Ultra fast DDoS Detection with FastNetMon at Coloclue (AS 8283)

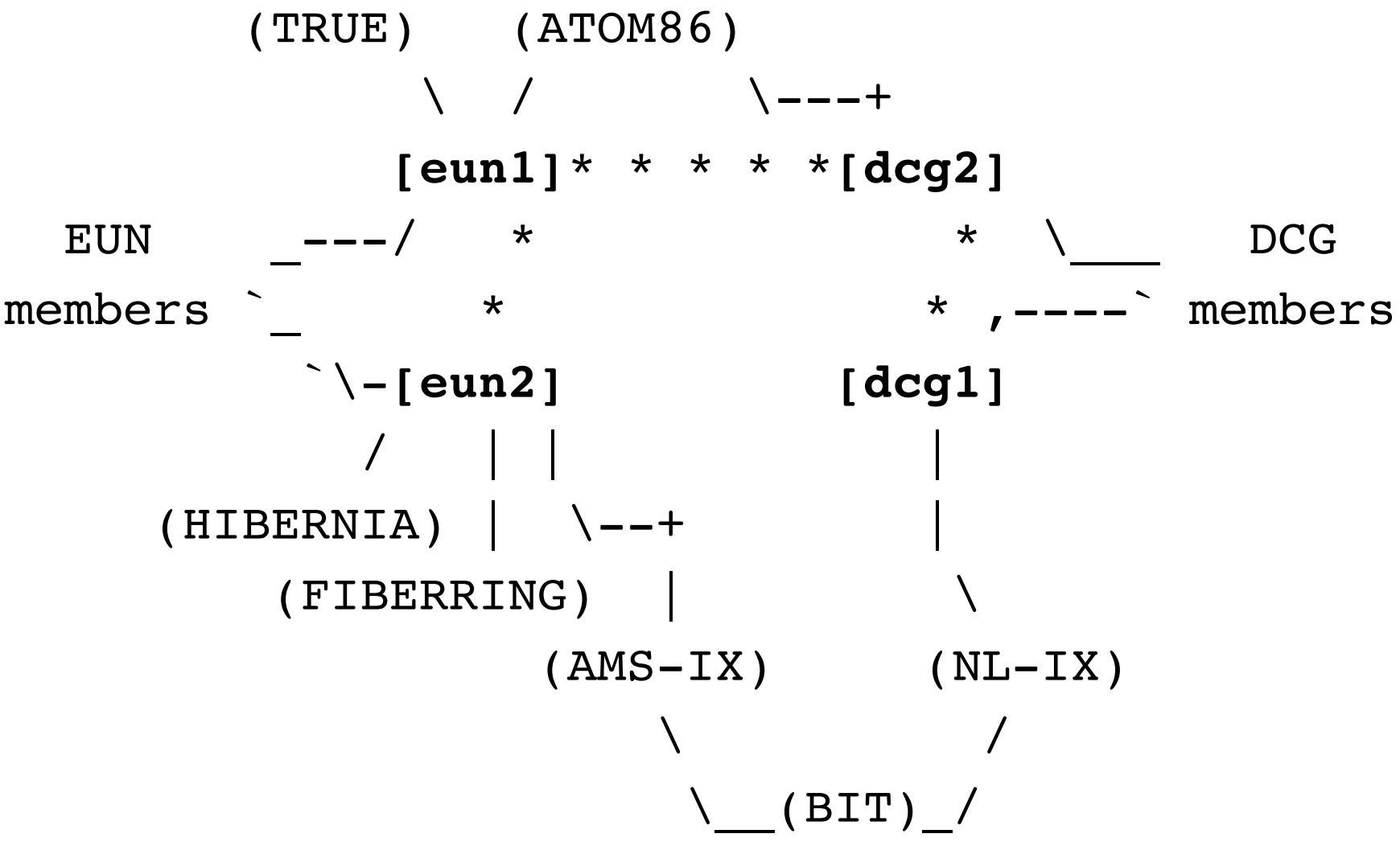
Job Snijders

job@instituut.et

What who where how?

