Grupo de Trabajo de Mensajería, Malware y Antiabuso en Móviles
Recomendaciones iniciales del M3AAWG: Armar a las empresas contra los ataques DDoS

Marzo de 2017

La URL de referencia de este documento: www.m3aawg.org/DDoS-Recommendations-Business

Índice de contenidos

Introducción 1
Ataques DDoS 1
Preparación antes de que se produzcan los ataques 2
Durante un ataque 5
Después de un ataque 5
Conclusión 6
Referencias 6
Glosario 7

Introducción

Los ataques de denegación de servicio distribuido siguen siendo una gran preocupación para las empresas que dependen de Internet para el correo electrónico, el marketing, el comercio y el almacenamiento de datos. Los trastornos causados por los ataques de denegación de servicio distribuido (DDoS) van desde la pérdida de ingresos y el aumento de los costes hasta el daño dramático a la marca. Esta guía proporciona conceptos e ideas para ayudar a las empresas a prepararse para los ataques DDoS. Como beneficio secundario, algunas de estas mismas técnicas también pueden ayudar a las empresas que de repente ven un gran aumento en el tráfico de clientes legítimos a sus sitios web.

Ataques DDoS

Los ataques de denegación de servicio distribuidos (DDoS) abarcan una amplia variedad de técnicas y pueden ir desde ataques volumétricos de capa 3 de IP hasta ataques de aplicación de capa 7. Las fuentes de los ataques se extienden desde los sistemas comprometidos que envían directamente el tráfico de ataque hasta las fuentes reflexivas no comprometidas que responden a paquetes IP falsos.

Los ataques DDoS pueden dividirse en cuatro categorías principales:[1]

- Volumétrico
- Aplicación
- Agotamiento del Estado
- Plano de control

Hay docenas de tipos de ataques dentro de estas cuatro categorías principales. La gran mayoría de los ataques DDoS aprovechan sistemas informáticos comprometidos que están bajo un sistema central de mando y control. Estos

1 Fonash y Glenn 2014

Los ordenadores infectados se denominan generalmente "bots". Una red de bots bajo un único sistema de mando y control se denomina "botnet". Las organizaciones de seguridad sin ánimo de lucro rastrean miles de botnets que operan en Internet en cualquier momento. [2]

Los ataques DDoS volumétricos pueden proceder de fuentes directas o de un servicio de reflexión en el que la IP de origen del paquete se falsifica con la dirección IP de la víctima. Normalmente, los delincuentes aprovechan los servicios de reflexión para amplificar el tráfico de ataque y aumentar considerablemente el tamaño del mismo. Hasta hace poco, los mayores ataques volumétricos vistos en Internet hasta la fecha eran ataques DDoS de amplificación reflexiva. Sin embargo, los ataques directos desde un gran número de dispositivos IoT inseguros han hecho que los mayores ataques DDoS superen el umbral de 1 Tbps. [3]

Los ataques también pueden clasificarse como **directos** o **indirectos**. Los ataques directos se dirigen a una víctima (diferente de las fuentes directas descritas anteriormente), mientras que los ataques indirectos se dirigen a servicios de red críticos que la víctima necesita para que su servicio funcione. Un ejemplo de este tipo de ataque es que el malhechor se dirija al servicio autoritativo o recursivo del DNS que utiliza la víctima.

En general, los **ataques a nivel de aplicación** son ataques de menor volumen; aprovechan los ordenadores comprometidos para enviar peticiones a nivel de aplicación a los sistemas con el fin de sobrecargar a la víctima con peticiones que parecen legítimas. Los ataques pueden ir hacia adelante o hacia atrás. Un ataque a nivel de aplicación hacia adelante puede tratar de abrumar a un servidor web enviando un gran número de solicitudes de búsqueda de uso intensivo de CPU y memoria al sitio web, mientras que un ataque a nivel de aplicación hacia atrás podría hacer un alto número de solicitudes de documentos de gran tamaño ubicados en el sitio web con el fin de consumir todo el ancho de banda disponible del sitio web.

Recientemente se observó un nuevo tipo de ataque de gran volumen a nivel de aplicación que comenzó el 18 de marzo de 2015.[4] Apodado el "Gran Cañón", se trataba de un ataque del tipo "man-on-the-side". Después de que se modificara el código JavaScript analítico del motor de búsqueda chino Baidu, las solicitudes de sitios web legítimos entraban en las redes chinas y enviaban solicitudes de ataque desde ordenadores no comprometidos que utilizaban el código modificado. Este tipo de ataque es inusual; debe ser realizado por un operador de red o por una organización que tenga acceso a la mayor parte del tráfico de red que transita por las redes de los operadores.

