Nick Sullivan
IETF 97 Technical Plenary
Wednesday, November 16, 2016

How to stay online

Harsh realities of operating in a hostile network

DDoS is in all of our futures

TWEETS 779 | FOLLOWING 2 | FOLLOWERS 4,541

Mirai Attacks

@MiraiAttacks

Live feed of DDoS attacks from Mirai botnets. Account run by @2sec4u and @MalwareTechBlog

The Internet of Things

Joined October 2016

Tweet to | Message

Tweets | Tweets & replies

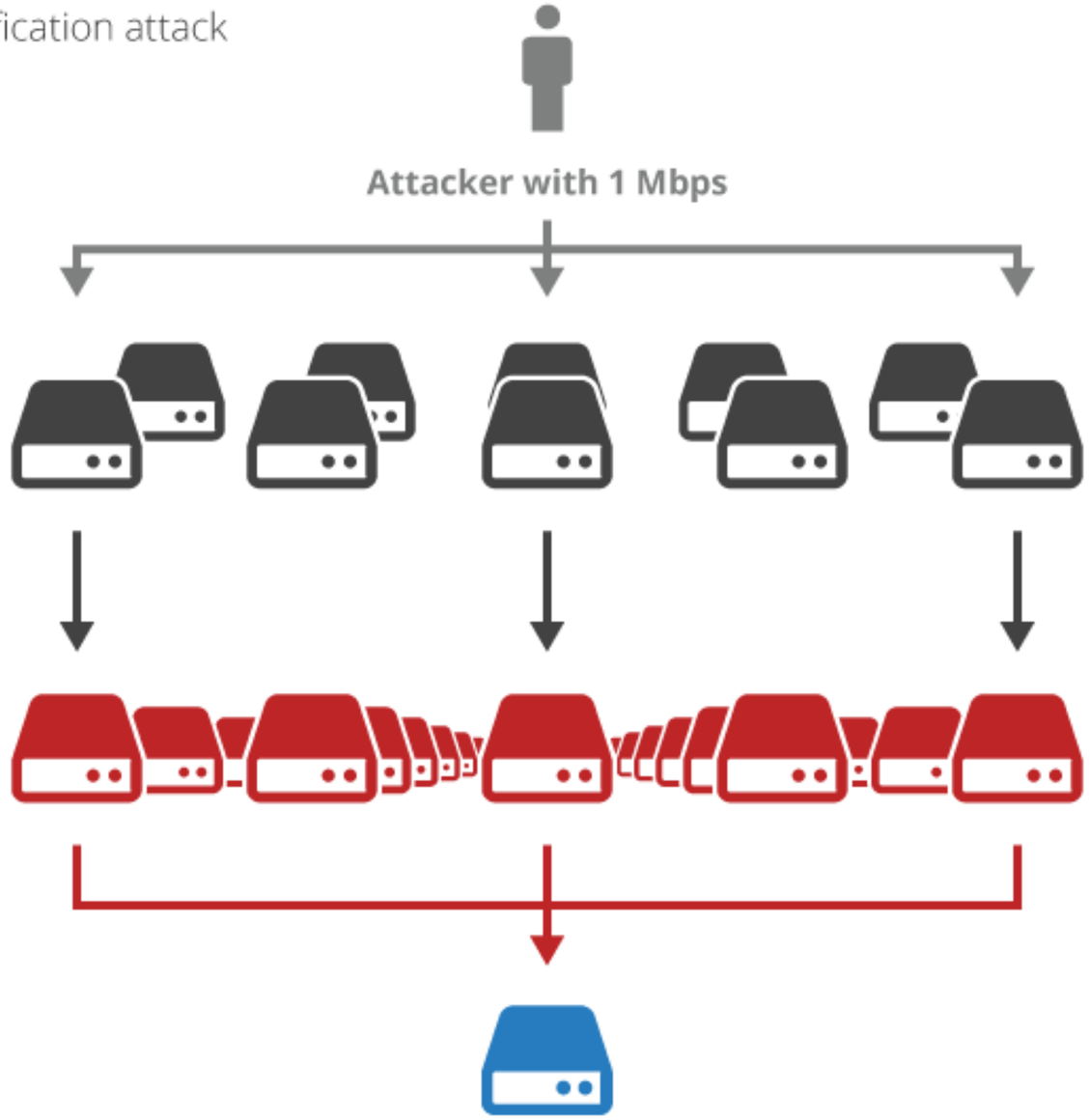
Pinned Tweet

Mirai Attacks @MiraiAttacks · Oct 26

- Account not monitored, see bio for contact.
- The frequent attacks are from smaller botnets.
- We monitor botnets, not run them.