- Coloclue non-profit 100% volunteer driven ISP
- 2 datacenters
- 4 routers
- 100 members
- < 100mbit/sec total traffic
- **Received 2 DDoS attacks in the last year**

Coloclue AS 8283

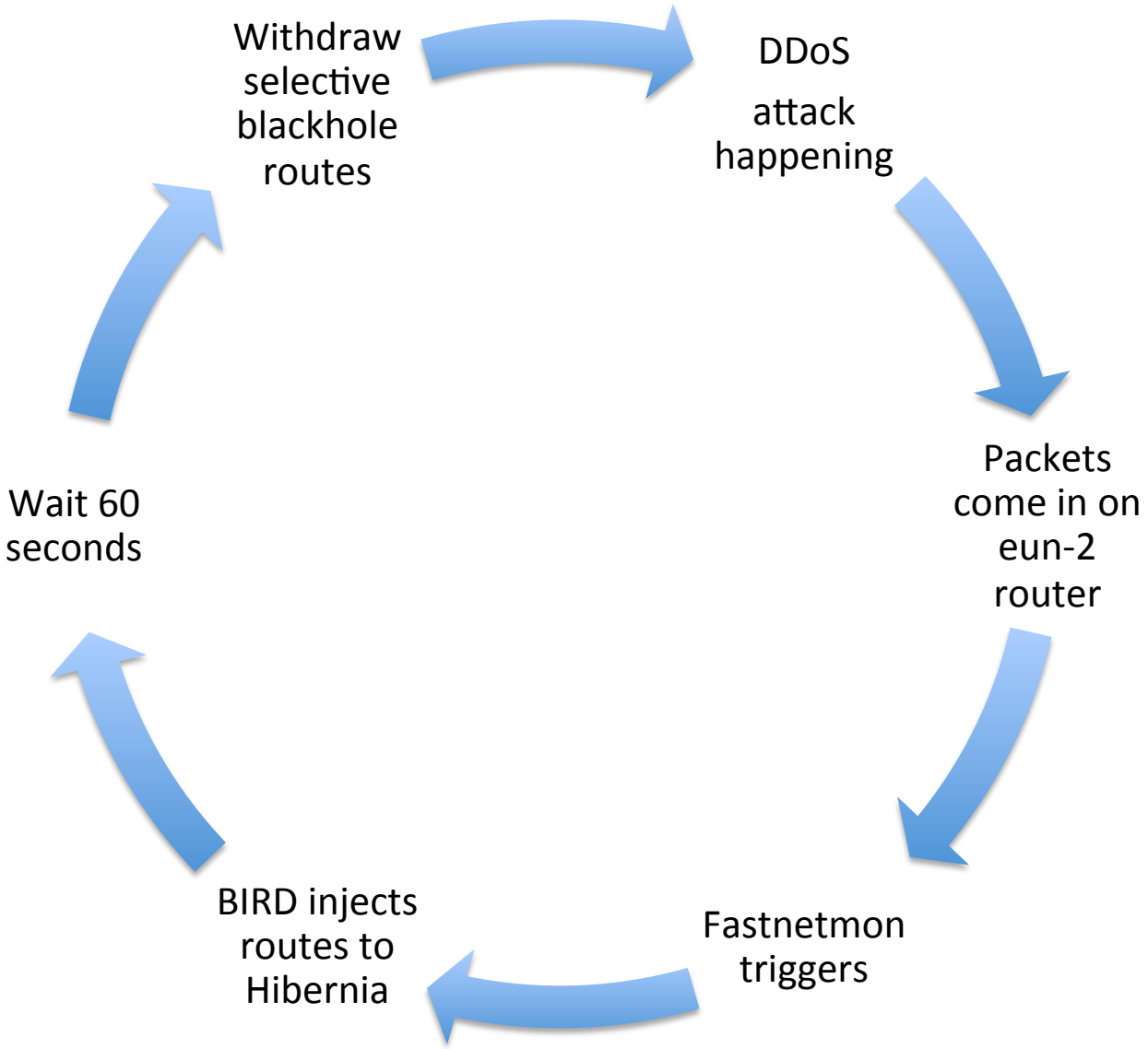


I got tired of it after second attack, decided to automate the problem away:

