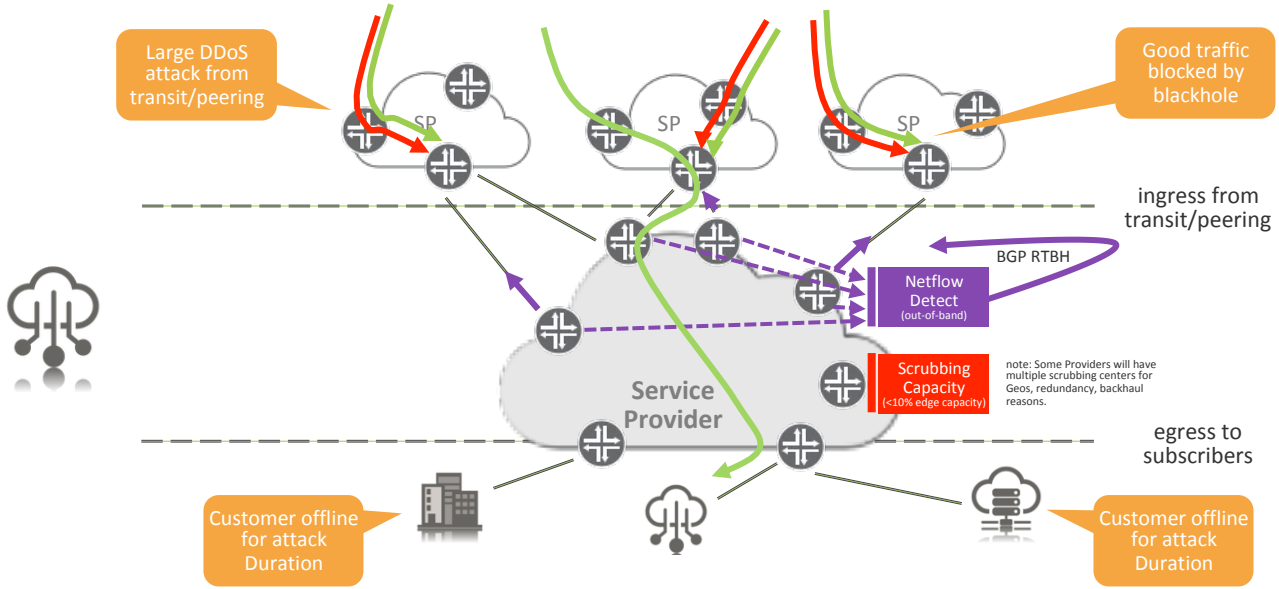
SP/Telco DDoS Scrubbing Protection



SP/Telco DDoS Scrubbing Redirect



SP/Telco Large DDoS Attack Blackhole



Scrubbing Approach Increasingly Challenged

Provider Edge Capacity

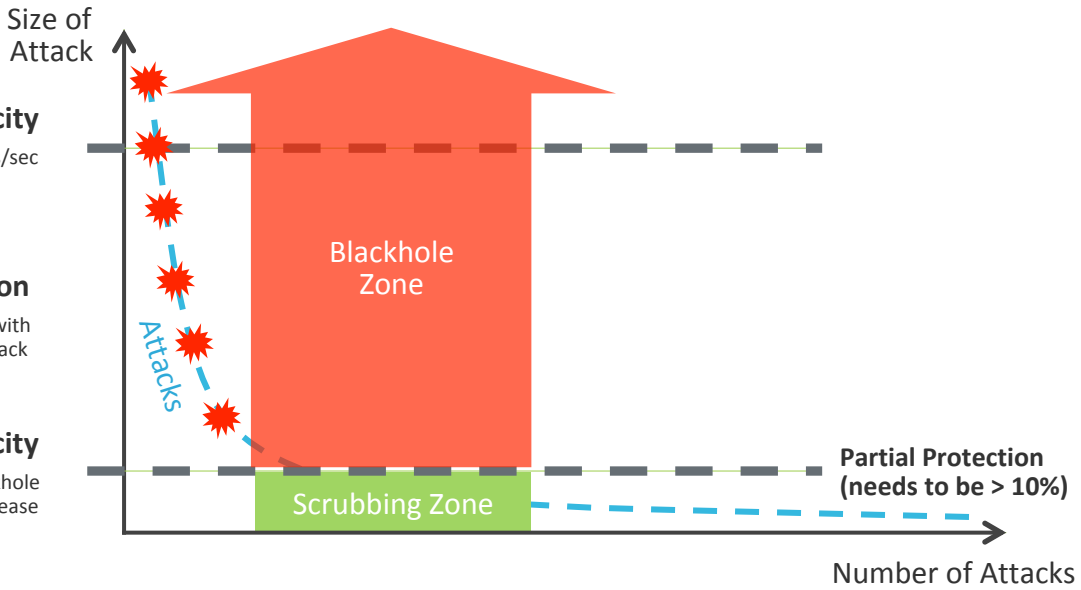
100s of Gbps to multiple Terabits/sec

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



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

