Protecting Beyond DNS Flood & DDoS

Charles Chong, 2014-06-03

The recent slate of cyber-attacks involving DNS and NTP systems has again prompted questions about the comprehensiveness of DNS infrastructure's security protection. Besides mitigating volumetric attacks such as DNS flood & DDoS, many organizations have realized the need for a more comprehensive DNS security protection, which helps in preventing DNS-related security frauds and non-volumetric based attacks such as amplification and cache poisoning attacks.

On DNS Amplification & DNS Reflection Attacks

You might concur that increasing DNS performance with adequate DNS rate limiting mechanism is probably one of the best approaches to tackle the problem of overwhelming DNS traffic and DNS DoS attacks. However, this does not address the issue of DNS Amplification and DNS reflection attacks, which has been made popular through the Spamhaus-Cyberbunker attack incident. In this incident, CyberBunker took the advantage of open DNS resolvers to launch DNS amplification attacks, causing Spamhaus to be unreachable at times. DNS amplification and reflection attacks are typically sent to DNS servers as legitimate DNS request, in hope to receive large data size responses. The huge data size responses will eventually use up all the available bandwidth causing congestion to genuine DNS queries and responses. As such, DNS query rate limiting mechanism and higher QPS performance will not be able to counter the attack since the attacks typically come in small numbers of DNS requests.

One of the ways to limit such attacks is to filter the request based on query type. Typically, DNS amplification and reflection attacks will request for 'TXT' or 'ANY' Query Type which tends to return responses with significant data size. By applying bandwidth rate limit to these query type request and large-data-size query responses, we will be able to prevent bandwidth congestion caused by these attacks. Worried about the complexity of the bandwidth rate limiting solution? Well, it only takes less than 10 lines of iRules (shown as below) on F5 DNS platform to get this enforced and implemented.

```
when DNS_REQUEST {
                if { ([DNS::question type] eq "TXT") } {
                    rateclass dns_rate_shape
                }
            }
when DNS_RESPONSE {
                if { ([DNS::len] value > 512) } {
                    rateclass dns_rate_shape
                }
            }
```

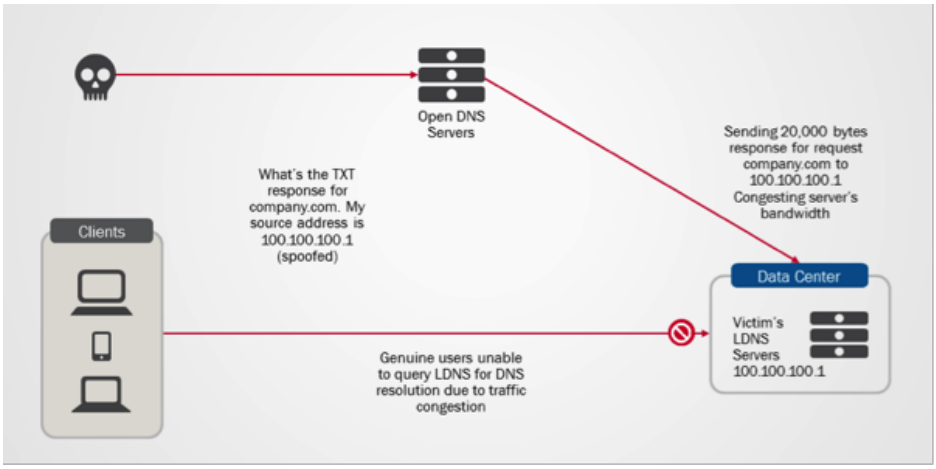

Diagram 1: DNS Reflection attacks blocking genuine users from accessing LDNS server.

Cache Poisoning Attacks

DNSSEC is poised as the eventual and ultimate solution to counter DNS cache poisoning attacks. Though the adoption rate of DNSSEC is encouraging, it takes all parties to deploy DNSSEC signing and validation to fully protect against cache poisoning. While waiting for DNSSEC adoption rate to mature, is there any interim solution to reduce or prevent cache poisoning attacks?

Based on DNS RFC standards, name servers are required to treat domain names request with case-insensitivity. In other words, the names www.foo.com and WWW.FOO.COM should resolve to the same IP address. However, most name servers will preserve the original case when echoing back the domain name in the response. Hence, by randomly varying the case of characters in domain names queried, we will be able to add entropy to requests. With this verification mechanism, the name server response must match the exact upper and lower case of every character in the name string; for instance, wWw.f5.CoM or WwW.f5.COm, which significantly reduces the success rate of cache poisoning attacks.

With F5's DNS solution, this mechanism can be enabled with just a check box on the management pane. The packet capture of the query case randomization process by F5 DNS is shown as below. As depicted in the diagram, for queries to www.google.com, F5 Cache DNS will randomize the character case of the query prior sending the query to Google's authoritative DNS server. This greatly reduces the chances of unsolicited queries matching the domain name and DNS request transaction ID, which causes the poisoning of cached DNS records.

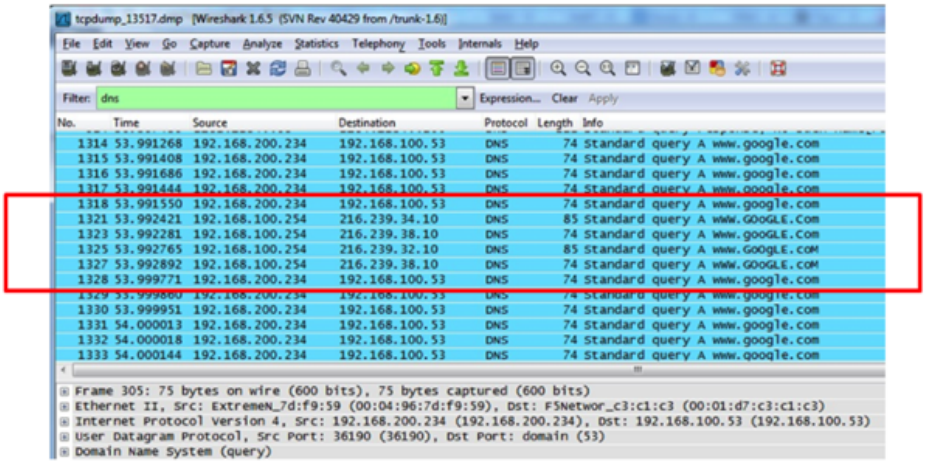

Diagram 2: Character case randomizer in F5 DNS solution dramatically reduces the possibilities of DNS cache poisoning attacks

DNS is among the hoariest of internet services that is still widely used today. Its usage continues to grow due to its simplicity and proliferation of smart devices. Hence, it is truly important that proper solution design and architecture approach are being put in place to protect the infrastructure. After all, the protection investment might be only a fraction of what you are paying for during an attack.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com