8 21

Amplification attack

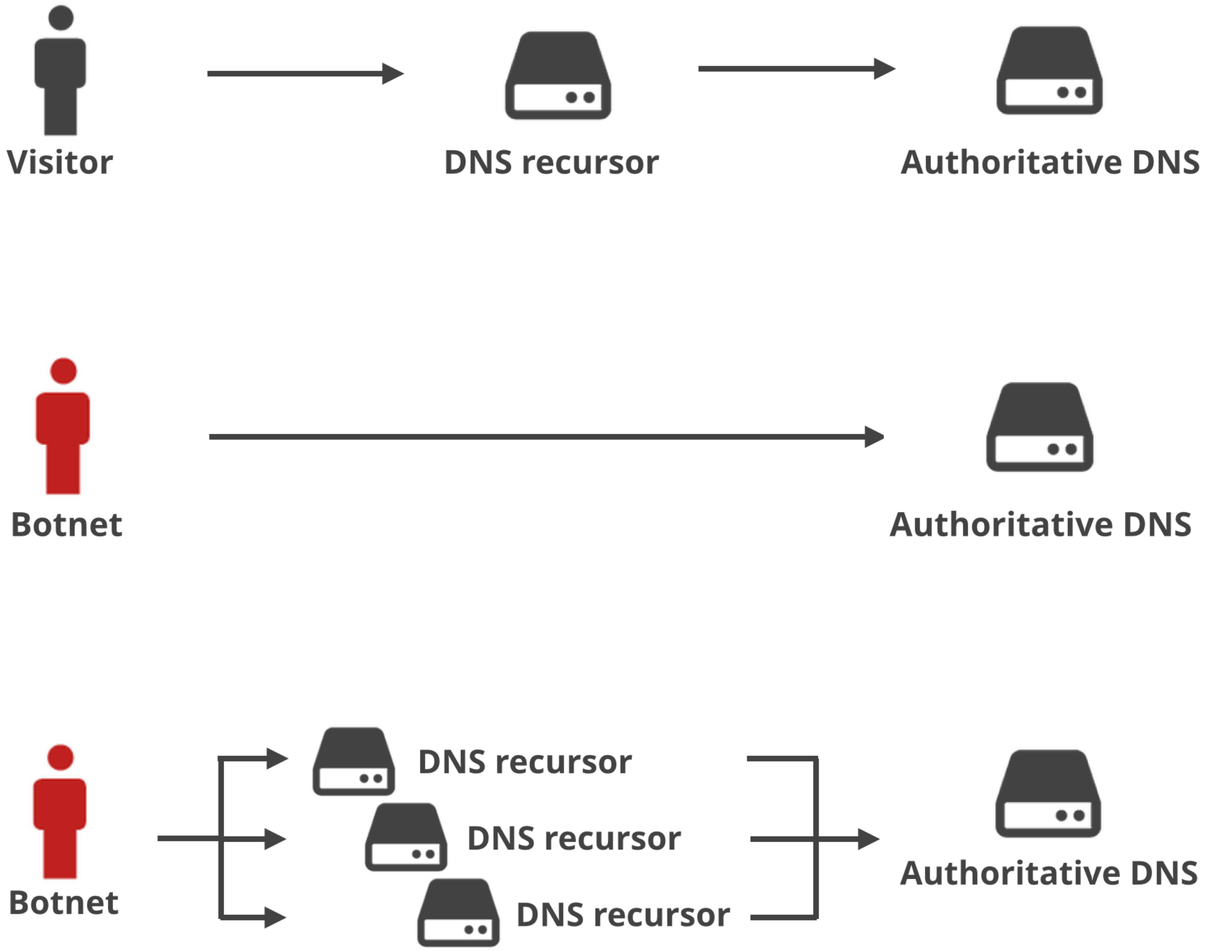


Popular attack types in 2016

- DNS Floods against authoritative DNS
- SYN Floods
- HTTP(S) Floods

CLOUDFLARE

Authoritative DNS Attacks



Direct to Authoritative

