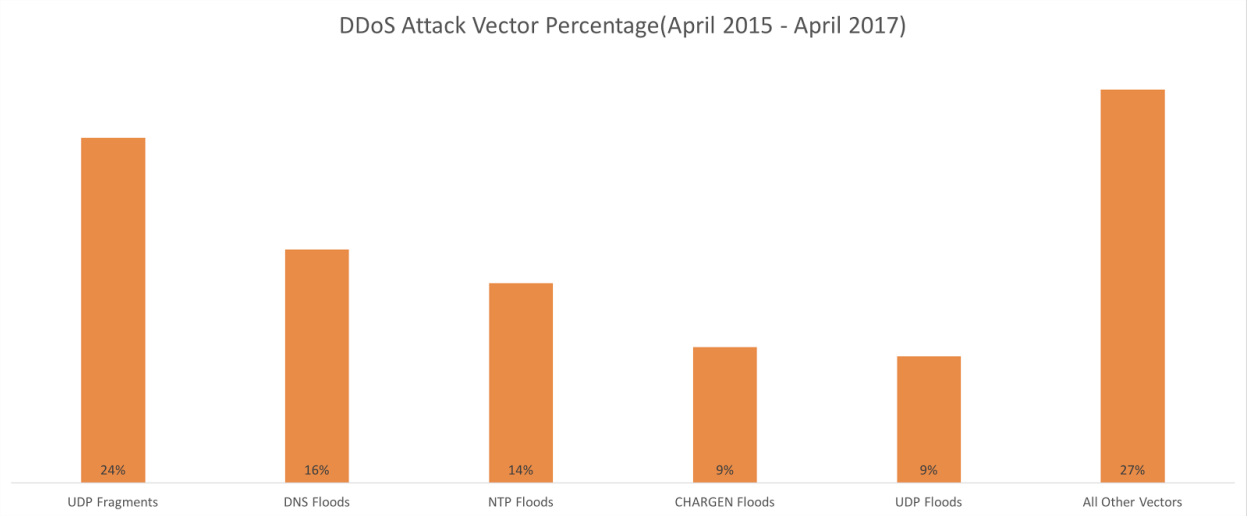
TLP: GREEN
RISK FACTOR: HIGH

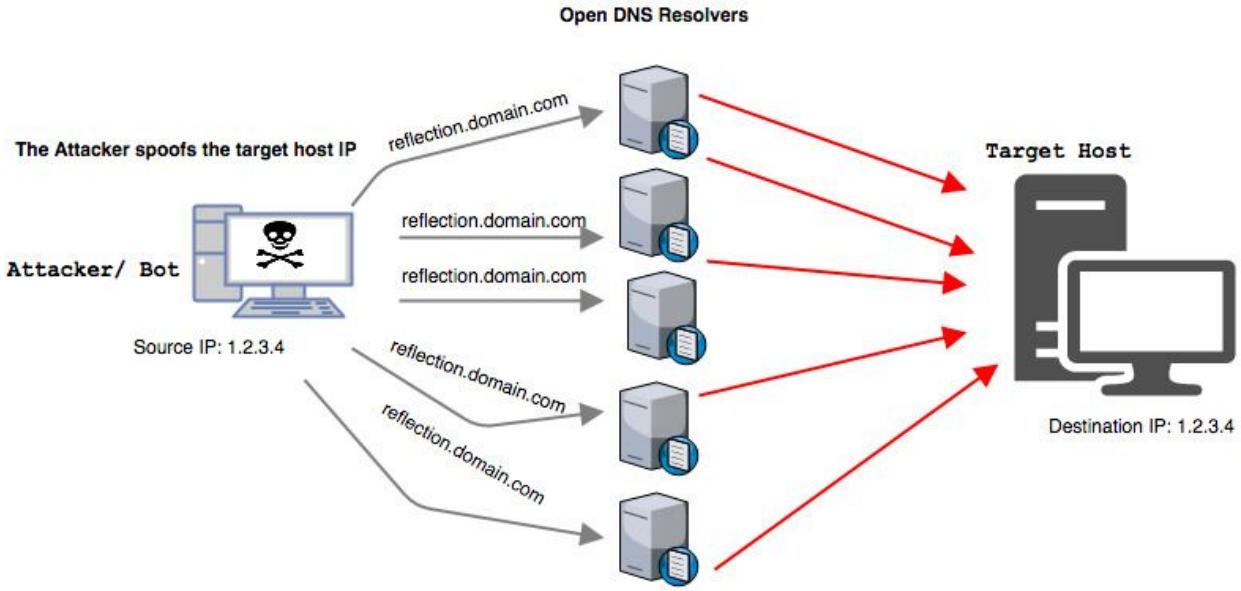
Whitepaper: DNS Reflection, Amplification, & DNS Water-torture

