BOLETIN DE ALERTA

Boletin Nro.: 2014-03

Fecha de publicación: 19/05/2014

Tema: Ataque de Reflección de DNS

Descripción:

Un ataque de amplificación o reflección de servidor de nombres de dominio (DNS) es una forma popular de denegación de servicio distribuida (DDoS), en que los atacantes utilizan los servidores DNS abiertos públicamente accesibles para inundar a la víctima con tráfico de respuesta de DNS. La técnica principal consiste en que el atacante envía una petición de resolución de nombre a un servidor DNS abierto con una dirección de origen falsa, correspondiente a la dirección de la víctima. Cuando el servidor DNS envía la respuesta, ésta es enviada a la víctima, en vez de al solicitante (el atacante). Esto se conoce como reflección DNS.

El atacante normalmente enviará la mayor solicitud de información de zona posible, para maximizar el efecto. Esto se conoce como amplificación DNS.

En la mayoría de los ataques de este tipo observados, las consultas enviadas por el atacante son del tipo "ANY", que devuelve toda la información conocida sobre una zona DNS en una única solicitud. Como el tamaño de la respuesta es considerablemente más grande que la solicitud, el atacante es capaz de aumentar la cantidad de tráfico dirigido a la víctima. Mediante el uso de *botnets* el atacante puede crear una cantidad inmensa de tráfico con poco esfuerzo.

Además, dado que las respuestas son datos legítimos procedentes de servidores válidos, es extremadamente difícil evitar estos tipos de ataques. Mientras que los ataques son difíciles de detener, los operadores de red pueden aplicar varias estrategias de mitigación.

La forma más común de este ataque implica a servidores DNS configurados para permitir la resolución recursiva sin restricciones para cualquier cliente en Internet (open resolver).

También pueden implicar a servidores de nombres autoritarios que no proporcionan resolución recursiva, el método de ataque es similar al de *resolver* recursivos abiertos, pero es más difícil mitigar ya que incluso un servidor configurado con las mejores prácticas puede ser utilizado igualmente en un ataque. En el caso de servidores autoritativos, la mitigación debe centrarse en el uso de limitación de velocidad de respuesta para restringir la cantidad de tráfico.

Impacto:
Un servidor DNS mal configurado que permite la resolución recursiva sin restricción para cualquier cliente (*Open Resolver*) puede ser explotado para participar de un ataque de denegación de servicio distribuido (*DDoS*).

Detección:
Existen diversas herramientas web públicas y gratuitas para verificar los DNS de una red en búsqueda de servidores DNS *open resolver* vulnerables. Estas herramientas escanean los rangos IP de toda la red y listan la dirección de cualquier DNS o*pen resolver* identificado.

http://www.dnsinspect.com/
http://dns.measurement-factory.com/surveys/openresolvers.html

En un ataque de amplificación de DNS, el principal indicador es una respuesta de consulta DNS sin la correspondiente solicitud previa.

Mitigación:
Debido al volumen de tráfico masivo que puede ser producido por uno de estos ataques, a menudo es poco lo que la víctima puede hacer para detener un ataque de denegación de servicio distribuido basado en amplificación DNS. Sin embargo, es posible reducir el número de servidores que pueden utilizarse por los atacantes para generar el volumen de tráfico, evitando que sus servidores sean intermediarios en este tipo de ataques.

OBS.: Las configuraciones básicas en este documento se detallan únicamente para BIND9 y Microsoft DNS Server, ya que se tratan de los más utilizados. En caso de tener un servidor DNS diferente, consultar la documentación de su vendedor para mayor información sobre las configuraciones

1) **Verificación de IP de origen**

Como las consultas DNS son enviadas por clientes controlados por el atacante deben tener una dirección de origen es un número IPV4 que no fue delegado a su organización, por eso es necesario que los proveedores de servicios de Internet rechacen cualquier tráfico DNS con direcciones falsas. El *Network Working Group* de la *Internet Engineering Task Force* lanzó BCP38 (*Best Current Practice* – Mejores Prácticas Actuales) y BCP84, documentos que describen cómo un proveedor de servicios de Internet puede filtrar el tráfico en su red para rechazar los paquetes con direcciones de origen no accesibles a través de camino del paquete actual. La implementación de las recomendaciones de este documento haría que un dispositivo de enrutamiento evalúe si es posible llegar a la dirección de origen del paquete mediante la interfaz que transmite el paquete. Si esto no es posible, se considera que el paquete tiene una dirección de origen falsificada. Estos cambios reducirían sustancialmente el potencial de los tipos de ataque DDoS más populares.

