Using Blackholing Against DDoS Attacks

Peter Hessler

Hostserver GmbH

1 December, 2015

ddos challenge

- two challenges
- external: do not overload connection link
- internal: do not overload firewalls / servers

why blackhole

- blackholing is not what we want to do
- ... it's the best option we have right now
- the point is to keep the business running
- ... normal traffic == upgrade links

blackholing with transit / private peers

- single point of contact
- an actual contract is in place
- can change rules for business reasons
- easy

blackholing with ixp

- contract is with ixp, not peers
- many peers (un)intentionally ignore your cries for help
- most hardware routers have less computing power than a box of cereal
- most filter announcements smaller than /24 and /48
- _will_ miss some

no blackholing ixp

- N ixps, M ways of declaring a blackhole
- not all ixps support blackholing
- ... DE-CIX does
- simply stop announcing to those ixps
- ... choice between latency and availability

blackholing with decix

- set nexthop 80.81.193.66 / 2001:7f8::1a27:66:95
- ... special ip addresses are filtered on switch edge
- requires peers to accept these announcements
- ... did you know about these before today?

blackholing with decix and openbgpd

```
# IPv4 Blackhole
allow from group "iBGP-Peers" community 29140:666 \
        set { localpref 666, nexthop blackhole }
# Allow blackholes from DE-CIX peers
allow from group "DECIX-Peers" \
        inet prefixlen = 32 nexthop 80.81.193.66

# Tell DE-CIX
allow to group "DECIX-Peers" community 29140:666 \
        set { community NO_EXPORT  \
              community BLACKHOLE  \
              nexthop 80.81.193.66 \
        }
# Clean groups before sending outside
match to group "DECIX-Peers" community 29140:666 \
        delete community 29140:*
```

blackholing with decix

- nothing scientific
- ... but 80% of peers don't accept host routes for blackholes
- ... so, 80% will still send you traffic!

ddos attack may 2015

- DD4BC attacked one of our customers
- exactly 1 hour of an attack
- immediate blackhole affected addresses, then analyse

ddos attack may 2015

- udp/80 only
- relaxed filtering
- ... allowed ixps
- transit: region-specific filtering
- real customer traffic during the last 30 min of the attack

ddos attack may 2015

- told DD4BC to go pound sand
- ... NEVER PAY EXTORTION
- ... contact relevant police orgs
- ... nanog65: DD4BC will go away if you defend

ddos reasons

- boredom
- easy cash
- determined
- ... competitors
- ... activists
- ... criminals

why you are a ddos source

- ip spoofing allows DDoS to be effective
- BCP38
- don't run insecure software
- prevent reflection attacks
- should global services actually be global

scrub-a-dub-dub

- scrubbing services
- expensive
- gre tunnel all of your normal traffic
- depend on 'hijacking'
- sole transit

blackhole to the future

- accept blackhole routes
- draft-ymbk-grow-blackholing
- ... community BLACKHOLE / 65535:666
- ixp prefix filtering

blackhole to the future

- sadly, cannot depend on peers actually doing this
- ... more expensive than DDoS attacks?
- ... please upgrade and fix your configs

blackhole to the filter

- ixp filter on dst ip address
- ixp filter on layer 4
- ... udp/80, ntp, dns
- flow spec
- sdn magic

Questions?