Ataques DDoS. Recomendaciones y buenas prácticas

Abstract: un escenario de protestas digitales puede ser compatible con la organización por parte de determinados colectivos que conducen la protesta de una conexión coordinada y masiva por parte de los participantes, que en algunos servidores web podría provocar por sí misma una caída momentánea del servicio por saturación de peticiones, constituyendo un ciberataque por denegación de servicio dirigido.

Contenido:

1 ANTECEDENTES

En situaciones de crisis, una amenaza a considerar puede venir determinada por las protestas digitales que buscan obtener visibilidad mediante ataques de denegación de servicio distribuido (DDoS) sobre servicios concretos que capten la atención de los medios de comunicación.

El escenario de ciberataques marcado por denegación de servicio dirigido, hipotéticamente podría ser llevado a cabo con facilidad por los participantes a través de paquetes de software descargado en sus ordenadores y ampliamente disponible en el dominio público, paquetes de software que permite por ejemplo a una sola persona lanzar peticiones masivas a los servidores con el fin de saturarlos, anonimizando al mismo tiempo su dirección IP y haciéndola parecer que la petición procede del extranjero; así mismo, también hay disponibles para su alquiler “tiempo de botnet” en diversos servicios de proveedores en el dominio público, pensados para llevar a cabo ataques por denegación de servicio, a los que simpatizantes con determinadas protestas digitales podrían haber recurrido potencialmente.

2 AFECTACIÓN Y VECTOR DE ATAQUE

Los ataques DDoS a través de Internet se utilizan para intentar interrumpir el normal funcionamiento de un servidor, servicio o red. Estos pueden clasificarse de acuerdo con los protocolos de la capa del modelo TCP/IP que utilizan, de este modo existen ataques dirigidos a:

- La capa de aplicación: donde se utilizan los protocolos de aplicación, tales como HTTP o DNS para saturar los sistemas objetivos, dentro de este tipo de ataques los más habituales son:

- TLS Renegociation: el ataque consiste en aprovechar el consumo de CPU necesario en el servidor para negociar una conexión SSL al inicio de una petición. Si el atacante es capaz de mandar muchas conexiones por segundo, el consumo de CPU en el servidor puede saturarlo.
- Slow HTTP Attacks: el ataque consiste en enviar al servidor peticiones HTTP en fragmentos lentamente, de uno en uno al servidor Web, con el objetivo de que el servidor mantenga los recursos en espera del resto de datos, si el servidor espera demasiado y el número de conexiones concurrentes alcanza el máximo del servidor, este dejará de responder otras peticiones legítimas.
- HTTP Flood: ataque al protocolo HTTP donde se inunda al servidor de peticiones GET o POST, para intentar saturar al servidor con un número elevado de peticiones legítimas, que logren agotar los recursos de los servidores objetivo. La gran ventaja de este ataque es que no es necesario generar un gran ancho de banda para lograr el éxito.
- DNS Flood: ataques donde se inunda un servicio DNS de peticiones con el objetivo de que el servicio no pueda responder a solicitudes legitimas.
- DNS Amplification: ataque que se aprovecha de los servidores DNS públicos para inundar un servicio o red de destino con una gran cantidad de tráfico, no permitiendo que otros servicios en la misma red respondan.
- NTP Amplification: al igual que el ataque DNS Amplification, este se basa en aprovechar los servidores NTP públicos con el objetivo de inundar un sistema objetivo con una gran cantidad de tráfico UDP que impida al resto de servicios operar con normalidad.

- La capa de transporte: donde se utiliza el protocolo TCP y UDP para saturar los recursos del objetivo. Algunos de los más habituales son:
  - SYN Flood: este ataque busca consumir todos los recursos del servidor inundando el objetivo de solicitudes de conexión inicial (SYN) sin cerrarlas, de modo que el servidor agote sus recursos para atender otras peticiones.
  - UDP Flood: este ataque busca inundar el objetivo de paquetes UDP que deben ser procesador por el destino para determinar si existe el servicio en ejecución en el puerto especificado.
- La capa de Internet: donde se utilizan los protocolos de Internet con el mismo objetivo de saturar los recursos de la máquina, el ataque más habitual es:
  - Ping Flood: este ataque busca inundar el destino de peticiones ICMP para que sea procesado y se envíe una respuesta, buscando de este modo saturar el servidor o la red.

De acuerdo con los ataques descritos, es posible determinar qué elementos son los afectados por este tipo de ataques, y, por lo tanto, cuáles deben ser protegidos:

- El ancho de banda en los ataques volumétricos.
- Los dispositivos de red intermedios en los ataques a los protocolos de red.
- Las aplicaciones y servicios, destacando los servicios HTTP.