Otra forma de ataque indirecto tiene como objetivo el servicio DNS de un ISP. El objetivo pueden ser los servidores recursivos o los autoritativos, lo que puede causar interrupciones a gran escala en los clientes. La interrupción del servicio DNS puede tener un amplio impacto en la base de clientes de un ISP o proveedor de DNS.

Preparación antes de que se produzcan los ataques

Las empresas deben tomar medidas para prepararse para los ataques DDoS que podrían afectar significativamente a sus actividades. Estos pasos incluyen preparaciones internas para sus redes y servidores junto con servicios adicionales de mitigación de DDoS de su ISP o de una empresa dedicada a la mitigación de DDoS. Los pasos que se enumeran a continuación son directrices generales y variarán en función del tamaño de la empresa, el tamaño de la red de la empresa (incluida la capacidad de enlace ascendente de Internet) y el nivel de conocimientos de DDoS de los empleados.

Apoyo a la gestión

Probablemente, el primer paso más importante en la preparación para un ataque DDoS es conseguir la participación de la dirección. Calcule el impacto empresarial que se produciría si un ataque DDoS afectara a las operaciones de la empresa. ¿Cuánto tiempo pueden estar fuera de servicio antes de que se produzcan diferentes niveles de impacto en los clientes? ¿Qué ocurre si los clientes no pueden

---

2https://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts

3 "Mapeo de Mirai: A Botnet Case Study", 2016.

4"Uso de Baidu para dirigir millones de ordenadores para lanzar ataques de denegación de servicio", 2015

¿pagar sus facturas o pedir productos? ¿Cuál es el impacto de que el correo electrónico de los empleados y la conectividad a Internet estén fuera de servicio durante un periodo prolongado de tiempo? ¿Tiene la empresa comunicaciones fuera de banda? Recuerde: durante un ataque DDoS, el servicio telefónico VoIP que funciona en el mismo circuito de Internet no funcionará.

Evaluar los servicios dependientes de Internet

El siguiente paso que debe dar una empresa es una evaluación de todos sus servicios que dependen de Internet. Hay que considerar el impacto y la posible pérdida de ingresos que experimentaría la empresa si estos servicios dejaran de estar disponibles. Los servicios típicos son:

- Portales web de comercio electrónico orientados al cliente: para muchos sectores, estos sitios pueden afectar significativamente a los ingresos de la empresa si no están disponibles para los clientes
- Sistemas de correo electrónico corporativo
- Sistemas DNS corporativos orientados a Internet
- Sistemas de acceso remoto de los empleados
- Redes VPN que podrían verse afectadas por ataques DDoS en Internet

Las empresas deben evaluar el impacto que la pérdida de estos sistemas tendría sobre los ingresos y la productividad de los empleados.

Establecer sistemas de supervisión de ataques DDoS

En el caso de los servicios importantes o críticos que se conectan a Internet, deben existir sistemas para supervisar los ataques DDoS y realizar el registro y la captura de paquetes cuando se producen los ataques. Durante las primeras etapas de un ataque, la información sobre el mismo puede ayudar a los esfuerzos de mitigación. La capacidad de ver las solicitudes web, las solicitudes de conexión, los registros del cortafuegos, los registros de IPDS y realizar la captura de paquetes completos en el tráfico entrante permitirá a la empresa y a su proveedor de mitigación de DDoS tener una idea del tráfico de ataque. Además, la supervisión de los ataques DDoS por parte del proveedor de servicios de la empresa puede ser muy útil.

Puntos clave a recordar:

1. Captura la fecha y la hora de todos los registros y capturas de paquetes.
2. Ejecute un cliente NTP en sus sistemas para asegurarse de que tiene tiempos precisos.
3. Capturar las direcciones IP de origen de los paquetes infractores.
4. Cuando sea posible, realice una captura de paquetes completos del tráfico de ataque.