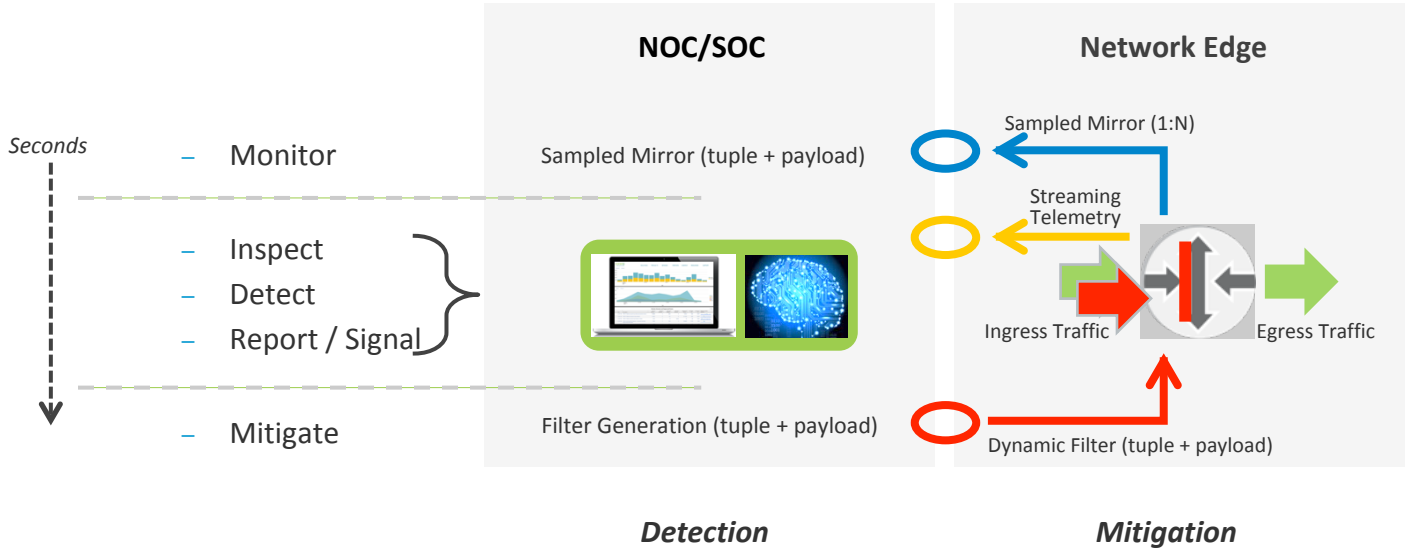
BGP/RTBH/FlowSpec

- BGP propagation
- Header only
- Limited visibility

ACL Filters

- Rapid configuration
- Header and payload
- Streaming telemetry

New Opportunity for Edge Mitigation



Full Edge Capacity Mitigation

Provider Edge Capacity

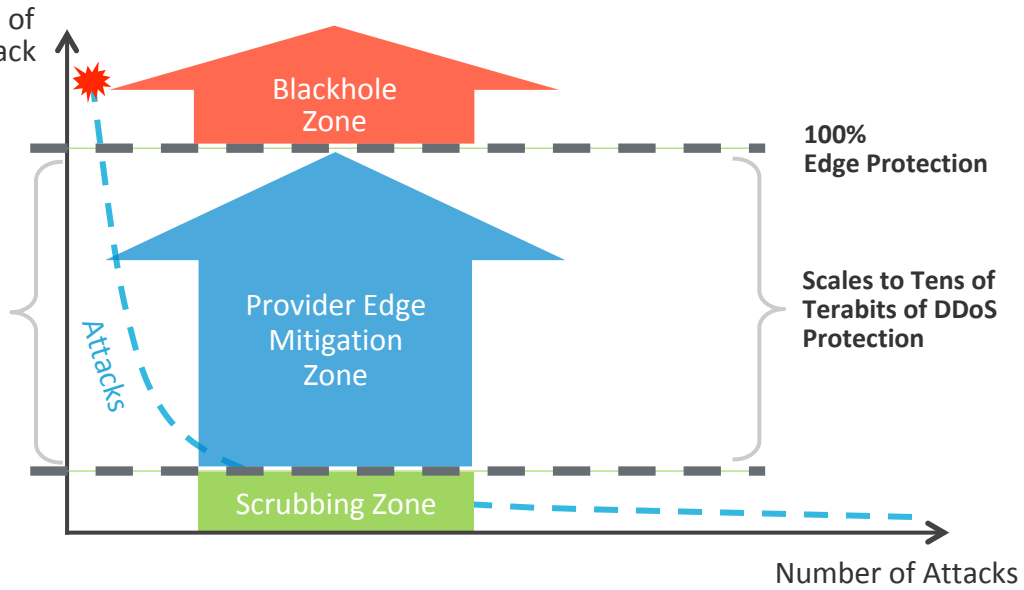
100s of Gbps to multiple Terabits/sec
<1% of attacks need to be blackholed

Provider Edge Mitigation