- Ingredients: FastNetMon, BIRD & shellscripts
- Detection within 3 seconds
- Mitigation selective blackholing: 1 second
- 100% automated
- ???
- Non-profit ;-)

Solving a DDoS problem in 4 seconds!!

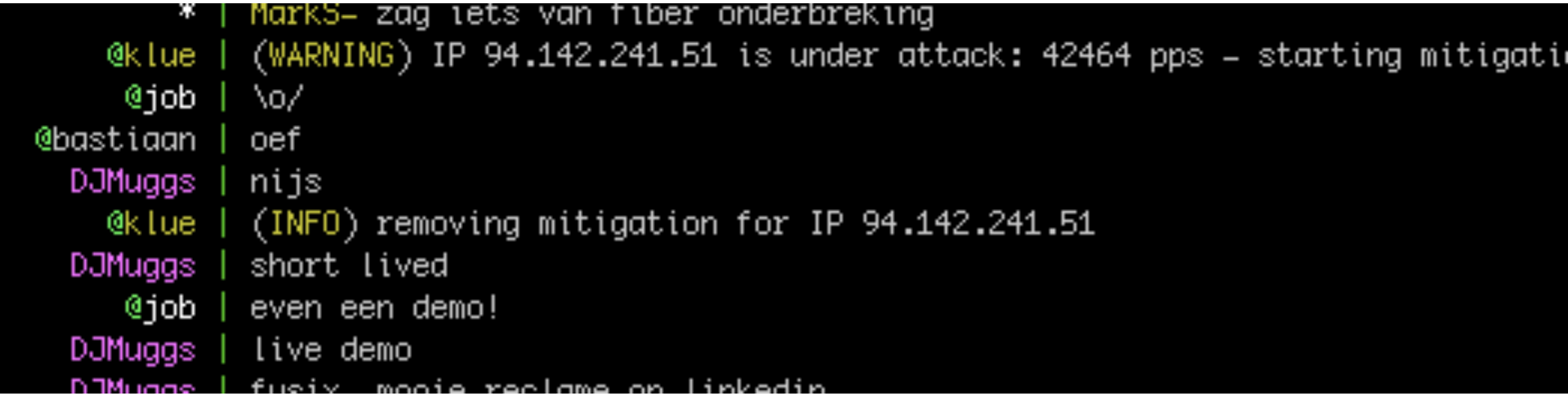
Circle of life



Launch a DDoS (iperf)

```
job@scarlett:~$ sudo iperf -u -c masteen.6core.net -b 200M --parallel 5
------------------------------------------------------------
Client connecting to masteen.6core.net, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  4] local 83.231.213.226 port 45850 connected with 94.142.241.51 port 5001
[  3] local 83.231.213.226 port 55930 connected with 94.142.241.51 port 5001
[  5] local 83.231.213.226 port 59579 connected with 94.142.241.51 port 5001
[  7] local 83.231.213.226 port 40184 connected with 94.142.241.51 port 5001
[  6] local 83.231.213.226 port 59186 connected with 94.142.241.51 port 5001
^C[ ID] Interval       Transfer     Bandwidth
[  4]  0.0- 1.0 sec  23.3 MBytes   203 Mbits/sec
[  4] Sent 16601 datagrams
[  3]  0.0- 1.0 sec  20.9 MBytes   181 Mbits/sec
[  3] Sent 14875 datagrams
```

Immediate IRC notification in #coloclue



FastNetMon?

