Manual para la mitigación de DDoS

Alcance de DDoS: infraestructura del DNS para ccTLD

Taller de TLD-OPS

Versión 1.0 - 25 de abril de 2018

Descripción general del taller

El objetivo del taller fue explorar la manera en la que los miembros de TLD-OPS pueden colaborar para elaborar un Manual para la Mitigación de DDoS. El taller se basó en DDoS orientado a la infraestructura del DNS autoritativa y anycast, operada por los ccTLD y sus socios proveedores del DNS.

Motivación

Este taller se creó en respuesta al taller de mitigación de DDoS de TLD-OPS llevado a cabo en ICANN58 en Copenhague el 12 de marzo de 2017. Dado que los ataques de DDoS pueden ocasionar un grave impacto en el objetivo (y posiblemente daño colateral a otros), el Comité Permanente de TLD-OPS considera que es importante utilizar la experiencia colectiva de la comunidad de TLD-OPS para elaborar y documentar un marco a fin de preparar mejor a los ccTLD para responder ante ataques de DDoS.

El taller permitió este diálogo al compartir experiencias, debates y generación de ideas.

Taller sobre Mitigación de DDoS de TLD-OPS N.° 2 - ICANN61, 29-10-2017, observaciones generales

Tuvimos un grupo más reducido para este taller: 22 personas. Esto permitió un buen nivel de dinámica y colaboración. Nos reunimos frente a un solo rotafolio, analizamos los resultados del taller anterior y ampliamos cada tema para centrarnos en los elementos que formarían parte del manual, para cada etapa del ciclo de vida. Los resultados que se capturaron en el rotafolio se plasman en este documento.

Los ciclos de vida para una mitigación de DDoS eficaz son los siguientes:

- Identificar
- Proteger
- Detectar
- Responder
- Recuperar

El alcance de este documento no consiste en elaborar un marco de seguridad complejo para la mitigación de DDoS. El objetivo es resaltar los componentes importantes en cada ciclo de vida para que un ccTLD sea eficaz en la mitigación de un ataque de DDoS (si es implementado y, de ser así, cuándo).

Se mencionó en el taller que siempre es una buena idea implementar mejores prácticas como Operaciones de Servicios de TI (ITIL) y Gestión de Seguridad de la Información (ciberseguridad).

IDENTIFICAR:

El objetivo de IDENTIFICAR es documentar y entender la infraestructura del DNS de su ccTLD antes de que se produzca un ataque -- para saber a quién llamar, en quién confiar, a quién notificar (y la vía de escalonamiento para la resolución de problemas). Asegúrese de tener una relación sólida con sus ISP, proveedores, el gobierno, la prensa, los registratarios y los usuarios de Internet de su ccTLD. Este es el trabajo que debe llevarse a cabo de manera continua antes de que ocurra un ataque.

CONTACTOS	
Su equipo de gestión de ccTLD	Cargo, nombre, número de teléfono, número de teléfono particular, correo electrónico personal (Presidente - Junta Directiva)
Número de emergencia de la IANA	+1 (310) 306-6308 (a ser actualizado)
Proveedores de anycast	Correo electrónico y números de teléfono, números de contacto de SoC/NoC
ISP de tránsito ascendente	Correo electrónico y números de teléfono, números de contacto de SoC/NoC
ISP dentro del país	Correo electrónico y números de teléfono de SoC/NoC
CERT	Correo electrónico y números de teléfono de SoC/NoC Nombre, número de teléfono y correo electrónico de contacto
Operadores de resolutores principales (recursivos)	Direcciones IP Operador, correo electrónico y números de teléfono
Lista de contactos de TLD-OPS	Acceso a la lista de contactos de TLD-OPS
Prensa	Nombre, número de teléfono y correo electrónico de contacto
Regulador	Nombre, número de teléfono y correo electrónico de contacto
Proveedores de software	Nombre, número de teléfono y correo electrónico de contacto
Consultor forense	Nombre, número de teléfono y correo electrónico de contacto
Registratarios	Método para comunicarse con los registratarios eficazmente
Otros contactos relevantes	

Documente claramente la infraestructura del DNS de su ccTLD:

Es de suma importancia que documente claramente la infraestructura del DNS de su ccTLD, qué servidores de nombres tiene en funcionamiento, su ubicación física, las conexiones de red, los

proveedores de tránsito, las conexiones IXP, los proveedores de anycast, la capacidad de cada tránsito y enlace de IXP.

Este es el activo que usted debe proteger.

