OARnet

An OH·TECH Consortium Member

DDoS Mitigation Strategies

Internet2 Security Working Group

23 Feb 2016

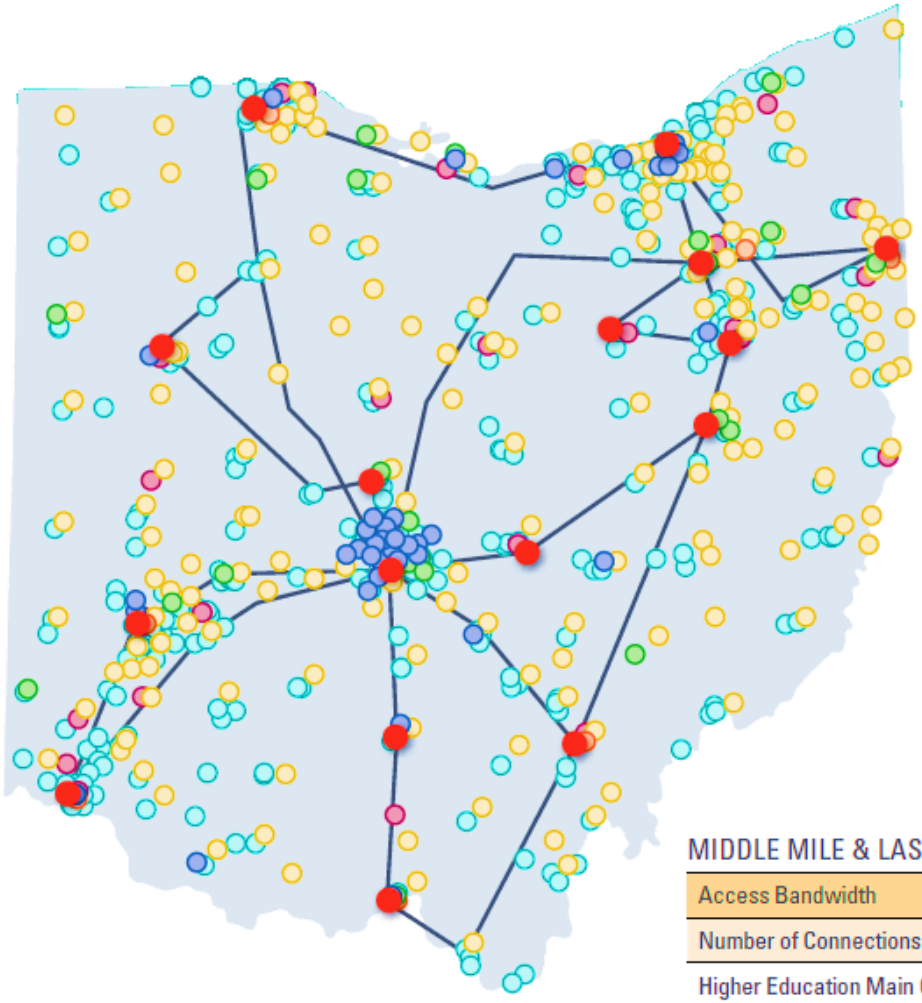
Mark Beadles
Information Security Officer
mbeadles@oar.net

Kevin Nastase
Network Security Engineer
knastase@oar.net

About OARnet

- Created in 1987 by Ohio Board of Regents
- A division of Ohio Department of Higher Education
- Serves Ohio's education, research, health care, public broadcasting and government communities

- 100Gb network backbone
- 2200+ miles of fiber in 6 rings
- 90 higher education clients
- 700 K-12 districts via 32 technology centers
- 750+ State government locations



LEGEND

- 90 Higher Education Institutions & 333 Higher Education Regional Branches & Sites
- 32 K–12 Education Centers (Connecting 700 School Districts)
- 33 Local Government Agenices
- 750+ State of Ohio Sites
- 52 Health Care Sites & Research Institutions
- 14 Broadcast Education Media Stations & Services
- OARnet Backbone PoP Locations
- OARnet Backbone