Direct To Authoritative

- Treat every request not from a known resolver with suspicion

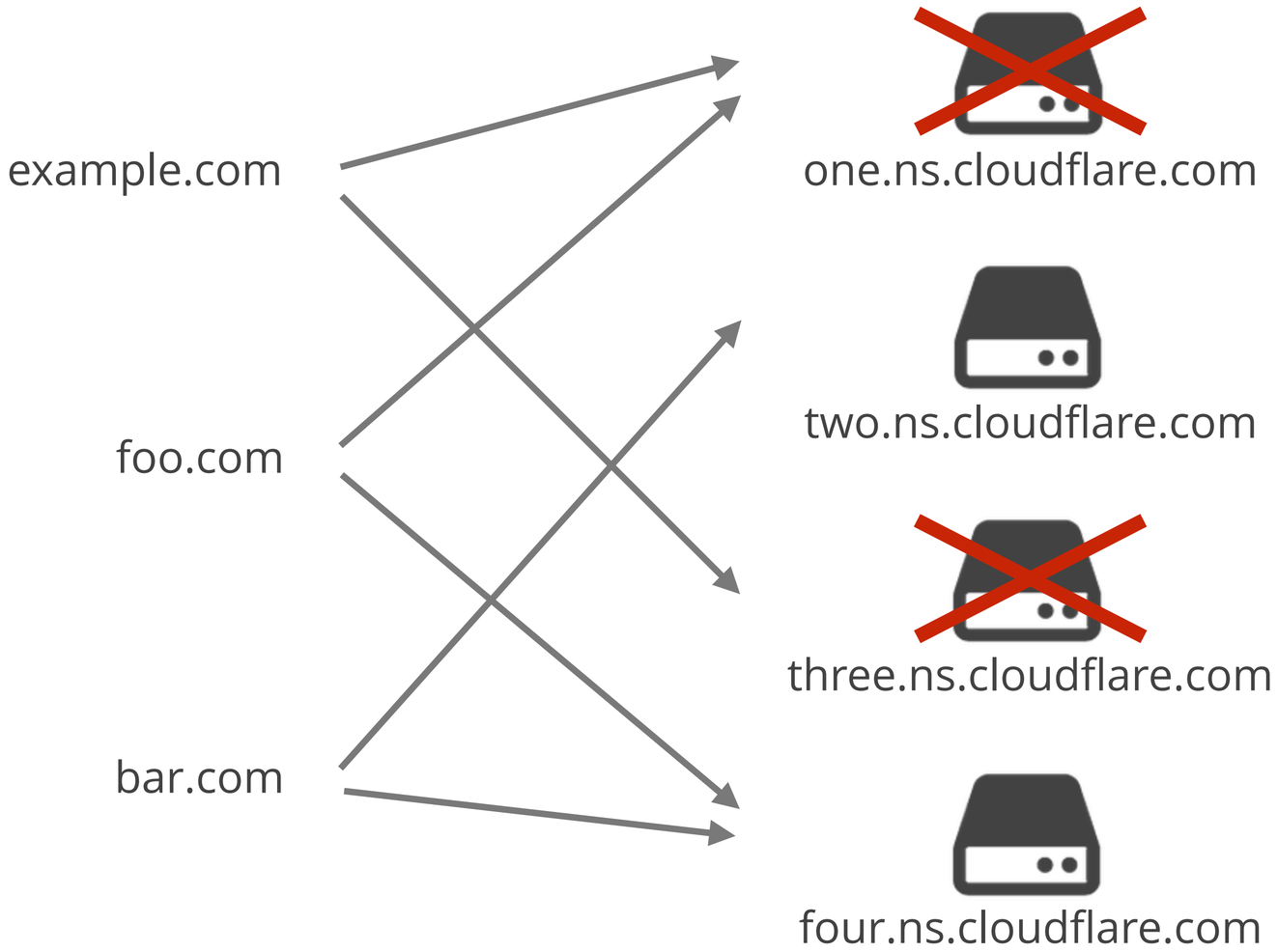
- A flood of requests to authoritative servers from non-resolvers is an attack
- **Just drop the packets**