1.0 / OVERVIEW / In Akamai's quarterly *State of the Internet - Security* report, DNS floods comprise one of the top five vectors mitigated on our DDoS platform. In fact, they are the second most prominent attack type over the last two years, with a 16% share of all DDoS attack vectors we've seen. These attacks either target DNS servers directly with a flood of queries or abuse open DNS resolvers to reflect DNS response traffic to a target host. The latter is the most commonly observed, and is specifically referred to as a DNS reflection and amplification attack. While this attack type makes up the bulk of DNS flood attacks, the DNS query flood can potentially be a more disruptive attack when backed by a large botnet. The latest wave of DNS query floods is powered by the Mirai malware based botnets. While these two attack types are both classified as DNS floods, they have different methods of operation that require different mitigation strategies.



2.0 / DNS reflection - Answers To Unasked Questions / DNS reflection attacks have been observed for years. Akamai noted upticks in this attack method back around November 2012. Despite the name, typical targets of this attack are web servers and online gaming servers. However, any other Internet addressable endpoint can become a potential target. The name of the attack is specific to its abuse of the DNS protocol. In particular, this attack leverages the connectionless nature of the UDP protocol to abuse DNS servers that are configured as open resolvers. The attack is similar to sending someone a letter in the mail that requires a response, but putting someone else's address as the return address. Figure 1 illustrates how an attacker leverages multiple open resolvers to initiate a DNS reflection attack against a single target.

DNS Reflection Flood



2.0a / DNS Reflection - Attack Tool And Methods / This attack does not appear to have evolved much from what was observed early on. The attacks are also not complicated in nature but they do require some initial leg work to be done by the attacker. For example, many of the reflection based attack scripts will also have a companion script for scanning and discovering usable reflectors. Attackers must first determine which hosts will not only respond but also provide the required amplified response payload. The resolvers make up one of the components of a reflected DNS attack.

Common components of a DNS reflection and amplification attack

- DNS open resolvers (fuel)(reflector)
- Domain name with large amounts of data (catalyst)(payload)
- Attack tool (weapon)
- Attacker
- Target IP

Current observed attacks exhibit attributes indicating that they are still being launched using the DNS flooder(aka DNS amp) attack tool. The attack script allows for automation of the task of sending out queries to large lists of open dns resolvers.

DNS flooder command-line parameters

dnsflooder [target ip] [target port] [list of dns reflectors] [threads] [attack time in seconds]

Applying the same request characteristics used by the DNS flooder tool with the command-line tool dig, reveals the difference in payload size from a regular A query record request and the DNS flooder ANY request.

Query sample MSG SIZE - default dig DNS request
dig @x.x.x.x activum.nu
;; Query time: 287 msec
;; MSG SIZE rcvd: **102**

Query sample MSG SIZE - dig ANY request
dig @x.x.x.x +bufsize=9000 +ignore +retry=0 any activum.nu
;; Query time: 349 msec
;; MSG SIZE rcvd: **3322**

Amplified DNS response example from attack traffic(3,322 bytes of data without IP and UDP headers):
09:57:50.974647 IP (tos 0x0, ttl 57, id 1507, offset 0, flags [+], proto UDP (17), length 1500)
x.x.x.x.53 > x.x.x.x.**55638**: 22390| q: ANY? activum.nu. 26/0/1 activum.nu. RRSIG, activum.nu. RRSIG, activum.nu. RRSIG, activum.nu. Type51, activum.nu. RRSIG, activum.nu. RRSIG, activum.nu. RRSIG, activum.nu. TXT "Hosted by Exeo - www.exeo.se - +46-141-48600", activum.nu. RRSIG, activum.nu. RRSIG, activum.nu.[|domain]
09:57:50.974907 IP (tos 0x0, ttl 57, id 1507, offset 1480, flags [+], proto UDP (17), length 1500)
x.x.x.x > x.x.x.x: ip-proto-17
09:57:50.974910 IP (tos 0x0, ttl 57, id 1507, offset 2960, flags [none], proto UDP (17), length 390)
x.x.x.x > x.x.x.x: ip-proto-17