Preparación del sitio de comercio electrónico

Las organizaciones que pueden verse afectadas de forma significativa por un ataque a su infraestructura web de comercio electrónico deben preparar el sitio para un ataque DDoS. Esta preparación incluye:

- Priorizar las funciones más importantes del sitio
- Creación de un plan en el que el sitio pueda operar en un estado de funcionalidad mínima para servir a las funciones más importantes, al tiempo que se eliminan características para que el sitio web sea más resistente a los ataques DDoS o al agotamiento de los recursos

Los ataques DDoS vienen en muchas variedades. Cosas a tener en cuenta para un sitio web minimizado:

- **Reducción o eliminación de la funcionalidad dinámica**. Las funciones de búsqueda, las páginas web generadas dinámicamente y cualquier funcionalidad que requiera el acceso a recursos de back-end, como las bases de datos, facilitan que un atacante agote los recursos de CPU, disco o memoria. Incluso un sitio web diseñado para ser mejorado con CDN (Content Delivery Networks) o un servicio de mitigación de DDoS no funcionará si el atacante encuentra una URL que sólo puede ser servida por un único recurso back-end dinámico. En la medida de lo posible, presente a los clientes contenidos web estáticos que seguirán siendo servidos si son atacados, especialmente la página principal.

- **Gráficos reducidos. Los** gráficos de menor tamaño o la eliminación de la mayoría de los gráficos pueden ayudar a que los servidores web funcionen con mayor eficacia durante un ataque.

- **Limitar el acceso a documentos o archivos de gran tamaño.** Un tipo de ataque DDoS consiste en realizar miles de solicitudes desde el sitio web para documentos de gran tamaño. Esto puede inundar el enlace ascendente del sitio web e interferir con otro tráfico legítimo.

- **Limitar el número de conexiones entrantes permitidas al sitio web.**

No todos los eventos de gran volumen son ataques DDoS. Un enlace desde un sitio web muy visitado al sitio web de una organización también puede parecer un ataque. [5]

Como beneficio inesperado, toda esta preparación también puede ayudar a las empresas a gestionar grandes aumentos repentinos de tráfico *legítimo*.

Preparación de la red y del servidor

Se debe considerar un trabajo de preparación adicional que incluya:

1. Añadir más capacidad local (ancho de banda o servidores) al servicio atacado.

2. Desplegar dispositivos de mitigación específicos para DoS/DDoS basados en las instalaciones y/o utilizar capacidades antiDoS en el hardware local. Esto puede incluir equilibradores de carga, depuradores de datos DDoS locales, servidores DNS con capacidades de mitigación DDoS y otros dispositivos especializados.

3. Coordinación con los proveedores de software y hardware para orientar la configuración óptima de los dispositivos.

4. Utilizar las redes de distribución de contenidos (CDN) para ayudar a mitigar los ataques mediante la distribución de los volúmenes de ataque a través de una amplia infraestructura de CDN.

5. Considerar un servidor de correo electrónico secundario o terciario fuera del sitio para almacenar el correo electrónico durante un ataque y para su recuperación fuera del sitio.

6. Garantizar que el tráfico del plano de control de la red tenga prioridad sobre el tráfico DDoS.

7. Garantizar que el tráfico de gestión de la administración del sitio web se transmita en una red fuera de banda y en una(s) interfaz(es) de servidor que no se vea(n) afectada(s) por el tráfico de ataque DDoS, o que se establezca una priorización adecuada de la calidad de servicio (QoS) y de las listas de control de acceso (ACL) del tráfico de gestión para garantizar que el sitio web pueda ser gestionado durante un ataque.

8. Disminuir los TTL de los DNS de la empresa para poder cambiar rápidamente las direcciones IP si planea utilizar técnicas de blackhole para mitigar un ataque.

No sea parte del problema. Encuentre cualquier servidor NTP o DNS y otros servicios basados en UDP que no deberían estar expuestos externamente y elimínelos de la red o ubíquelos en una red interna para que estos servicios no participen en los ataques DDoS reflexivos.

5https://en.wikipedia.org/wiki/Slashdot_effect

Proveedores de mitigación DDoS de terceros
La preparación in situ no puede defenderse de los ataques volumétricos a gran escala que son mayores que el ancho de banda de la conectividad de su red a Internet. Estos ataques deben ser mitigados por su ISP, proveedor de alojamiento o proveedor de mitigación DDoS de terceros. Planifique con antelación y disponga de un servicio de mitigación antes de un ataque real. Además, algunos servicios de mitigación de tráfico de ataque funcionan mejor si el tráfico normal se basa antes del ataque. Es mejor negociar los contratos legales y de precios antes de un ataque.

Coordinación con los recursos centrales
Las empresas deben identificar proactivamente y haber contactado con los puntos de contacto apropiados en organizaciones externas antes de un ataque DDoS, incluyendo:

- ISP ascendente
- Proveedor de mitigación de DDoS de terceros
- Agencia policial
- Equipo Nacional de Respuesta a Emergencias de la Comunidad (CERT)
- Proveedor de alojamiento
- Otras organizaciones que pueden ayudar antes, durante y después de un ataque DDoS.