MIDDLE MILE & LAST MILE CONNECTIONS

Access Bandwidth				
Number of Connections	100 Gbps	40 Gbps	10 Gbps	1 Gbps
Higher Education Main Campuses	3	—	14	62
K–12, ITCs & Large Urbans	—	—	30	—
State	2	1	10	—
Research	2	—	—	3
Shared Gbps Service*	—	—	—	38

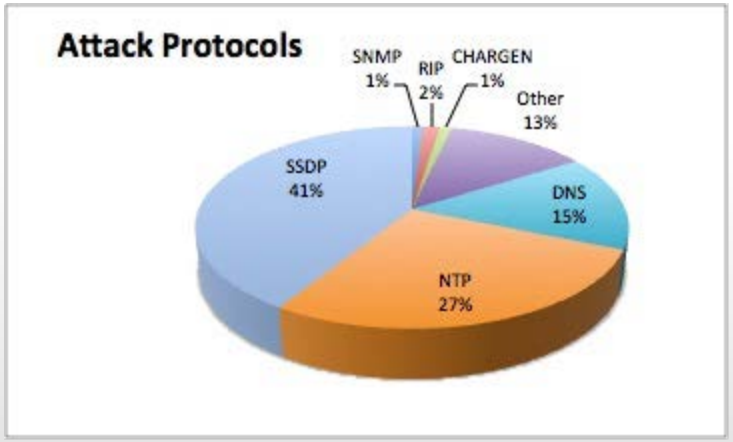
* Shared Gbps Services for Higher Ed, State & Local Governments

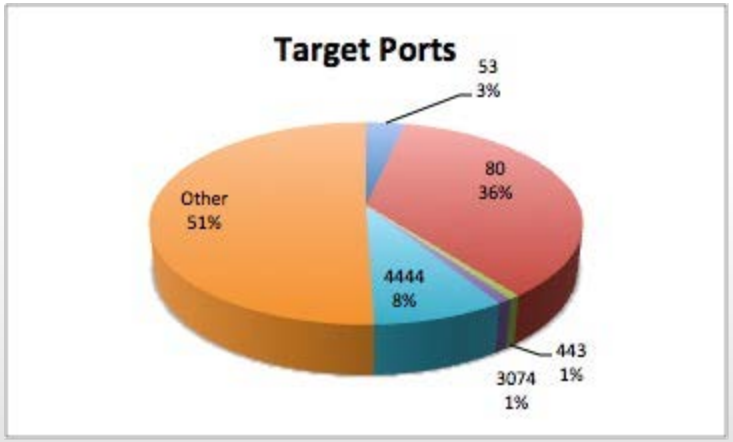
Denial of Service Background Statistics

- 3.6 events per day, 25.3 events per week, 110 events per average month
  - “event” here is an anomalous UDP flow
- 79 Unique clients have seen events
  - Targeted vs 267 different IP’s
- Average event size:
  - 2.454 Gb (1.686 Gb UDP, 0.761 Gb TCP)
- Largest event size:
  - 17.867 Gb (17.653 Gb UDP, .213 Gb TCP)

  - Data collected 3/15-2/16

Denial of Service Characteristics





1900/ssdp	41%
123/ntp	27%
53/dns	15%
520/rip	2%
161/snmp	1%
19/chargen	1%

80	36%
4444	8%
53	3%
443	1%
3074	1%

(also src prt 0)