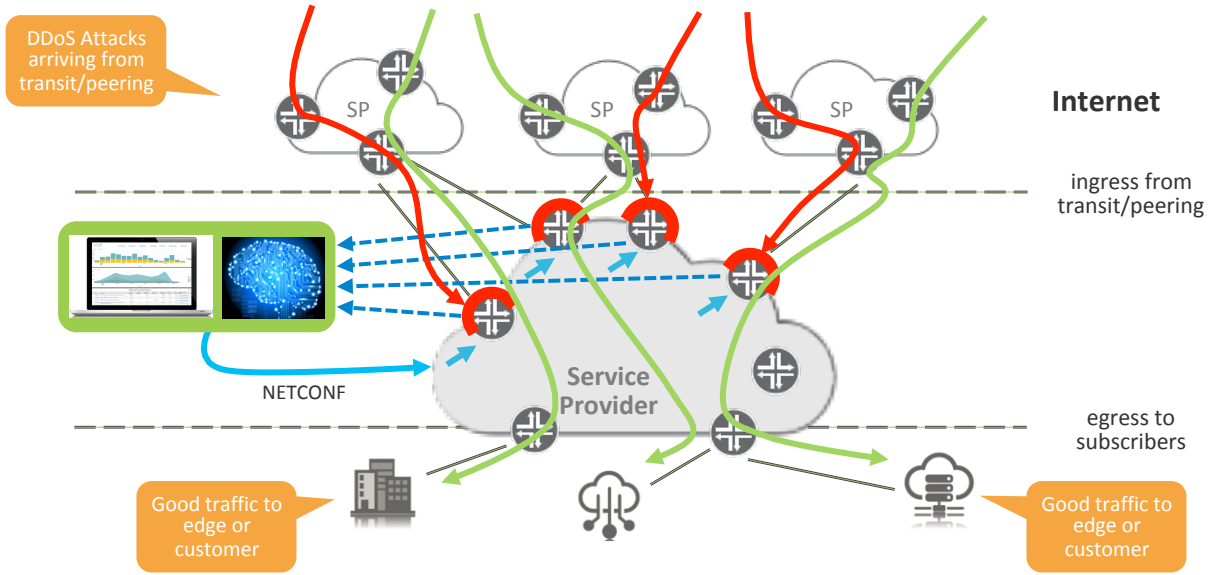
Leverage real-time data and analytics
to deliver intelligent automation

Provider Scrubbing Capacity

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



Provider Edge DDoS Protection



Example Edge Filtering with Juniper MX

- Matching Firewall-type rules with defined actions:

```
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?

corero

Thank You!