2) **Deshabilitar la recursión en DNS autoritativos**

Muchos de los servidores DNS actualmente desplegados en Internet proporcionan exclusivamente la resolución de nombres para un solo dominio. En estos sistemas, la resolución DNS para sistemas clientes privados puede ser proporcionada por otro servidor separado y el servidor autoritativo actúa únicamente como fuente de información de la zona DNS para clientes externos. Estos sistemas no necesitan apoyar una resolución recursiva de otros dominios en nombre de un cliente, por lo cual la resolución debe ser desactivada en la configuración.

BIND9

En las opciones globales, añadir lo siguiente:

```
options {
     allow-query-cache { none; };
     recursion no;
};
```

Microsoft DNS Server

En la consola de Microsoft DNS:

- Click derecho en el servidor DNS e ir a Propiedades.
- Ir a la pestaña Avanzado
- En Opciones de Servidor, seleccionar “Desactivar recursión” y Aceptar.

3) **Limitar la Recursión a clientes autorizados**

Para servidores DNS implementados dentro de una organización o proveedor de servicios de Internet, el resolver debe configurarse para permitir consultas recursivas solamente a clientes autorizados. Normalmente estas solicitudes sólo deben provenir de los clientes dentro del intervalo de direcciones de red de la organización; recomendamos que los administradores de servidor restrinjan la recursividad sólo a estos clientes.

BIND9

En las opciones globales, incluir lo siguiente:

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

Microsoft DNS Server

Actualmente no es posible restringir las consultas DNS recursivas para un rango de direcciones particular en Microsoft DNS Server. Para aproximar la funcionalidad de las listas de control de acceso en el servidor DNS de Microsoft, debe configurarse internamente un servidor sólo caché diferente para proporcionar resolución recursiva. Deben crearse reglas en el firewall para bloquear el acceso desde fuera de la red de la organización al servidor caché. El servidor DNS autoritativo tendría que estar alojado en un servidor independiente y con recursividad deshabilitada según se describió anteriormente.

4) **Response Rate Limiting (RRL)**

BIND9 permite a un administrador limitar el número máximo de respuestas por segundo que son enviadas a un cliente desde el servidor DNS. Esta funcionalidad está diseñada para ser utilizada en los servidores DNS autoritativos solamente, ya que afecta el desempeño en resoluciones recursivas. Esta propiedad reduce la efectividad y el impacto de un ataque de amplificación DNS, ya que reduce la cantidad de tráfico proveniente de otro servidor autoritativo, sin afectar el desempeño de los *resolver* recursivos internos.

Para proporcionar una protección más eficaz, recomendamos que los servidores autoritativos y los recursivos se ejecuten en sistemas diferentes, implementando RRL en el servidor autoritativo y ACL (listas de control de acceso) en servidores recursivos.

BIND9

Esta característica está disponible desde la versión 9.8. Se deben añadir las siguientes líneas entre las opciones de las vistas autoritativas:

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

Microsoft DNS Server:

Esta característica no está diponible para Microsoft DNS Server.

OBS.: La limitación del ratio de respuestas DNS (RRL) puede evitar que clientes legítimos obtengan respuestas DNS, por lo que estos clientes pueden quedar más expuestos a ataques de envenenamiento de caché DNS.

Información adicional:

http://www.securitybydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html
http://tools.ietf.org/html/bcp38
http://www.bcp38.info/index.php/Main_Page
http://cert.inteco.es/extfrontinteco/img/File/intecocert/ManualesGuias/guia_de_seguridad_en_servicios_dns.pdf
http://openresolverproject.org/

CERT-PY Equipo de Respuesta ante Emergencias Cibernéticas (CERT-py)
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Mcal. Estigarribia 1349 c/Curupayty
cert@cert.gov.py | +595 21 217 9000 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py