Drilling Down into DNS DDoS

NANOG 63

Bruce Van Nice
DNS DDoS in Increasing: 2014 Data

MILLIONS OF UNIQUE NAMES

DATA REPRESENTS ABOUT 3% OF GLOBAL ISP DNS TRAFFIC

MILLIONS

[Graph showing millions of unique names over months with notable events:
- Late January: New attack starts
- June: Large increase to attack activity
- November: New exploit, powerful malware, more sophisticated
- December: Another increase in attack activity]
Random Subdomain Attacks

**RANDOM**  **TARGET NAME**

wxctkzubkb. liebiao.800fy.com

- Queries with random subdomains
  - Answer with “non-existent domain” (NXD)
- Creates lots of work for resolvers
  - Queries require recursion
- Creates lots of works for authoritative servers
  - Heavy volumes of NXD queries often cause failure
Attacks have Evolved

- We have seen 4 distinct attacks:

  - 2014 - Worldwide attacks using open DNS proxies
  - Nov 2014 – first attacks using bots
  - Dec 2014 – Spike in intensity per IP
  - Jan 2014 – Highly focused attacks
Different Kinds of “Random”

nbpdestuvjklz.pay.shop6996.com.

1lHecqrP.xboot.net.

hxdfmo.iyisa.com.

a6ca.cubecraft.net.

Different Patterns = Different Attacks
First Method of Attack

Attacks Using Open DNS Proxies

1. Query with randomized subdomains
   - Compromised hosting
   - Open DNS Proxy (Home Gateway)

2. Recursive queries
   - ISP Resolver
   - ISP

3. NXD responses
   - Authoritative Server
   - Target Web Site

ISP

Internet
Open Resolvers Are Declining

Open Resolvers

Open Resolver Project Data

Millions

Feb 13 2014
Jan 28 2015

nominum
Where Are They Now?
Second Method of Attack

Attacks Using Bots

1. ISP
   - Queries with randomized subdomains

2. Recursive queries
   - ISP Resolver

3. NXD responses
   - Authoritative Server
     - Target Web Site

Bot infected devices
1. Bots scan networks for home gateways or other vulnerable devices
2. Attempt to login with default passwords
3. Load malware on gateway
4. Malware sends huge volumes of specially crafted DNS queries
5. When DNS servers cannot handle requests websites become unreachable

A single device sourced 1.5M queries in 3 mins (8000 QPS)!
Example Attack: One DNS Server

Number of random subdomain queries per hour

Several times normal load
Example Attack Data

**Attack Queries as a Percentage of Total Traffic**

70% of queries from attack

- **Nov 16 19:00**
- **Nov 18 8:00**
Example Attack Data

Number of IPs used in attack per hour

Very small numbers of IP addresses
200 IPs have taken down large network