Denial of Service Measures

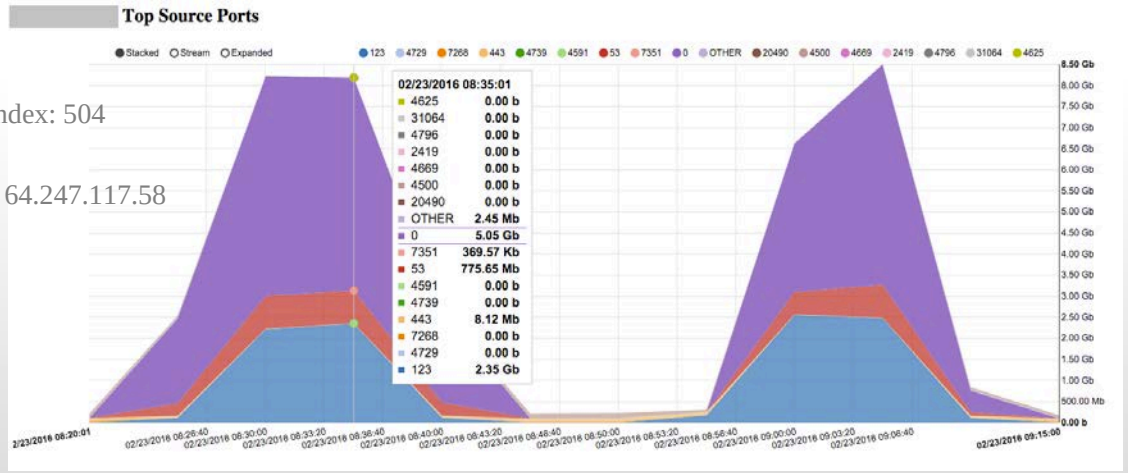
- Monitoring
  - Alerting
  - Visualization
  - Escalation
- Proactive
  - DNS
  - Targeted policing
- Reactive
  - RTBH
  - Hybrid DDoS Mitigation

