OARnet

An OH·TECH Consortium Member

DDoS Trends 2015

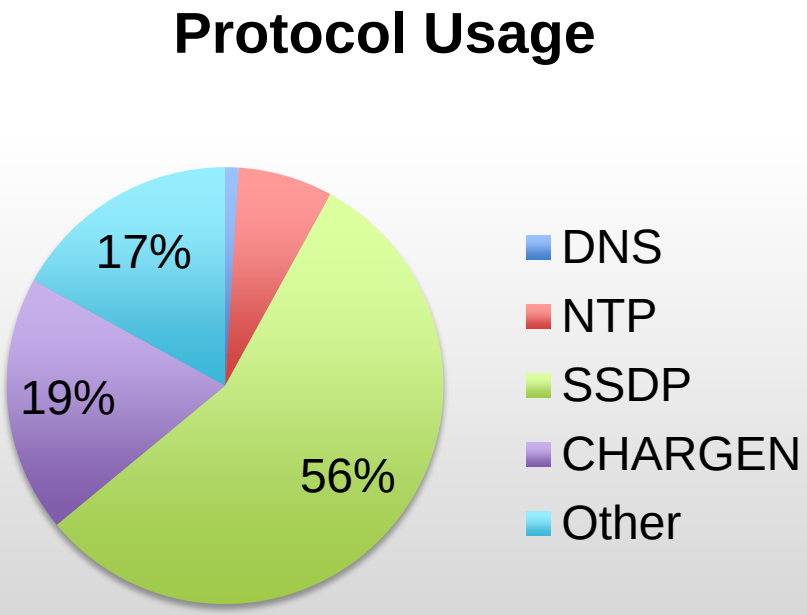
Kevin Nastase

OARsec

June 10, 2015

Attacks

- UDP Amplification
  - SSDP
  - NTP
  - DNS
  - CHARGEN
- TCP SYN Floods
- Combination of both



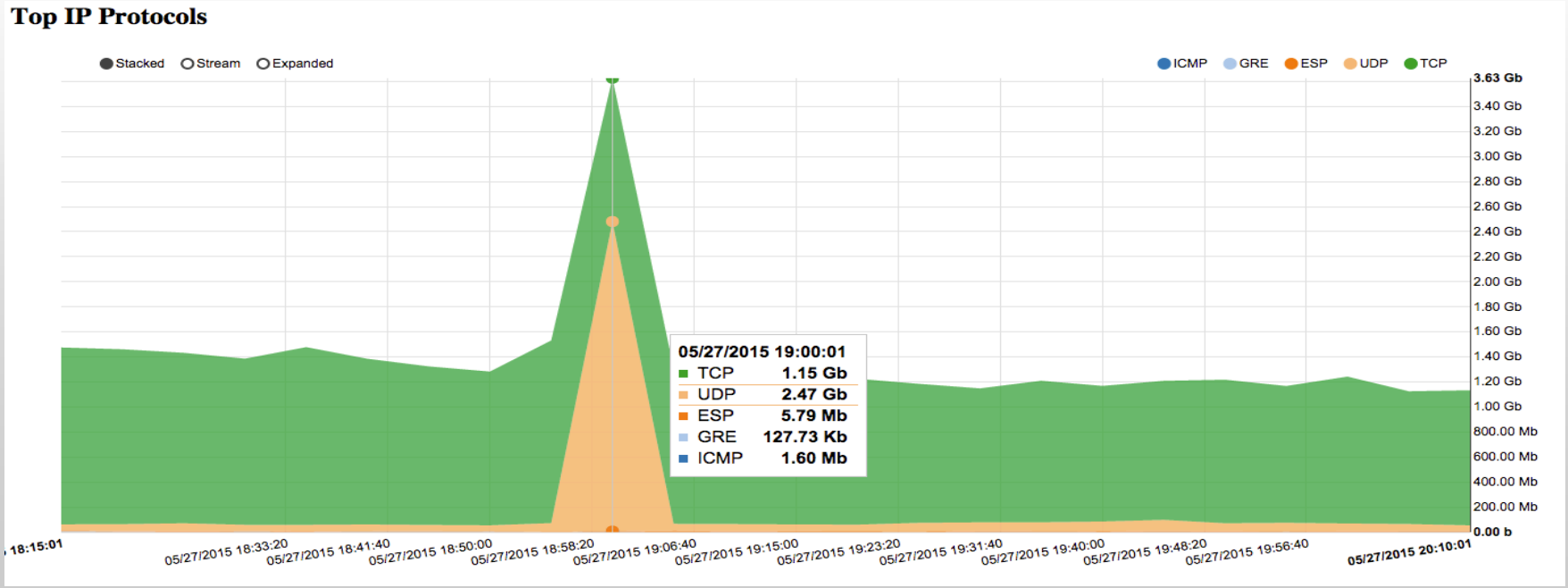
- Commodity Internet AND Internet2

Fun Facts

- Common Targeted Ports:
  - 0, 53, 123, 80, 443, 3074
- Largest Attack:
  - 7.9 Gbps (SSDP)
- Longest Attack:
  - 5 hours
- Top Source AS:
  - 4134 (ChinaNet)

Detection

- Netflow
  - Sampled



OARnet Mitigation Techniques

- IP filtered at customer edge (Black hole)
  - Discard all packets destined for IP
- Protocol/IP/Port discard or police
  - Granular packet filtering
- RTBH
  - Requires setup by both parties
  - Send host route with BGP community to activate

Questions

Kevin Nastase
Security / IdM Engineer, OARnet
knastase@oar.net

Like Us on Facebook: https://facebook.com/OARnet
Follow Us on Twitter: https://twitter.com/oarnet

1224 Kinnear Road
Columbus, OH 43212
Phone: (614) 292-9248