DNS Amplification Attack - ANY+RD

October 2012

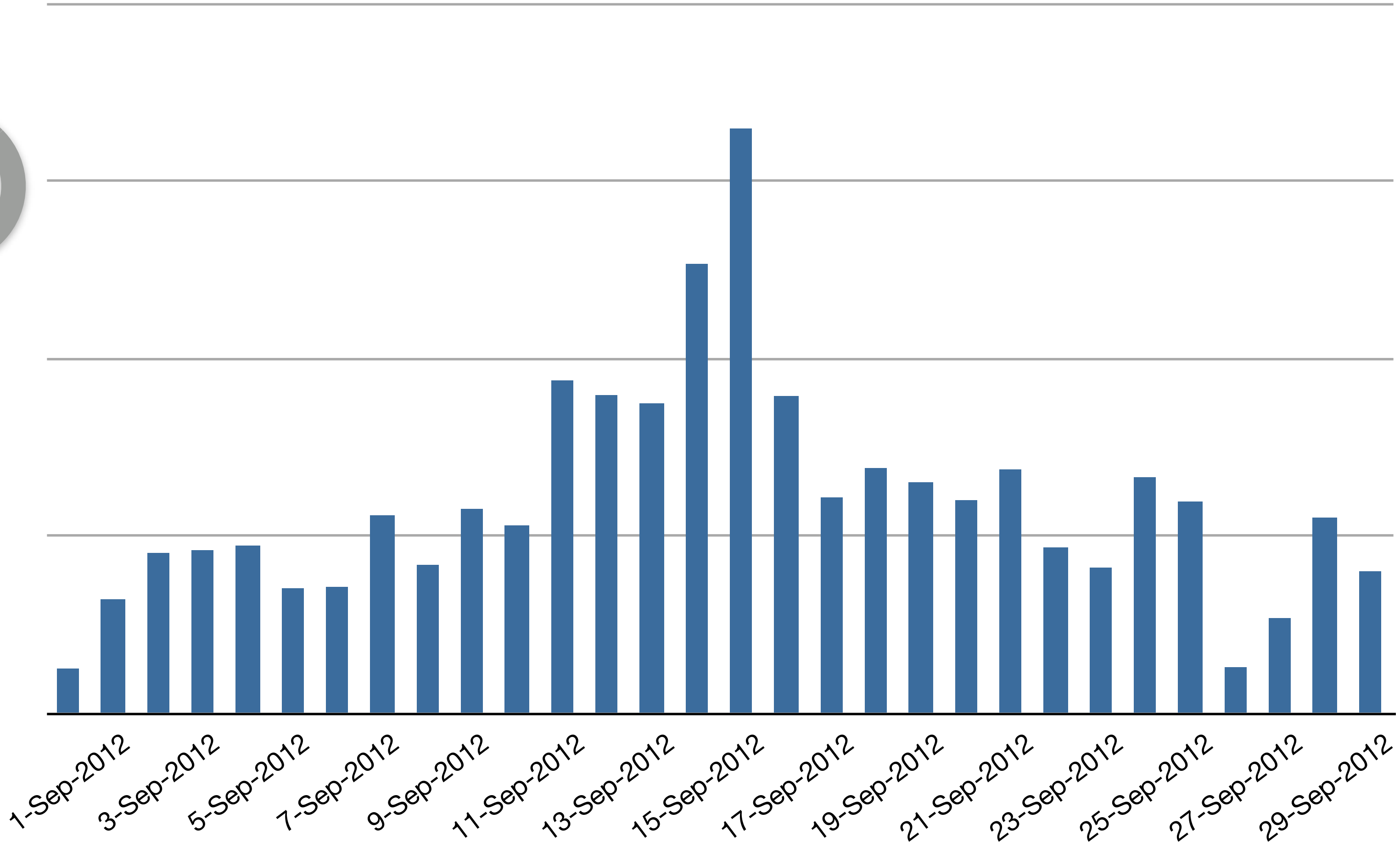
History

- First seen by Dyn in November 2011
- Seen on both our consumer and enterprise authoritative products (Standard DNS and DynECT Managed DNS)
- http://dyn.com/active-incident-notification-recent-chinanetany-query-floods/ - 2-Dec-2011

