Ciberseguridad
UV-CSIRT

Guía de respuesta a incidentes – DDoS

1. Preparación:

El objetivo establecer contactos, definir procedimientos y recolectar información con el fin de ahorrar tiempo durante un ataque:

a. Contactar al ISP para conocer los servicios de mitigación de ataques de DDoS que ofrece y saber que proceso se debería seguir.
b. Si es posible, contratar una conexión redundante a Internet
c. Establecer contacto con tu ISP y las fuerza de justicia, asegurándose de usar una comunicación fuera de banda (ejemplo: celular)
d. Crear una whitelist de las IPs y protocolos que serán permitidos y priorizados durante el ataque.
e. Documentar los detalles de la infraestructura de TI, incluyendo dueños de los servicios, direccionamiento IP, configuración de switches y routers, preparar un diagrama de la topología de la red y un inventaría de los equipos.
f. Diseñar una buena infraestructura de red sin un único punto de falla o cuello de botella.
g. Distribuir los servidores DNS y los servicios críticos (SMTP, etc.) a través de diferentes AS.
h. Reforzar la configuración de la red, sistemas operativos y aplicaciones que podrías servir como objetivo de ataques DDoS.
i. Tener una valoración del desempeño actual de la red, para una identificación de de ataques más rápida y efectiva.
j. Verificar la configuración time-to-live TTL de los sistemas que pueden ser atacados, bajar el valor TTL de ser necesario para facilitar la redirección DNS si las IPs originales fueran atacadas, un valor TTL de 600 es un buen valor de configuración.
k. Dependiendo de la criticidad de los servicios, considerar tener un respaldo que pueda entrar en operación en caso de algún problema.
l. Establecer contactos para tus IDS , firewall, sistemas y departamento de redes
m. Colaborar con los departamentos financieros y legales para entender el impacto en estas áreas (ejemplo: pérdida de dinero), en los posibles escenarios de ataque.
n. Involucrar a los coordinadores de los planes BCP/DRP en los incidentes DDoS

2. Identificación

El objetivo es detectar el incidente, determinar su alcance e involucrar a las partes correspondientes.

Análisis del ataque

a. Entender el flujo lógico de un ataque DDoS e identificar los componentes de la infraestructura afectados.
b. Determinar si se es el objetivo principal del ataque o una víctima colateral.
c. Revisar los archivos logs de servidores, ruteadores, firewalls, aplicaciones y cualquier otro recurso afectado.
d. Identificar que aspectos del tráfico del ataque DDoS se diferencia del tráfico benigno.

-Direcciones IP fuente, AS, etc.

-Puertos destino

-URLs

-Banderas de protocolos

e. De ser posible crear firmas NIDS para facilitar la diferenciación del tráfico benigno del malicioso.

Involucrar actores internos y externos.

a. Contactar los departamentos internos para saber cuál es su visibilidad en el ataque.
b. Contactar al ISP para solicitar ayuda. Se especifico acerca del tráfico que se quiere controlar.
-Segmentos de red involucrados
-Direcciones IP fuente
-Protocolos

c. Notificar a las direcciones de administrativas y legales.

Investigar los antecedentes

a. Averigüe si se recibió una demanda de extorsión como precursor del ataque.
b. Busque si alguien tiene algún interés en amenazar a la institución
c. Competidores
d. Grupos ideológicamente motivados (hacktivistas)
e. Antiguos empleados.

3. Contención

El objetivo es mitigar los efectos del ataque en el ambiente objetivo

a. Si el cuello de botella es una característica particular de una aplicación, desactivarla temporalmente.

b. Intentar estrangular o bloquear el tráfico DDoS tan cerca de la "nube" de la red como sea posible a través de un router, firewall, balanceador de carga, dispositivo especializado, etc.

c. Termine las conexiones o procesos no deseados en servidores y routers y ajuste sus configuraciones TCP/IP.

d. Si es posible, cambie a sitios o redes alternativos utilizando DNS u otro mecanismo. Tráfico DDoS de Blackhole que apunta a las direcciones IP originales.

e. Configure un canal de comunicación alternativo entre usted y sus usuarios/clientes (por ejemplo: servidor web, servidor de correo, servidor de voz, etc.)

f. Si es posible, encaminar el tráfico a través de un servicio o producto de depuración de tráfico a través de DNS o cambios de rutas (por ejemplo: sinkhole routing).

g. Configure filtros de salida para bloquear el tráfico que sus sistemas pueden enviar en respuesta al tráfico DDoS (por ejemplo: tráfico de retroceso), para evitar añadir paquetes innecesarios a la red.

h. En caso de un intento de extorsión, trate de ganar tiempo con el estafador. Por ejemplo, explique que necesita más tiempo para obtener la aprobación de la dirección.

Si el cuello de botella está del lado del ISP, sólo éste puede tomar medidas eficaces. En ese caso, trabaje estrechamente con su ISP y asegúrese de compartir la información de manera eficiente.

4. Remediación

El objetivo es tomar medidas para detener la condición de Negación de Servicio.

a. Póngase en contacto con su ISP y asegúrese de que aplica las medidas correctivas. Estas son algunas de las medidas posibles:

-Filtración (si es posible a nivel Tier1 o 2)

- Traffic-scrubbing/Sinkhole/Clean-pipe

- Blackhole Routing

c. Si se han identificado los responsables del DDoS, considere la posibilidad de involucrar a las fuerzas del orden. Esto debe realizarse bajo la dirección de los equipos ejecutivos y legales de la institución.

Las medidas técnicas de remediación pueden ser aplicadas en su mayoría por el ISP.

5.- Recuperación

El objetivo es volver al estado funcional anterior.

a. Evaluar que la condición DDoS haya terminado

-Asegurarse de que los servicios afectados sean accesibles de nuevo.

-Asegurarse de que el rendimiento de la infraestructura vuelva a su operación inical.

b. Remover las medidas de mitigación

- Regresar el tráfico a su red original.
- Reiniciar los servicios interrumpidos.

Asegurarse que las acciones relacionadas con la recuperación se decidan de acuerdo con los departamentos de TI. El levantamiento de los servicios podría tener efectos secundarios inesperados.

6.- Repercusiones

El Objetivo es documentar los detalles del incidente, discutir las lecciones aprendidas y reajustar los planes y las defensas.

a. Considerar qué pasos de preparación que se podrían haber tomado para responder el incidente de una manera más rápida o eficazmente.
b. Si es necesario, ajustar las suposiciones que afectaron las decisiones tomadas durante la preparación de incidentes de DDoS.
c. Evalúe la efectividad de su proceso de respuesta DDoS, involucrando a personas y comunicaciones.
d. Considere qué relaciones dentro y fuera de su organización podrían ayudarle con futuros incidentes.
e. Colaborar con equipos legales si una acción legal está en proceso.