3 POTENCIALIDAD DEL ATAQUE

Uno de los ataques más habituales es el basado en HTTP Flood (capa de aplicación), es decir, ataques cuyo objetivo es inundar de peticiones HTTP (GET o POST) las aplicaciones web, buscando agotar los recursos de los servidores.

Es importante remarcar la duración de los ataques de denegación de servicio, se han visto tendencias de una duración de menos de 10 minutos. Un ataque de denegación de servicio contra plataformas cuyo negocio no contenga transacciones económicas, debe ser evaluado por el organismo para determinar cuánto tiempo es tolerable a tener la web caída si no tiene servicios económicos. Las duraciones de tiempo inferiores a 10 minutos vienen determinadas por el coste de realizar el ataque de denegación de servicio y el tiempo que tardan en activarse las contramedidas de mitigación.

El éxito de este tipo de ataques depende de varios factores, entre los que se encuentran:

- La capacidad del atacante para disponer de máquinas, botnets, dispositivos IoT o cualquier otro elemento para lanzar peticiones de forma simultánea.
- El número de dispositivos de red y servidores con los que cuenta la entidad para dar servicio a la comunidad.
- La configuración de los dispositivos intermedios, servidores y demás elementos de la entidad que debe absorber toda esa cantidad de peticiones.
- Arquitectura, desarrollo y personalizaciones de las aplicaciones web objetivo del ataque, en ocasiones aplicaciones mal concebidas o programadas pueden ser “tumbadas” con un ataque DoS desde un solo equipo.

La capacidad del ataque no depende de la entidad y las aplicaciones. No obstante, este no es un tema objetivo de este documento, el cual se centrará en dar recomendaciones de cara a configurar los sistemas perimetrales y las posibles alternativas para protegerse de este tipo de ataques.

La importancia de haber desarrollado un plan de pruebas de las aplicaciones expuestas a Internet con connotaciones de seguridad ayuda a la mitigación de estos tipos de ataques. El desarrollo de los planes de prueba y su aplicación se deben hacer antes de la puesta en producción, pero se pueden reformular durante la vida del aplicativo.

Se deben añadir pruebas de seguridad a los planes de pruebas junto con la comprobación de la funcionalidad, conocer los tiempos de ejecución de los módulos de la aplicación y probar cuántas conexiones concurrentes (legitima o ilegitimas) puede procesar el sistema.

4 CONFIGURACIÓN DE LOS SISTEMAS PERIMETRALES

La primera medida de protección frente a este tipo de ataques de denegación de servicio es configurar los dispositivos perimetrales y los servidores web de la forma más adecuada posible, para minimizar el impacto de estos.

Se recomienda siempre que los servidores web no estén expuestos a Internet directamente (por ejemplo, detrás de un firewall perimetral de capa 4), sino que siempre se ponga detrás de un firewall de capa 7 (WAF), un balanceador o un reverse proxy (hardware o software) que permita balancear la carga y tomar medidas frente a ataques DoS y DDoS.

A continuación, se muestran una serie de recomendaciones básicas para mitigar los ataques DDoS. Estas configuraciones deberán realizarse en aquellos dispositivos perimetrales donde sea posible, que dependerá de la arquitectura de cada entidad:

- Limitar el número de conexiones por dirección IP.
- Bloquear direcciones IP pertenecientes a países donde no se presta servicio.
- Activar las protecciones frente a ataques SYN Flood.
- Limitar el número de peticiones por segundo desde una misma dirección IP.
- Cerrar las conexiones HTTP lentas, no permitiendo más de unos pocos segundos entre el envío de cabeceras o contenido por parte del cliente.
- Bloquear todas las direcciones IP sospechosas de ataques DDoS utilizando Dynamic IP Restrictions (DIR).
- Bloquear peticiones con cabeceras HTTP User-Agent no estándar o pertenecientes a herramientas de hacking.
- Implementar sistemas de cache que permitan devolver peticiones sin que sean procesadas por el backend.
- Limitar el número de conexiones a los servidores de backend.
- Implementar sistemas *captcha* en los formularios públicos sin autenticación.
- Establecer los umbrales de las conexiones por segundo o bajar el umbral.
- Activar Mod_security y/o instalar firewall de aplicaciones destinado al servidor de aplicaciones.
- Activar Dynamic IP Restrictions (DIR).

- Regular el número de conexiones máximas simultáneas (MaxClients).
- Controlar el número de descargas desde una única dirección IP (mod_limitpconn).
- Activar mod_bwshare para permitir conexiones basadas en histórico.
- Activar mod_dosevasive módulo de apache destinado contra DDoS.
- Tener detectadas y monitorizadas las peticiones más pesadas a las bases de datos.