A high performance DoS/DDoS load analyzer built on top of multiple packet capture engines:

- NetFlow v5, v9
- IPFIX
- sFLOW v5
- Port mirror/SPAN capture with **PF_RING** (with ZC/DNA mode support need license), NETMAP and PCAP

Fastnetmon config

```
average_calculation_time = 5
average_calculation_time_for_subnets = 20
ban_details_records_count = 100
ban_for_bandwidth = on
ban_for_flows = off
ban_for_pps = off
ban_time = 60
check_period = 1
enable_ban = on
enable_connection_tracking = off
enable_pf_ring_zc_mode = off
enable_subnet_counters = off
interfaces = p1p2,p2p1,p2p2.1003
max_ips_in_list = 10
mirror_netmap = off
mirror = on
monitor_local_ip_addresses = on
networks_list_path = /etc/networks_list
notify_script_path = /usr/local/bin/notify_about_attack.sh
process_incoming_traffic = on
process_outgoing_traffic = off
sort_parameter = bytes
threshold_flows = 3500
threshold_mbps = 400
threshold_pps = 20000
white_list_path = /etc/networks_whitelist
```

/etc/networks_list:

94.142.240.0/21

185.52.224.0/22

195.72.124.0/22

“deal with it”

```
root@eunetworks-2:~# cat /usr/local/bin/notify_about_attack.sh | grep -v \#

email_notify=routers@coloclue.net
if [ "$4" = "unban" ]; then
    rm /etc/bird/blackholes/${1}.ipv4.conf
    birdc configure
    echo "(INFO) removing mitigation for IP $1" | /usr/local/bin/klue.pl
    exit 0
fi
if [ "$4" = "ban" ]; then
    cat | mail -s "FastNetMon: IP $1 blocked: $2, $3 pps attack" $email_notify;
    cat << EOF > /etc/bird/blackholes/${1}.ipv4.conf
route ${1}/32 via "lo";
route $(echo ${1} | sed 's/\.[0-9]*$/.0\/24/') via "lo";
EOF
    birdc configure
    echo "(WARNING) IP $1 is under attack: $3 pps - starting mitigation" | /usr/
local/bin/klue.pl
    exit 0
fi
if [ "$4" == "attack_details" ]; then
    cat | mail -s "FastNetMon Guard: IP $1 blocked because $2 attack with power
$3 pps" $email_notify;
fi
```

Injecting into BIRD

```
# in /etc/bird/bird.conf

protocol static blackhole1 {
        include "/etc/bird/blackholes/*.ipv4.conf";
}

template bgp ibgp { .. }    # don't tell iBGP neighbors about blackholes
protocol kernel { .. }      # don't push blackholes into FIB
    …
 export filter {
                if proto = "blackhole1" then reject;
                accept;
        };
    ….

root@eunetworks-2:/etc/bird/blackholes# cat 1.ipv4.conf
route 94.142.241.51/32 via "lo";   # victim IP address
route 94.142.241.0/24 via "lo";    # draw traffic
```

```
filter ebgp_export_hibernia {
      if ( is_coloclue_supernet() ) then {
            accept;  # coloclue space
      }
      else if ( (8283,2) ~ bgp_community ) then {
            accept;  # customer routes
      }
      else if proto = "blackhole1" then {
            if (net.len = 32 && is_coloclue_more_specific()) then {
                  # selective blackhole - discard outside 1000km
                  bgp_community.add((5580,663));
                  accept;
            }
            else if ( net.len = 24 && is_coloclue_more_specific() ) then {
                  accept;
            }
            reject;
      }
      reject;
}
```

Selective blackholing effect: Discard outside 1000 KM radius

Customer connects in Amsterdam, Netherlands
White dot means traffic cannot reach destination
Colored dot implies reachability

Tools

- BIRD (for BGP) - http://bird.network.cz/

- FastNetMon - https://github.com/FastVPSEestiOu/fastnetmon

  &&

  http://fastvpseestiou.github.io/fastnetmon/

Questions?