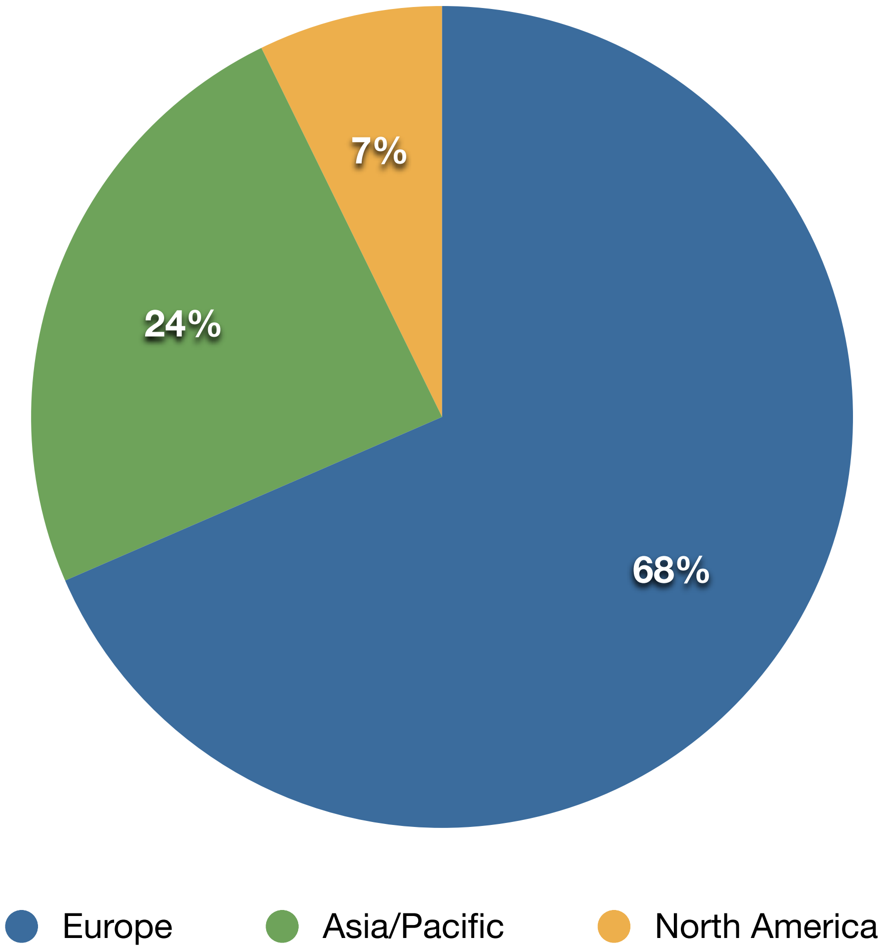
Attack Vector

- Recursion bit set (RD=1)
- QTYPE=ANY
- DNSSEC signed domains
- No EDNS

Attack Queries by Day



Anycast Region



Top Targets

IP	ASN	Org	Country
23.29.116.196	13354	EBLGLOBAL	US
113.21.221.18	45474	NEXUSGUARD	HK
122.248.238.198	38895	AMAZON	SG
64.31.29.26	46475	LIMESTONE	US
114.141.72.36	32787	PROLEXIC	SG
103.22.245.55	6939	HURRICANE	HK
122.248.245.102	38895	AMAZON	SG
113.21.221.21	45474	NEXUSGUARD	HK
121.12.116.52	4134	CHINANET	CN
114.141.72.40	32787	PROLEXIC	SG