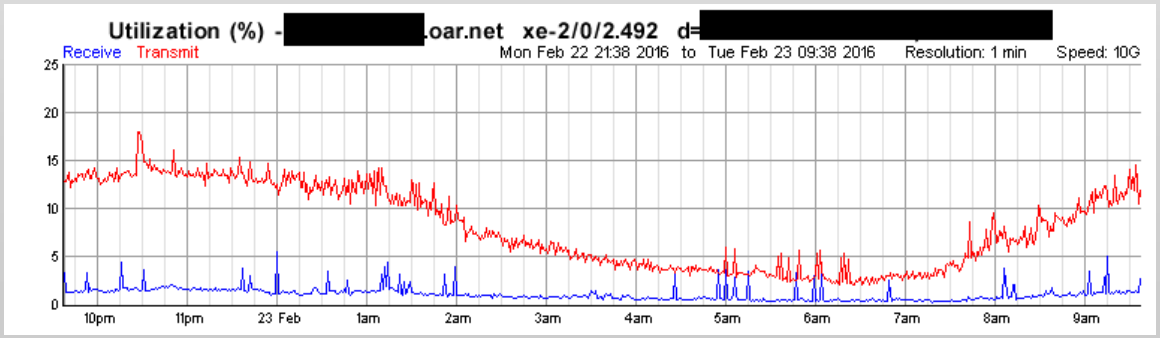
Denial of Service Measures: Alerting

Sample Alert

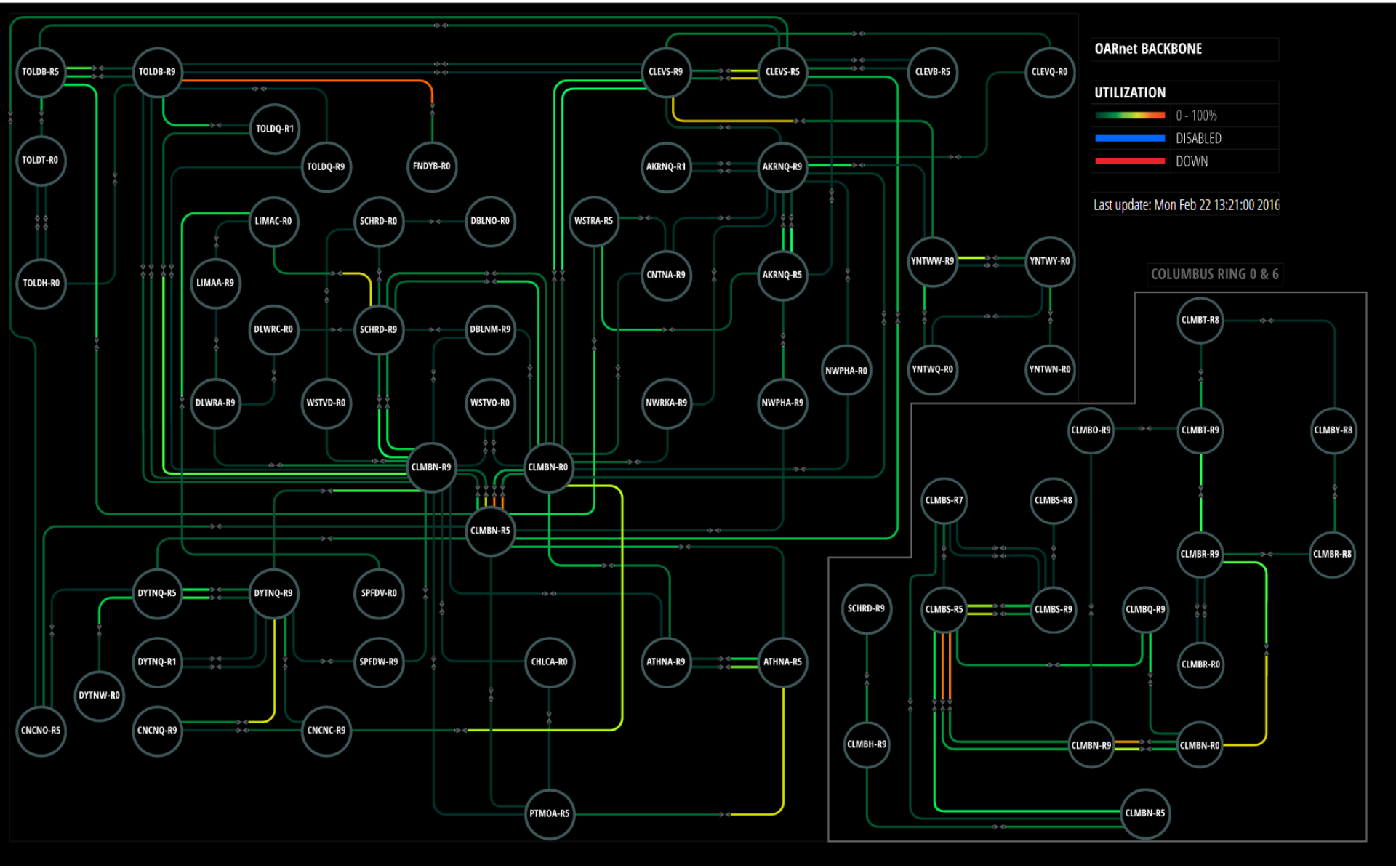
Suspected UDP (D)DoS Attack - Client: <redacted>
Service: INTERNET, Router: <redacted> - xe-1/0/0.395, ifIndex: 504
UDP: 16.15 Gbps, TCP: 424.44 Mbps, Total: 16.57 Gbps
UDP Src Port: 0 53, UDP Dest Port: 0 4444, Destination IP: 64.247.117.58

Statseeker Utilization Graph: <link>
Netflow Reports:
Top IP Protocols - <link>
Top UDP Source Ports- <link>
Top UDP Destination Ports - <link>