Servidor de nombre de ccTLD, direcciones IPv4 e IPv6.

```
Example…
;; AUTHORITY SECTION:
dk.                     172800  IN      NS      a.nic.dk.
dk.                     172800  IN      NS      b.nic.dk.
…
;; ADDITIONAL SECTION:
a.nic.dk.               172800  IN      A       212.88.78.122
b.nic.dk.               172800  IN      A       193.163.102.222
b.nic.dk.               172800  IN      AAAA    2a01:630:0:80::53
…
```

Topología adecuada del DNS, la red y el servidor:

Documente la arquitectura de red, servidor y software para la infraestructura del DNS de su ccTLD, y actualícela en forma regular.

<Inserte diagramas de red aquí>

- Proporcione enlaces a diagramas de topología y red

Direcciones IP maestras ocultas

Dirección IP	
maestra oculta	Detalles de lista de acceso (en caso de que necesite agregar un nuevo proveedor)
Cómo agregar	Pasos rápidos para agregar un nuevo servidor de nombre...

Infraestructura de firma de las DNSSEC

Agregue detalles de su infraestructura de las DNSSEC y protección/almacenamiento de claves aquí.

Servidores de nombres recursivos importantes que usan su ccTLD (un ejemplo sería servidores de nombres recursivos de grandes ISP en su país que brindan servicio a una población grande)

Nombre de ISP	
recursivo	Direcciones IP
Cómo incluir en la lista blanca	¿Pasos rápidos para incluir en la lista blanca a algunos recursivos?

Mantenga su información actualizada:

Acceso a información importante	
Contraseña segura	Ubicación (para iniciar sesión en enrutadores y servidores)
Inventario de equipos	Ubicación (cuál es la dirección IP, nombre)
Plan de comunicaciones	Ubicación (cómo nos ponemos en contacto, comunicamos)
Roles y responsabilidades	Ubicación (quién hace qué y cuándo)
Planes de DR, BCP	Ubicación

Proceso de gestión de riesgos:

Identifique riesgos y el impacto asociado, y la probabilidad de que ocurran, y ubique esto en el análisis de impacto comercial para los servicios de resolución de ccTLD. Cree un proceso para revisar y actualizar periódicamente este documento.

Proceso de gestión de cambios:

Resulta vital que esta información esté actualizada; implemente procesos para mantener actualizada esta información. Cree un proceso trimestral para revisar y actualizar este documento.

PROTEGER:

El objetivo de PROTEGER es elaborar e implementar las medidas de protección adecuadas para garantizar la prestación de servicios del DNS autoritativos de su ccTLD, y para permitir la capacidad de contener o limitar el impacto de un ataque de DDoS.

Específicamente contra ataques de DDoS, el resultado de PROTEGER es elaborar e implementar mejores prácticas de seguridad tales como controles de acceso, tecnologías de protección, diversidad e infraestructura del DNS. Esta sección se centra en identificar las mejores prácticas (procesos) en materia de seguridad para tecnología, personas y socios.

Tecnología:

Implemente medidas de protección para garantizar operaciones seguras y estables.

Listas de acceso:

- ACL, donde resulte pertinente, solo permiten acceso a puerto de destino 53 (TCP/UDP)
- ACL para gestión fuera de banda

Anycast:

- Implementación de topología del DNS de anycast global para aumentar la flexibilidad de la entrega
- Implementación de nodos locales anycast para aumentar la flexibilidad de la entrega (Nodos del DNS sin tránsito global), preferentemente mediante:
    - Extensión de su DNS de anycast global con nodos locales anycast que prestan servicio a una comunidad de resolutores 'importantes' específicos (principalmente en redes regionales, gubernamentales e ISP de país)
    - Adición de nodos locales anycast en IXP principales

Otras medidas de protección:

- Diversidad de software de servidor del DNS (BIND, NSD, Knot, etc.)
- Filtrado de agujero negro accionado remotamente (RTBH)
- Hardware para mitigación de DDoS
- Implementación de RRL (indispensable)
- Protección de interfaz de gestión (cable/puerto físico independiente, tránsito, túnel VPN, ...)
- Suficientes recursos de sistema (desde la perspectiva de capacidad)
- Suficiente conectividad de la red y diversificación en la selección de proveedor de servicio (ISP, IXP, etc.)

Personas/Proceso:

Capacite al equipo de TI

- Capacitaciones sobre conocimientos de seguridad
- Ejercicio anual <- compartir código de escritura sobre simulación de ataque de DDoS y TLD-OPS
- Fortalecimiento de la configuración (mejor práctica, ...) y pruebas de penetración
- Cómo usar herramientas de supervisión externa del DNS (¿por ej., DNSMON, DNS-OARC, BGPMon o similar?)
- No realice cambios manuales, use proceso de gestión de cambios y configuración

Trabaje con los ISP (proveedores de tránsito) con anticipación

- Averigüe cómo ellos pueden ayudar a mitigar futuros eventos de DDoS

- Asegúrese de que entiendan la importancia de su ccTLD

Socios:

Trabaje con los socios donde los servicios de mitigación de DDoS pueden ser útiles:

- Agregue proveedores externos de anycast de manera permanente
- Asegúrese de contar con proveedores externos de anycast de emergencia
- Investigue servicios de limpieza de DDoS

DETECTAR:

El objetivo de DETECTAR es elaborar e implementar las actividades adecuadas para identificar, de manera oportuna, la ocurrencia de un ataque de DDoS y para determinar el alcance y la envergadura de los ataques de DDoS. Cuanto mejor sea el mecanismo de detección más eficaces podrán ser las técnicas de mitigación.