The actual request size is a total 39 bytes of data, without the headers, creating an amplification of 85x based on this domain's response data. If we revisit the letter analogy, this would be like sending a letter to someone and then another address receives a pile of anvils. Needless to say this is a bandwidth generating attack.

2.1 / DNS Query Floods - Too Many Questions To Answer / DNS, or Pseudo Random Subdomain (PRSD), floods are characterized by the attackers targeting a domain with nonexistent randomly generated prefixed subdomain requests causing the target DNS servers to look up the nonexistent subdomain and reply with a NXDOMAIN response. The potential impact of this attack was suddenly realized when the Mirai botnet was used to launch its own brand of DNS query flood, named the "DNS water torture" attack. This is a high packet rate flood of DNS A record queries for a given domain prepended with a randomly generated sub-domain. The target DNS server is tasked with responding to their usual query workload along with this flood of bogus queries.

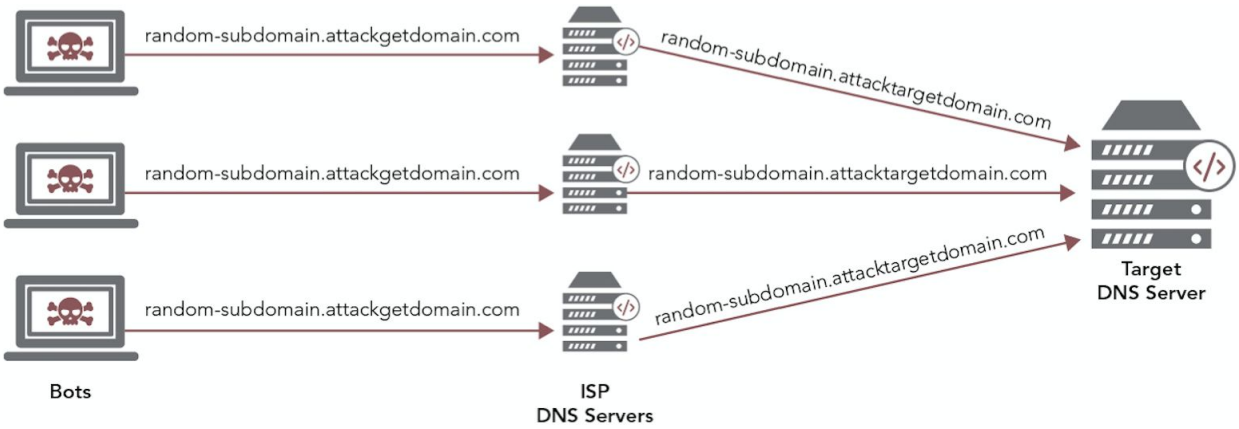


Figure 5 - DNS query flood(Mirai water torture).

2.1a / DNS water torture - Attack Tool And Methods / The contemporary topic of discussion when it comes to DNS query floods centers on the Mirai sourced DNS water torture attacks. In the case of Mirai, massive attacks were launched from a large collection of compromised IoT devices and servers around the Internet. While this technique does not require a botnet, leveraging a botnet greatly increases impact.

Common components of Mirai DNS water torture attack

- Infected bots
- C2(s)
- Mirai malware
- Attacker
- Target IP

When machines are infected with Mirai, they will maintain communications with the botnet's command and control server. These "zombies" will wait for attack commands to be issued. An example command for a DNS query flood would be structured as shown here:

Typical attack command options sent to bots

- Attack Type (DNS)
- Target Domain
- Attack Duration

The command will ultimately result in a flood of DNS queries originating from the infected machines that received the attack command to their upstream resolvers. These queries, for nonexistent domains, will ultimately be resolved by the upstream resolver as far as the target's authoritative servers are concerned. Since a given domain may have more than one authoritative name server, and the distribution of the attacking sources is likely widespread, this traffic may be split among all known DNS servers for the targeted domain.

