MADDVIPR: Mapping DNS DDoS Vulnerabilities to Improve Protection and Prevention

Raffaele Sommese, Anna Sperotto, Roland van Rijswijk-Deij
University of Twente
Alberto Dainotti, Kimberly Claffy
CAIDA, UCSD

Why?
The Domain Name System is a fundamental pillar of the Internet's Core Infrastructure. DDoS Attacks against DNS infrastructure will have devastating effects.

DNS as Source of Attack
- Reflection Attack
- Bandwidth Request
- OpenDNS Resolver
- Looted Response

Potential Vectors of Amplification:
- EDNS Record
- ANY Record
- DNSKEY Record
- NSEC(3) Record
- TXT Record (Special Domain Crafted)

Open Resolvers:
Due to the connectionless architecture of DNS Protocol and its amplification factor, OpenDNS Resolvers pose a significant threat to the global network.

Is it really effective?
- The AmpPot project monitors reflection attacks through different HoneyPots, detecting DNS Amplification Attacks.
- DNS Reflection Attacks were monitored similarly through the CAIDA Network Telescope by discovering responses to spoofed queries in the Internet Background Radiation.

DNS as Destination of Attack
- Random Subdomain Attack
- Random DNS Resolvers
- Random Authoritative DNS
- Distributed Reflection Denial of Service (DRDoS)

DNS Attacks:
- Cache Poisoning
- Domain hijacking
- Random subdomain attack
- NXDOMAIN attack
- Phantom domain attack
- NSEC White Lie DoS
- DDoS DNS flood attack
- Distributed Reflection Denial of Service (DRDoS)

Impact of an Attack: Dyn’s Case
One of the biggest DDoS attacks on the DNS infrastructure was performed in 2016 against Dyn DNS. This attack affected a number of large Internet services on the East Coast of the United States, including some big-name Internet brands such as Twitter, PayPal, and Spotify.

DNS Misconfiguration and Vulnerabilities
- Infrastructural SpOf
- Unreachability
- NSEC(3) Enumeration
- Parent-Child Zone Data Mismatch
- TTL and NS Mismatch
- Ghost Glue Record
- Lame Delegation
- Cyclic Zone Dependency
- Single Point of Failure (SpOf)
- Single and Duplicated NS Records
- Infrastructural Single Point of Failure
- Dangling Pointer
- DARE Records
- Cloud IP Addresses and DNS names
- Expired Domain Hijacking

Proposed Solution in Literature
- BCP38
- Spoofer Project
- Rate Limiting
- Feature and Record Disabling
- Still vulnerable to Crafted Domains
- DNSSEC Key Shrinking
- Adoption of ECDSA

Spoofing Protection
- BCP38
- Spoofer Project

Rate Limiting
- Feature and Record Disabling
- Still vulnerable to Crafted Domains

DNSSEC Key Shrinking
- Adoption of ECDSA

Our Approach
1) Identification of impact of possible attacks
2) Provide a view of future attacks
3) Prioritization of the risks

Other Sources
- AmpPOT
- Reflector Honeypots
- Botnet command snooping

Measurements
- OpenIntel
- Large-Scale, active DNS measures
- UCSD Telescope
- /8 Darknet

Data Analysis
- (SpOf)
- Single Point of Failure Vulnerabilities
- DoS ecosystem (DNSAttackStream)

Synthesis and Consolidation
- MADDVIPR

DDoS Protection Services
- Adoption and Effectiveness
- Serving Stale Data
- “Stale bread is better than no bread”.
- Serving data with expired TTL if the Authoritative Nameservers become unreachable.

ANYCAST
- Rate Limiting
- Problem to manage situations of partial failures.

Actionable Intelligence
- on current and future DoS against the DNS

Other Sources
- AmpPOT
- Reflector Honeypots
- Botnet command snooping

Measurements
- OpenIntel
- Large-Scale, active DNS measures
- UCSD Telescope
- /8 Darknet

Data Analysis
- (SpOf)
- Single Point of Failure Vulnerabilities
- DoS ecosystem (DNSAttackStream)

Synthesis and Consolidation
- MADDVIPR

DDoS Protection Services
- Adoption and Effectiveness
- Serving Stale Data
- “Stale bread is better than no bread”.
- Serving data with expired TTL if the Authoritative Nameservers become unreachable.

ANYCAST
- Rate Limiting
- Problem to manage situations of partial failures.