ISC.ORG/ANY
(DNS Amplification Attacks)

Eric Ziegast / ISC
DNS-OARC/ICANN
March 13th, 2011
We want the Internet to work better.

**BIND 10**
The next big thing in DNS

**ISC Professional Services**
support, development, training, consulting, audit, design
Call in the experts!

**SNS@ISC**
The ultimate insurance policy for your DNS

**ISC is Public Benefit**
F-root, SNS-PB, BIND, DHCP, AFTR, and more
Do what you can to support us

**SIE**
Changing how the security communities productively collaborate

**RPZ**
New method for DNS-based policy enforcement
Taking back the DNS!

**RPKI**
Securing BGP from route hijacking
DNS Amplification

• What is it?
• Ingredients:
  – Bad actor (hosting, malware)
  – Lack of BCP38 filtering
  – Open recursive nameserver
Recipe Math

• Rent an unmetered 10Mbps server with stolen CC
  – Cloud? Bulletproof?
• Ask an open recursor a 36-byte “ANY” query resulting in 50x response directed at victim IP.
  – Your rate: 10 pps / 2880 bps (b = bits)
  – Victim rate: 10 pps / 144 kbps (will anyone notice?)
• Multiply by 3000 open recursors
  – Your rate: 60 kpps / 8.6 mbps (will ISP notice?)
  – Victim rate: 60 kpps / 432 mbps (victim will notice)
• Add servers as necessary to get N Gbps
Very hard to trace

• Start from the point of view of victim ISP
  – Where are the packets coming from?
    • Backtracing skills in industry are weak
    • Do NOC people have the tools they need?
  – How do I mitigate the flood?
    • Turn off customer, nope
    • Beg upstreams for help
      – What do they do?
Winning!

• In 2009, bad actors used to prefer “./NS”
  - Small query, large answer, widely used
  - Hard to differentiate illegitimate queries
  - Great write-up with pointers:
    http://www.secureworks.com/research/threats/dns-amplification

• In 2011, “isc.org/ANY” is preferred
  # dig @213.214.0.44 isc.org ANY | grep SIZE
  ;; MSG SIZE  rcvd: 3437

• Whose fault is this?
  - Must be ISC -> block ISC.ORG!
  - Must be DNSSEC -> scourge!
Why “isc.org/ANY”?

• Great documentation and tools available:
  – http://dnscurve.org/amplification.html
  – http://dnscurve.org/dnsseccamp.html
    ❤️ thanks ❤️
  – Interesting rebuttal:
    • http://dankaminsky.com/2011/01/05/djb-ccc/

• Why not? Hackers love ISC
  – That bastard who took a stand against SPAM
  – Security involvement

• Sucks to be ISC – or does it?
The real problems

- **Bad intentions**
  - Someone wants to inflict harm
- **Guns**
  - Rent-a-server, cost-shifting, malware, botnets
- **Bullets**
  - Open recursors
  - Lack of BCP38 enforcement
- **No accountability**
  - Not easy to trace back
  - Crooks don't get caught (?)
BCP 38

Ingress Filtering for Multihomed Networks


Snippet:

11.0.0.0/8

ISP  <------  ISP  <------  ISP  <------  ISP  <------ router  <------ attacker
    A                      B                      C                      D                      2
    /                       /                       /                       /                       
    /                       /                       /                       /                       
    /                       /                       /                       /                       
  router 3
  /                       /                       /                       /                       
12.0.0.0/8

(Also see BCP 84 - http://www.ietf.org/html/3704)
Peering

• What guidelines are used?
  – 24-hour NOC, Packet ratios, Multiple regions

• What about BCP38?
  – BCP38 ISP <=> BC38P ISP (yay!)
  – BCP38 ISP <=> non-BCP38 ISP
    Security headache – loaded gun
    Cost-shifting
    Need to filter traffic (?)
    Transitivity A<--->B<--->C
Peering (cont)

• Verification and reputation service for BCP38 enforcement?

• Transparency
  – How many Atlas/RIPE dongls are on your net?
  – Got a PCH box on there?
  – How about a Team Dragon box?
Open resolvers

- Check out RootCon 2011 presentation: http://tinyurl.com/6fxzxwd
Do ISPs need to maintain OR?

Really?
ANY filtering?

• Curious:

# Verizon
$ dig @198.6.1.3 isc.org ANY | grep SIZE
;; MSG SIZE rcvd: 258

# OpenDNS
$ dig @208.67.222.222 isc.org ANY | grep SIZE
;; MSG SIZE rcvd: 140

# Google
$ dig @8.8.8.8 isc.org ANY | grep SIZE
;; MSG SIZE rcvd: 2870

# Level3
$ dig @4.2.2.2 isc.org ANY | grep SIZE
;; MSG SIZE rcvd: 3117
Mitigation

• Education campaigns
  – Does your ISP abide by BCPs?
  – Turn off or modify open recursors

• Why are they needed?
  – Got Google, OpenDNS, Level3, Verizon, etc.

• If you need to run one, use some BCPs
  – Rate limiting, monitoring, reactive filtering

• Open resolver tracking
  – Action -> ORBL? (IP list, RPZ+FW)
  – Rate limiting from known open resolvers?
Backtracing and the Art of War

- Great overview:  
- Internet Samaurai mentoring
- 7 P's - no on-the-job training
- Centralized mobilization – real time
ISC Plan

- We don't yet know the source
  - Malware activation? Hosting? Bad CPE?
  - Not benign (define “benign”) - target appears typical
- Blog the problem
  - FAQ, recommendations, BCPs, monitoring toolkit
- Auth server packet capture
  - Already easily see open resolvers used in attack
  - Real-time release of NS list
  - Backtrace: Plug into snort / capture infrastructure
- CSIRT, NSP-SEC, CERTs, Rolodex
Plan A (cont.)

- Figure out and understand source
- Work with LE & operational security community to go after sources
- Unfortunately: Once we find it, the bad guys will adapt.
- Want to help?
  - Can offer feed directly to OARC servers
  - Login, join the fun