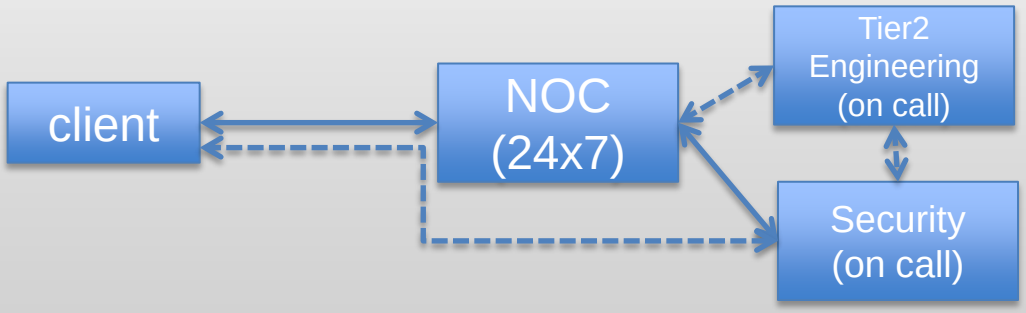


Denial of Service Measures: Visualization


OARnet BACKBONE
UTILIZATION
0 - 100%
DISABLED
DOWN
Last update: Mon Feb 22 13:21:00 2016
COLUMBUS RING 0 & 6
TOLDB-R5
TOLDB-R9
TOLDQ-R1
TOLDQ-R9
TOLDT-R0
TOLDH-R0
FNDYB-R0
LIMAC-R0
SCHRD-R0
DBLNO-R0
LIMAA-R9
DLWRC-R0
SCHRD-R9
DBLNM-R9
DLWRA-R9
WSTVD-R0
WSTVO-R0
CLMBN-R9
CLMBN-R0
CLMBN-R5
DYTNQ-R5
DYTNQ-R9
SPFDV-R0
DYTNQ-R1
SPFDW-R9
DYTNW-R0
CNCNO-R5
CNCNQ-R9
CNCNC-R9
CHLCA-R0
PTMOA-R5
CLEVS-R9
CLEVS-R5
CLEVB-R5
CLEVQ-R0
AKRNQ-R1
AKRNQ-R9
WSTRA-R5
CNTNA-R9
AKRNQ-R5
NWPHA-R0
NWRKA-R9
NWPHA-R9
ATHNA-R9
ATHNA-R5
YNTWW-R9
YNTWY-R0
YNTWQ-R0
YNTWN-R0
CLMBT-R8
CLMBO-R9
CLMBT-R9
CLMBY-R8
CLMBS-R7
CLMBS-R8
CLMBR-R9
CLMBR-R8
SCHRD-R9
CLMBS-R5
CLMBS-R9
CLMBQ-R9
CLMBR-R0
CLMBH-R9
CLMBN-R9
CLMBN-R0
CLMBN-R5

Denial of Service Measures: Escalation

- Plan your incident response and escalation paths ahead of time
- Both technical and business – DDoS is service affecting!
- Know who the right contacts are
- Practice & overcommunicate



Denial of Service Measures: DNS

- DNS is both a target and a source of DDoS activity

- OARnet DNS
  - 8 servers, 2 different OS's (secure64 + FreeBSD)
  - ½ recursive, ½ authoritative
  - Blind-master setup

Denial of Service Measures: Targeted Policing

- Large proportion of DDoS activity has a profile that lends itself to straightforward policing
  - UDP traffic in particular
  - E.g.: why does 1900/udp need to be sent over the Internet?
  - Considerations:
    - Mission to “deliver all the bits, fast”
    - Potential to disrupt applications (80/udp & Google)
    - Manageability of multiple custom policers

Denial of Service Measures: RTBH (aka BGP Null Route)

Remotely triggered black hole

- Mechanism:
  - Client sends specific host /32 route to OARnet tagged with appropriate BGP community value
    - nnn:nn for Internet
    - mmmm:mm for Internet2
  - OARnet backbone router sets next hop to discard
  - Once BGP policy is configured, client can send prefixes without escalating to OARnet

Denial of Service Measures: RTBH (aka BGP Null Route)

- Considerations:
  - Target IP will not be able to communicate with Internet. *(Yes, this may have been the intent...)*
  - However, this may allow the rest of your network to stay up during the attack!
- Strongly encouraging clients to set up RTBH for use when needed

```
mab@yyyyy-r0a> show configuration policy-options policy-statement MMM-ASnnnnn-IN
term CANDIDATE-NULL {
     from {
          community AS600-NULL;
          route-filter 64.113.176.0/20 prefix-length-range /32-/32;
          route-filter 208.108.232.0/23 prefix-length-range /32-/32;
     }
     then {
          next-hop discard;
          accept;
     }
}
```

Denial of Service Measures: Hybrid Mitigation

- Deployed for K12 networks in Ohio
- 28 locations serving 700 districts
- Vendor-based Hybrid architecture:
  - CPE device to filter, detect anomalies, trigger alert
  - Cloud scrubbing service for larger events
  - Manual intervention to approve BGP swing to cloud
  - OARnet provided addresses outside allocated IP space for GRE tunnel termination & management

Concluding thoughts

- Many “DDoS” events aren’t volumetric pipe-filling attacks but instead target weak points @CPE, in particular firewalls
- Education and communication with clients cannot be overemphasized
- Consider different solutions to protect different resources: e.g. protect a web site by outsourcing to a CDN

OARnet

An OH·TECH Consortium Member

Thank you