Probar la preparación de la empresa
Ponga a prueba la preparación de la empresa para ver lo bien que se ha planificado. Empiece con un ejercicio en papel para ver si la organización está realmente preparada para un ataque. ¿Cómo se pondrán en contacto con los clientes? ¿Estará el grupo de comunicación preparado para distribuir un comunicado de prensa sobre el asunto? ¿Qué mitigaciones se desplegarán para detener o reducir el ataque?

Durante un ataque

- **Capturar el tráfico de ataque**
  Esté preparado para capturar el tráfico durante el ataque. Las capturas de paquetes completos pueden proporcionar una gran información sobre el ataque y la naturaleza cambiante de un ataque.
- **Aplicar estrategias de mitigación**
  En función de las características del ataque, aplicar las estrategias de mitigación predefinidas. Estas pueden incluir:
  - cambios en el sitio web
  - filtrado y cambios en las entradas DNS
  - depuración previa con el ISP de la empresa o con un servicio de mitigación de DDoS de terceros
  - depuración de datos in situ.

Después de un ataque

Compartir el código hostil/de ataque capturado, las tácticas, las técnicas, las fuentes de ataque y los procedimientos con otras organizaciones que puedan experimentar tipos de ataques similares y con organizaciones de coordinación central como las organizaciones nacionales CERT, las organizaciones de intercambio de información y las posibles fuerzas de seguridad, cuando proceda. Trabajar con el operador de la red, el proveedor de alojamiento, la organización de intercambio de información o el CERT nacional para identificar los ordenadores atacantes y limpiar las máquinas en el extremo distante para minimizar la posibilidad de futuros ataques.

Conclusión:

Los ataques DDoS seguirán afectando a muchas empresas y usuarios de Internet en un futuro previsible. Las empresas que no se preparan para los ataques podrían experimentar un impacto sustancial en las operaciones, los clientes y, en última instancia, la pérdida de ingresos. Las empresas que se preparan para los ataques DDoS pueden reducir significativamente estos impactos. Una planificación y preparación adecuadas en coordinación con los proveedores de servicios no sólo puede ayudar a mitigar los ataques, sino que también puede preparar a las empresas para manejar mejor los aumentos legítimos de tráfico en el sitio web.

Referencias

Fonash, Peter, y Michael Glenn. "Remediation of Server-Based DDoS Attacks Final Report". Communications Security, Reliability and Interoperability Council (CSRIC) IV Working Group Report, FCC, Washington DC: FCC. http://docplayer.net/16237406-September-2014-working-group-5-remediation-of-server-based-ddos-attacks-final-report.html

"Mapeo de Mirai: Un caso de botnet". 3 de octubre de 2016. Consultado el 7 de octubre de 2016. https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fiflield, Sarah McKune, Arn Rey, John Scott-Railton, Ronand Deibert y Vern Paxson. 10 de abril de 2015. "El gran cañón de China". *Laboratorio del ciudadano.* Universidad de Toronto. Consultado el 3 de septiembre de 2015. https://citizenlab.org/2015/04/chinas-great-cannon/

"Uso de Baidu para dirigir millones de ordenadores para lanzar ataques de denegación de servicio". 25 de marzo de 2015. Consultado el 3 de septiembre de 2015. https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1.h