Además de servidores y dispositivos de protección perimetrales se han de tener en cuenta todos los dispositivos que manejan a cualquier nivel tráfico relacionado con el ataque DDoS. El desafío es prevenirlo cuando la mayoría de las veces este tráfico es legítimo según la definición del estándar del protocolo correspondiente.

Por lo tanto, no existe un método o método directo para filtrar o bloquear el tráfico infractor. Además, también existe una diferencia entre el tráfico de ataque volumétrico (que deja una mayor huella) y el de nivel de aplicación.

Las consideraciones a tener en cuenta en los dispositivos de red intermedios son:

- Si los dispositivos tienen capacidad de monitorizar los estados de una conexión y mantener una tabla de estos pueden tener un uso de la CPU y memoria muy intenso durante un ataque. Esto puede ocasionar que el dispositivo de red con esta capacidad se convierta en el punto más débil.
- Emplear técnicas de filtrado de rutas, como Remotely Triggered Black Hole (RTBH) que, activado de forma remota, puede eliminar el tráfico no deseado antes de que entre a una red protegida.
- Verificar la "accesibilidad" de la dirección de origen en los paquetes que se reenvían. Esta capacidad puede limitar la aparición de direcciones falsificadas en una red. Si la dirección IP de origen no es válida, el paquete se descarta (uRPF).
- Emplear recursos globales Anycast. Es posible encaminar el tráfico de una fuente a varios nodos (que representan la misma dirección de destino). Esta solución proporciona dispersión geográfica.
- Ajustar límites de conexión y tiempos de espera en un entorno de red, para garantizar que los ataques DDoS no se inicien o propaguen desde el interior de la red, ya sea intencionalmente o no. Se ha de tener la precaución de la suscripción excesiva de procesos con estado puede hacer que un dispositivo falle.
- Aplicar listas de control de acceso para una mitigación de primer nivel en ataques a nivel de aplicación. Los enrutadores y conmutadores admiten ACL, estos últimos de puertos y VLAN. Se pueden emplear para proteger redes y hosts específicos del tráfico innecesario o no deseado a través del filtrado.

El filtrado de ACL proporciona opciones de mitigación flexibles como: Protocolo de capa 4, Puertos TCP y UDP, Tipos y códigos ICMP, Tipos de IGMP, Nivel de precedencia, Valor de punto de código de servicios diferenciados (DSCP), Paquetes TCP con el conjunto de bits ACK, FIN, PSH, RST, SYN o URG y Conexiones TCP establecidas.

Además, se puede hablar de la siguiente metodología para enfrentarse a un ataque DDoS desde el punto de vista de los dispositivos de red y que se compone de seis (6) fases:

1. Preparación: la más importante, incluye procedimientos técnicos y no técnicos. Las tareas incluyen: instalar y probar herramientas y técnicas de seguridad que se van a utilizar, definir la política de seguridad y los procedimientos de respuesta a incidentes y establecer canales de comunicación con proveedores de servicios y establecer equipos de trabajo.
2. Fase de identificación: detección de actividad o comportamiento inusual y activación de las medidas apropiadas. Algunas herramientas y fuentes de datos para identificar un DDoS son los flujos de tráfico, el uso de CPU y la utilización de las interfaces.
3. Fase de clasificación: después de que se haya detectado un ataque, se deberá recopilar información completa sobre el mismo, incluidas las direcciones de origen falsas o no falsas, las direcciones IP de destino, los tamaños de paquetes y la información de la Capa 4, como el protocolo y los números de puerto. Se puede recopilar estos datos utilizando ACL de clasificación o instalando un sniffer.
4. Fase de rastreo: una vez identificado el vector de ataque, hay que encontrar los puntos de ingreso para mitigar el ataque de manera eficiente. Esto implica rastrear los flujos de ataque desde las secciones atacadas de la red hacia los bordes de la red. Esto se puede realizar a través de ACL (con o sin la cláusula de entrada de registro), mediante la implementación de NetFlow o mediante el uso de mecanismos de retrodispersión.
5. Fase de mitigación: mitigar los flujos de ataque utilizando los mecanismos identificados en la fase de preparación. Estas herramientas y técnicas pueden incluir ACL, blackhole basado en origen y en destino, limitación de velocidad o depuración de tráfico.
6. Fase Post Mortem: esta fase es crítica. Se revisa todo el proceso llevado a cabo durante el ataque, se analiza la experiencia y busca formas de mejorar los aspectos organizativos o técnicos de la respuesta. De esta manera, se cierra el círculo de seguridad en el que las medidas de seguridad se prueban y mejoran y las políticas se actualizan para que reflejen las necesidades de seguridad cambiantes e impulsen la mejora de la seguridad.

