Domain Name Server (DNS) Amplification Attack

Authored by: ***ASPHostServer Administrator*** *[asphostserver@gmail.com]*

Overview A Domain Name Server (DNS) Amplification attack is a popular form of Distributed Denial of Service (DDoS), in which attackers use publically accessible open DNS servers to flood a target system with DNS response traffic. The primary technique consists of an attacker sending a DNS name lookup request to an open DNS server with the source address spoofed to be the target"s address.

ref:https://www.us-cert.gov/ncas/alerts/TA13-088A

Disabling Recursion on Authoritative Name Servers Many of the DNS servers currently deployed on the Internet are exclusively intended to provide name resolution for a single domain. In these systems, DNS resolution for private client systems may be provided by a separate server and the authoritative server acts only as a DNS source of zone information to external clients. These systems do not need to support recursive resolution of other domains on behalf of a client, and should be configured with recursion disabled.

Bind9 Add the following to the global options [8]:

```
options {
 allow-query-cache { none; };
 recursion no;
 };
 Microsoft DNS Server In the Microsoft DNS console tool [9]:
```

1. Right-click the DNS server and click Properties.
2. Click the Advanced tab.
3. In Server options, select the "Disable recursionâ€• check box, and then click OK.

Limiting Recursion to Authorized Clients For DNS servers that are deployed within an organization or Internet Service Provider, the resolver should be configured to perform recursive queries on behalf of authorized clients only. These requests typically should only come from clients within the organization"s network address range. We highly recommend that all server administrators restrict recursion to only clients on the organization"s network.

BIND9 In the global options, include the following [10]:

```
acl corpnets { 192.168.1.0/24; 192.168.2.0/24; };
options {
allow-query { any; };
allow-recursion { corpnets; };
};
```

Microsoft DNS Server It is not currently possible to restrict recursive DNS requests to a particular client address range in Microsoft DNS Server. To approximate the functionality of the BIND access control lists in Microsoft"s DNS Server, a different caching-only name server should be set up internally to provide recursive resolution. A firewall rule should be created to block incoming access to the caching-only server from outside the organization"s network. The authoritative name server functionality would then need to be hosted on a separate server, but configured to disable recursion as previously described.

Response Rate Limiting (RRL) There is currently an experimental feature available as a set of patches for BIND9 that allows an administrator to limit the maximum number of responses per second being sent to one client from the name server [11]. This functionality is intended to be used on authoritative domain name servers only as it will affect performance on recursive resolvers. To provide the most effective protection, we recommend that authoritative and recursive name servers run on different systems, with RRL implemented on the authoritative server and access control lists implemented on the recursive server. This will reduce the effectiveness of DNS amplification attacks by reducing the amount of traffic coming from any single authoritative server while not affecting the performance of the internal recursive resolvers.

BIND9 There are currently patches available for 9.8.latest and 9.9.latest to support RRL on UNIX systems. Red Hat has made updated packages available for Red Hat Enterprise Linux 6 to provide the necessary changes in advisory RHSA-2013:0550-1. On BIND9 implementation running the RRL patches, include the following lines to the options block of the authoritative views [12]:

```
rate-limit {
responses-per-second 5;
window 5;
};
```

Microsoft DNS Server This option is currently not available for Microsoft DNS Server.