Glosario

AntiDoS	Técnicas y dispositivos utilizados para mitigar los ataques DoS/DDoS.
Agujero negro/escaparazón	También conocido como "enrutamiento nulo", el tráfico de red de blackholing deja caer el tráfico malicioso en un router correctamente configurado. El ISP o el cliente envía un anuncio de ruta que identifica la dirección IP de destino que se va a descartar. Ese anuncio puede hacer caer el tráfico a través de un grupo de enrutadores configurados como agujeros negros. Una variante de esta técnica puede eliminar el tráfico basándose en la dirección IP de origen. Los ISP han descubierto que esta técnica es menos eficaz debido a: a.) el gran número de direcciones IP de origen atacantes en un ataque DDoS normal; b.) las limitaciones de los routers; y c.) los daños colaterales derivados de la caída inadvertida de tráfico legítimo].
Bot	Un dispositivo infectado con software malicioso que puede ser controlado a distancia.
Botnet	Un grupo de bots que son controlados a distancia por una sola entidad.
CERT	Equipo de respuesta a emergencias informáticas.
Redes de distribución de contenidos (CDN)	Un sistema de servidores distribuidos geográficamente que replican archivos y contenidos y los entregan a los usuarios finales desde el servidor más cercano o mejor. Una CDN puede ayudar a distribuir y minimizar el impacto de los ataques DDoS, especialmente en el tráfico web.
Depuración de datos	Actividad en la que un servidor diferencia entre el tráfico legítimo y el tráfico ilegítimo de ataque, descartando el tráfico ilegítimo y permitiendo al ISP entregar el tráfico legítimo al destino apropiado.
Denegación de servicio (DoS) **Ataque**	Tráfico malicioso que intenta denegar el acceso a los recursos de la red, el servidor o la aplicación.
Ataque de denegación de servicio distribuido (DDoS)	Un ataque DoS en el que el tráfico de ataque proviene de (se distribuye a través de) múltiples fuentes, que pueden ser cualquier cosa, desde ordenadores hasta smartphones o dispositivos conectados al IoT.
Sistema de nombres de dominio (DNS)	Un servicio crítico de Internet que traduce los nombres alfanuméricos a direcciones IP.
Proveedor de servicios de Internet (ISP)	Empresa u organización que proporciona acceso a Internet a sus abonados.
Protocolo de Internet (IP)	El principal protocolo utilizado para entregar paquetes a través de Internet.
Internet de los objetos (IoT)	Término utilizado para describir la adición de conectividad de red a una variedad de objetos físicos para la comunicación local o la comunicación a través de Internet. Algunos ejemplos de dispositivos son las bombillas, los frigoríficos, las lavadoras, los equipos de fitness domésticos, los vehículos, las señales de tráfico, los sensores de humedad del suelo y muchos más. Las principales categorías de dispositivos IoT son las de consumo, ciudades inteligentes, industriales, sanitarias, gubernamentales y financieras, entre otras.
Sistema de detección de intrusos (IDS)	**Sistema de prevención de intrusiones (IPS)**

Un sistema de detección de intrusiones (IDS) supervisa las redes o los sistemas en busca de actividades maliciosas o inusuales. Un sistema de prevención de intrusiones (IPS) tiene la capacidad de detener, bloquear o responder a los paquetes identificados. Un IPDS (o IDPS) combina un IDS y un IPS.

Protocolo de tiempo de red (NTP)	Un protocolo utilizado para sincronizar los relojes a través de Internet y otros paquetes. redes conmutadas.
Ampliación reflexiva Negación distribuida de Servicio (DDoS) Ataque	Un ataque DDoS en el que la dirección de origen de los paquetes IP se cambia de la remitente real a la dirección IP de la víctima. Los paquetes IP se envían entonces a un servicio en Internet que amplifica su efecto. Los paquetes IP originales se "reflejan" del servicio legítimo y la respuesta va a la víctima del ataque DDoS, inundándola con paquetes IP que no solicitó. Los protocolos vulnerables más comunes son DNS, NTP, SSDP, SNMP y aproximadamente otros 10. Algunos de los mayores ataques DDoS vistos en Internet han utilizado esta técnica.
Tbps	Terabits por segundo
Tiempo de vida (TTL)	Un campo en la cabecera del paquete IP. El campo TTL normalmente se disminuye en cada IP router. Cuando el TTL del paquete IP llega a cero, el router descarta el paquete. De esta forma se evitan los bucles de enrutamiento en los que el paquete hace un bucle eterno.
Control de la transmisión Protocolo (TCP)	Un protocolo de red que se ejecuta sobre el protocolo IP para proporcionar una método de entrega de paquetes de datos ordenados.
Protocolo de datagramas de usuario (UDP)	Un protocolo de red que se ejecuta sobre el protocolo IP para proporcionar paquetes para aplicaciones tolerantes a las pérdidas. Un ejemplo de aplicación es una transmisión de televisión.
Voz sobre IP (VoIP)	Un grupo de tecnologías y protocolos para la entrega de voz y multimedia comunicaciones a través de una red de conmutación de paquetes como Internet.
Red privada virtual (VPN)	Una red privada que aísla los paquetes que transitan por una red pública como la internet. Una VPN puede hacer que parezca que el usuario o el sistema está conectado a una red privada.

Al igual que con todas las mejores prácticas que publicamos, consulte el sitio web del M3AAWG (www.m3aawg.org) para conocer las actualizaciones de este documento.

M3AAWG108