What do floods look like

- Typically apex domain or random subdomains
  - foo.com
  - www.foo.com
  - <random>.foo.com
  - <random>.www.foo.com
- Sometimes spoofed source address, sometimes not
  - Spoofed is harder to deal with

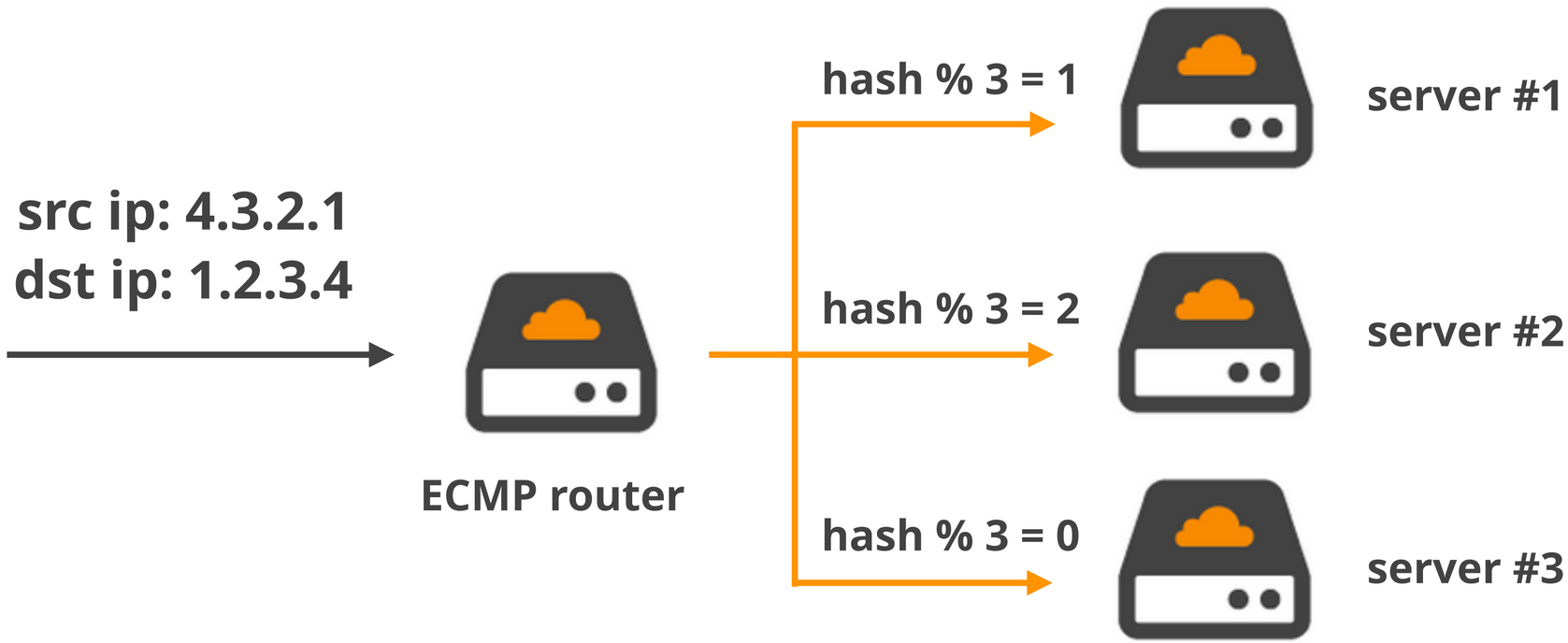
DNS Flood Survival Kit

Null-routing upstream



Anycast: Spread the load worldwide

ECMP: Spread the load in the datacenter



router	10M+ pps	flowspec
network card	6M pps	iptables bpf
kernel	1.2M pps	iptables bpf
DNS application	0.3M pps	selective drops, just handle