Los resultados de DETECTAR son procesos de detección y monitoreo internos y externos del DNS.

Monitoreo:

Monitoreo interno

- Monitoreo del tráfico de SNMP (enrutador, servidores, enlaces)
- Flexibilidad de notificación de alarmas de umbrales (sms, correo electrónico
- Comprensión del funcionamiento normal de cada nodo.
- Herramientas de análisis del DNS
- PCAP Capture (ofrece un panorama completo cuando ocurre el incidente, pero los volúmenes de tráfico pueden crear un DoS interno al momento de un ataque de DDoS, véase nota más abajo)

Monitoreo externo

- RIPE Atlas DNSMON externo (tiempo de respuesta de consulta del DNS, tendencias y pérdida de consultas)
- Estadísticas de enlaces de tránsito de ISP (uso real de tráfico saliente a su nodo del DNS)
- Monitoreo de SLA de la ICANN (API del Sistema de Monitoreo de la ICANN (MoSAPI)) (aún en adopción temprana para los ccTLD)
- Netlabs 360 - https://ddosmon.net/

Herramientas escalables (funcionales en el modo de DDoS)

- PCAP, algunas herramientas pueden colapsar en el caso de ataques de DDoS o afectar negativamente las operaciones
    - Procedimiento para desactivar temporalmente la recopilación de datos en condiciones adversas
    - Envío remoto de registros en tiempo real para garantizar que no se pierdan datos

Identificación del tipo de ataque:

Comprensión del ataque

- Tipo de ataque
- Lista de ataques clásicos, perfil, herramientas y mitigación
- Origen (¿de dónde proviene?)
- Qué nodos (¿a qué afecta?)
- ¿Cuál es el impacto real en los usuarios de Internet?

RESPONDER:

El objetivo de RESPONDER es elaborar e implementar las actividades adecuadas para tomar medidas respecto de un ataque de DDoS detectado. La función de respuesta respalda la capacidad de mitigar el impacto de un posible evento de DDoS.

El resultado de RESPONDER incluye planificación de respuesta, comunicaciones, análisis y mitigación.

Planes de respuesta:

¡No entre en pánico! La comunidad probablemente detecte la ocurrencia de un ataque de DDoS en su ccTLD al mismo tiempo que usted, y la comunidad deseará que la ayude a mitigar el ataque.

- Comuníquese
- Continúe con el análisis
- Resuelva el problema
- Céntrese en el núcleo del problema
- Documente {cambios que realiza y observaciones}

Plan de comunicaciones:

La comunicación es clave en la mitigación del ataque.

Mecanismos de comunicación	
CERT local	Póngase en contacto con el CERT local incluso si el ataque no está totalmente identificado
TLD-OPS	Envíe un mensaje de correo electrónico a tld-ops@dns-oarc.net Solicite ayuda con mayor identificación del ataque
Línea de teleconferencias	Solicítele a TLD-OPS/ICANN que abra una línea de teleconferencias para colaborar en la mitigación
Difusión y alcance	Solicite/autorice a los miembros de TLD-OPS que comuniquen en grupos/lista de correo electrónico alternativos para ayudar en la mitigación del ataque
otro	

RECUPERAR:

El objetivo de RECUPERAR es elaborar e implementar las actividades adecuadas para mantener planes para flexibilidad y para restaurar las capacidades o los servicios que se vieron afectados por un ataque de DDoS. La función de recuperación respalda la restauración oportuna a las funciones normales para reducir el impacto de un ataque de DDoS.

Los resultados de RECUPERAR incluyen planificación de recuperación, mejoras, lecciones aprendidas y comunicaciones.

Recuperación:

- Realice reversión de las medidas temporales
- Restaure la infraestructura del DNS al estado original
- Documente los cambios permanentes
- Compile notas

Lecciones aprendidas:

- Lleve a cabo una reunión después del incidente con las partes interesadas (internas) relevantes
- Documente:
    - Qué funcionó
    - Qué no funcionó
    - Determine mejoras

Mejoras:

- Identifique
- Evalúe
- Comparta
- Implemente mejoras

Comunicaciones:

- Comuníquese con socios, clientes, empleados, registratarios