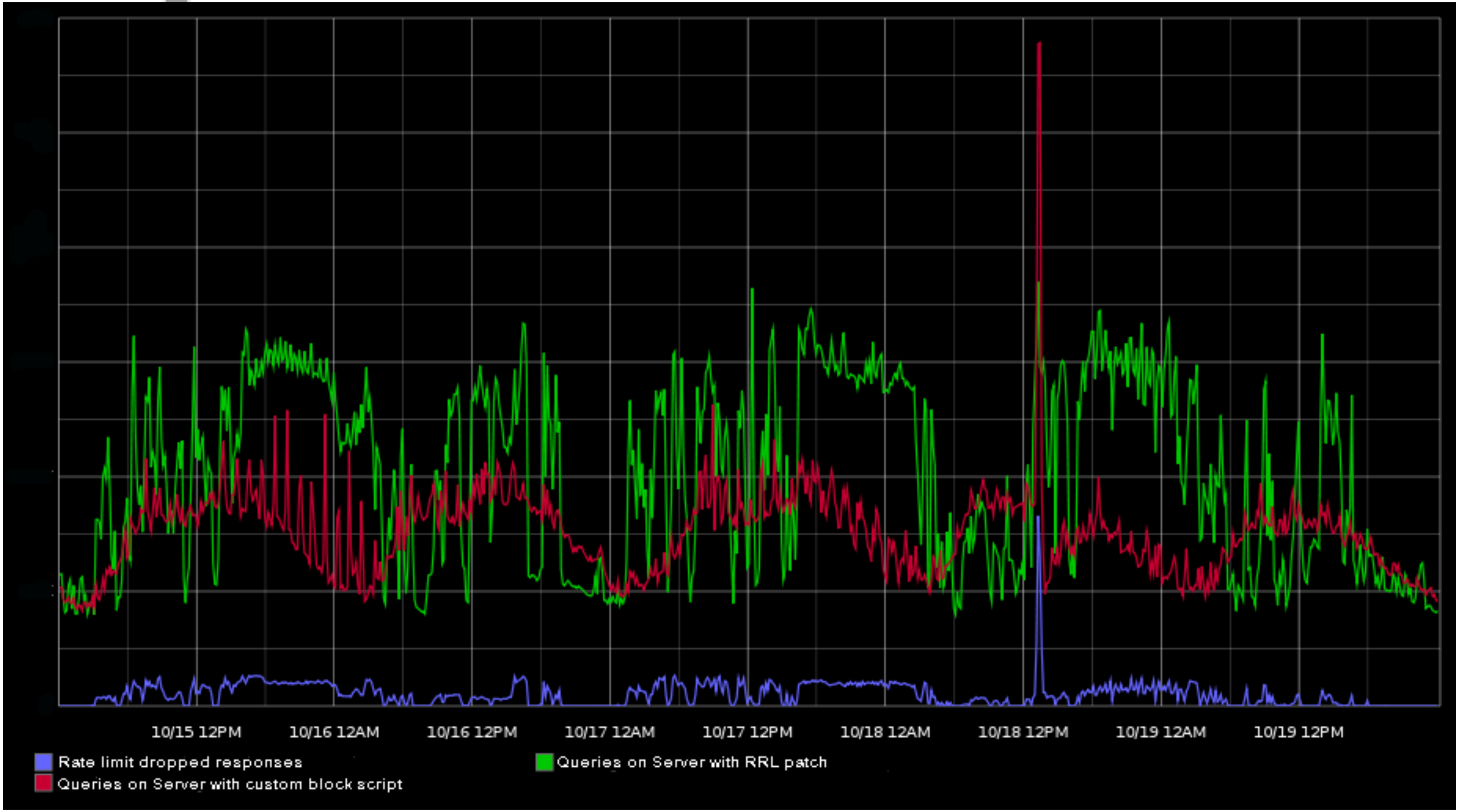
Blocking Sources

- Custom script, reads query logs, blocks sources with a high rate of ANY+RD queries.
- Pros
  - Very effective at blocking sources
- Cons
  - Blocks legitimate queries too
  - Slow to respond to new attacks (~1 min)

BIND RRL Patch

- Response rate limiting
  - http://www.redbarn.org/dns/ratelimits
- Pros
  - Very fast on detecting floods
  - TCP fallback for legit resolvers (“slip”)
  - No full block of client IP
- Cons
  - Ineffective against fast qname changes

BIND RRL Patch - Standard DNS



Dyn℠

DNS
EMAIL
LABS

Chip Marshall
Network and Security Analyst
cmarshall@dyn.com