Protect the application: iptables BPF

- BPF is arcane but powerful
- Does fairly complex, yet fast matching

```
iptables -A INPUT \
    -p udp --dport 53 \
    -m bpf --bytecode "14,0 0 0 20,177 0 0 0,12 0 0 0,7 0 0 0,64 0 0 0,\
                       21 0 7 124090465,64 0 0 4,21 0 5 1836084325, \
                       64 0 0 8,21 0 3 56848237,80 0 0 12,21 0 1 0, \
                       6 0 0 1,6 0 0 0," \
    -j DROP
```

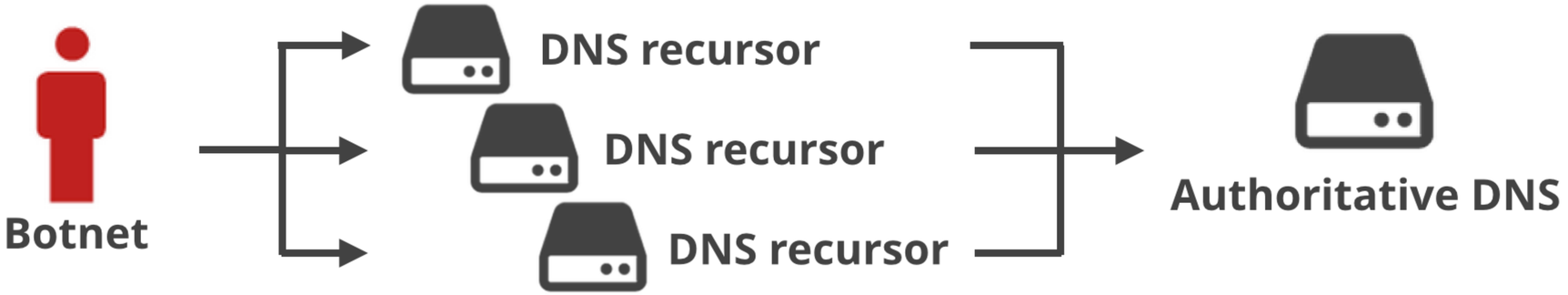
Automation is key

- Sample from sflow, netflow
- Use heuristics, machine learning for new attack types
- Fingerprinting is possible but should not be relied on exclusively
- iptables should not be static, or manually updated

- Push your rules to the NIC if possible

Attacks through the recursor

Attacks through the recursor



Attacks through recursor

- **The right response is to answer**
- Whitelist known recursive DNS servers

Attacks through recursor

- Rate limiting can cause negative effects
  - Recursor can mark rate-limiting server as down
  - Failed requests may be repeated, resulting in unintended amplification
- Recursor can help by caching negative ranges (NSEC)
  - Only available for DNSSEC-signed domains

Other attacks

SYN Floods

- Configure SYN cookies to avoid memory exhaustion
- Blacklist non-regional IPs (from Anycast)
- Use iptables BPF rules

HTTP(S) Floods

- Rate limit by request
- Rate limit by volume
- TCP reset — browsers will retry
- TLS cost is asymmetrical, but usually a low percentage of CPU
  - ECDSA is 10x less CPU for servers
  - Client puzzles??

Who is attacking?

Compromised Endpoints

- It’s going to get worse before it gets better (if it ever gets better)
  - When will we see the first major IoT worm?
  - Discoverability is key to virality. IPv6 has a place.
- The economics will drive the results
  - Secure firmware updates is an expensive proposal
  - Secure-by-default open source software will be used if available
- Attribution
  - ISPs, transits can use netflow to tell "where the attack originated" without relying on source IP’s, but don’t

Global Consequences

The shape of the Internet

- The Internet has choke points
- Attacker bandwidth will continue to grow
- Anycast prevents global attacks from focusing on one point

Keeping costs down

- Ingress << egress for most applications because of cache semantics
- Mixed-use data centers have excess ingress capacity
- Scrubbing centers are single-use, therefore not cost effective

Staying online requires scale

- DNS only one of many points of vulnerability
- Deal with DDoS by handling every packet
  - Spread the load over multiple dimensions (geography, resolution)
- You need to be close to the source, or you need a friend who is
- The techniques described try to approximate this as much as possible

Nick Sullivan
IETF 97 Technical Plenary
Wednesday, November 16, 2016

How to stay online

Harsh realities of operating in a hostile network