2.2 / Mitigated Attack Examples /

- Peak bandwidth: 10 Gigabits per second
- Peak packets per second: **14 Million Packets per second**
- Attack Vector: DNS Query Flood
- Source port: Random
- Destination port: **53**

```
DNS Query Flood(Aka Mirai DNS Water Torture Attack) - Target Domain Names Removed
11:48:43.171738 IP x.x.x.x.47645 > x.x.x.x.53: 59218 [1au] A?
02uqhuovfi1f.<redacted>.com. (xx)

11:48:43.171749 IP x.x.x.x.47371 > x.x.x.x.53: 62949 [1au] A?
qo5etoh5foab.<redacted>.com. (xx)
```

Fig 6 displays the payload of the incoming attack traffic.

- Peak bandwidth: **12 Gigabits per second**
- Peak packets per second: 1 Million Packets per second
- Attack Vector: DNS Reflection and Amplification Flood
- Source port: **53**
- Destination port: 443

```
DNS Reflection Flood
19:36:41.098600 IP x.x.x.x.53 > x.x.x.x.443: 12088 245/2/4 A x.x.x.114, A
x.x.x.204, A x.x.x.229, A x.x.x.38, A x.x.x.72, A x.x.x.84, A x.x.x.78, A
x.x.x.110, A x.x.x.76, A x.x.x.192, A x.x.x.26, A x.x.x.158, A x.x.x.208, A
<snip>,[|domain]

19:36:41.098603 IP x.x.x.x > x.x.x.x: ip-proto-17

19:36:41.098605 IP x.x.x.x > x.x.x.x: ip-proto-17
```

Fig 6 displays the payload of the incoming attack traffic.

3.0 / Suggestions & Mitigation / DNS based DDoS attacks are a potential concern for organizations across a wide variety of industries. The accessibility of DNS reflection in particular means that anything can be targeted, even individual home IPs. There are some techniques to help cope with these types of attacks and prevent them from having a significant impact on operations.

At A Glance Attack Overview:

DNS Reflection	DNS water torture
• volumetric attack (Layer 3)	• application attack (Layer 7)

• utilizes a large/crafted payload • high bandwidth • UDP only • requires source spoofing & open resolvers • attacks source from open DNS resolvers • potential for impact to other co-located hosts	• utilizes randomized subdomains • high packet per second • TCP & UDP • no spoofing required • attacks source from upstream DNS resolvers • potential for DNS server resource exhaustion

3.1 / DNS Query Floods / This attack is problematic because it causes the target DNS server(s) to waste resources looking up the nonexistent subdomains. In cases where clients are making the requests directly, rate limiting and blocking hosts can be fairly straight forward. In other cases, these requests will be routed through shared/upstream DNS resolvers (such as ISP level resolvers or public resolvers), which do not cache NXDOMAIN records. This further complicates mitigation because a victim cannot simply rate limit or block these requesting hosts, as they risk blocking legitimate queries from real users that happen to share the same resolvers.

First and most importantly, don't place all of your eggs in one basket. When looking at your DNS needs, consider distributing your risk and having failover measures in place. In late 2016, a large DDoS attack was able to take out significant properties across the East Coast of the US due to reliance on a single DNS provider by several large organizations. This highlighted the need for a more resilient and distributed DNS landscape for many organizations.

Organizations should consider distributing their DNS needs at multiple levels including service, network, and geographic. Had the affected entities had failover measures in place and utilized multiple DNS service providers as well as ensured better geographic and network distribution, performance may have been affected but outages could have potentially been prevented.

3.2 / DNS Reflection Attacks / With reflection attacks, the primary concern is the volume of the attack traffic. If the bandwidth capacity at the targeted site is insufficient to handle the traffic that the attack is generating, then the use of a third party mitigation provider or ISP level filtering may be needed. If bandwidth is not a concern, filtering at the edge of your network should provide a viable mitigation solution depending on the service being targeted.

References:

[1]
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/dns-txt-amplification-attacks-cybersecurity-threat-advisory.pdf
https://community.akamai.com/docs/DOC-1596
https://community.akamai.com/docs/DOC-5254