Debido a que los ataques por Internet no son un fenómeno temporal y solo se volverán más sofisticados, es importante revisar y refinar continuamente las herramientas y procedimientos de manejo de ataques.

5 SISTEMAS ANTI-DDOS

Dependiendo de la intensidad de los ataques DDoS, y pese a seguir las buenas prácticas de configuración de los sistemas perimetrales, los sistemas seguirán siendo susceptibles de ser vulnerables frente a este tipo de ataques.

Para mitigar los ataques de mayor capacidad, se abre una serie de posibilidades:

- Adquirir nuevos servidores y dispositivos de red para absorber más tráfico y peticiones (balanceadores, servidores frontales y de backend, ancho de banda, etc.).
- Adquirir soluciones hardware Anti-DDoS de distintos fabricantes como medida perimetral para evitar este tipo de ataques (CheckPoint, Radware, etc.).
- Recurrir a los servicios en la nube para prevenir los ataques Anti-DDoS (Akamai, Verisign, Cloudflare, Azure, etc.).

El número de fabricantes, soluciones y alternativas en este punto es muy variado. A continuación, se muestra una pequeña tabla de los más utilizados:

Solución	Localización	Tipo de protección	Capacidades frente a taques
Imperva DDoS Protection[1]	Cloud CDN	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 6 Tbps y 65 billones de pps.
Kona Site Defender de Akamai[2]	Cloud CDN	Protección en capa de aplicación (DNS requiere de FastDNS) e infraestructuras (de capa 3 a 7).	Hasta 61 Tbps
Cloudflare DDoS Protection[3]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 30 Tbps
Microsoft Azure DDoS Protection[4]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Varios gigabytes
Radware DDoS Protection[5]	Hibrido	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 300Gbps y 230 millones de pps.
AWS Shield Advanced[6]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	
Neustar[7][8][9]	Cloud, Hibrido	Protección en capa de aplicación e	Hasta 6 Tbps

[1] https://www.imperva.com/resources/datasheets/ImpervaDDoSProtection_Updated082019_v2.1.pdf
2 https://www.akamai.com/es/es/multimedia/documents/product-brief/akamai-kona-site-defender-product-brief.pdf
3 https://www.cloudflare.com/es-es/ddos/
4 https://docs.microsoft.com/es-es/azure/virtual-network/ddos-protection-overview
5 https://www.radware.com/products/defensepro/
6 https://aws.amazon.com/es/shield/features/

Solución	Localización	Tipo de protección	Capacidades frente a taques
	y aplicación	infraestructuras (de capa 3 a 7)	
Alibaba[10]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 11 Tbps.
StackPath[11]	Cloud CDN	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 65Tbps.
Link11[12]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 724.003 Mbps.
SiteLock[13]	Aplicación	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 16Tbps.
Netscout[14]	Dispone de cloud y/o aplicación	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Arbor Sightline hasta 400 Gbps en un solo dispositivo TMS y hasta 140 Tbps en un solo despliegue Arbor Cloud hasta 11 Tbps
AppTrana[15]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	
Sucuri[16]	Hibrido	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	
Paloalto[17]	Firewall físico	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Múltiples modelos de firewalls disponibles (ver referencias)
Fortinet[18]	Firewall físico	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Múltiples modelos de firewalls disponibles (ver referencias)
Checkpoint[19]	Cloud y firewall físico	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Múltiples modelos de firewalls disponibles (ver referencias). Hasta 400 Gbps.

Si se opta por utilizar un proveedor en la nube que sirva de protección frente a ataques DDoS, es necesario tener en cuenta varios puntos fundamentales:

1. Los servicios publicados deben contestar únicamente a las direcciones IP del CDN o del servicio utilizado como medida de protección anti-DDoS.

7 https://www.home.neustar/ddos-protection/cloud-based-ddos-protection
8 https://www.home.neustar/ddos-protection/hybrid-ddos-protection
9 https://www.home.neustar/ddos-protection/on-premises-ddos-protection
10 https://www.alibabacloud.com/product/ddos
11 https://www.stackpath.com/products/ddos-protection/
12 https://www.link11.com/en/services/ddos-protection/
13 https://www.sitelock.com/products/ddos-attack-protection
14 https://es.netscout.com/product/arbor-threat-mitigation-system y https://es.netscout.com/product/arbor-cloud
15 https://apptrana.indusface.com/managed-ddos-protection-mitigation/
16 https://sucuri.net/website-security/how-we-do-it/
17 https://www.paloaltonetworks.es/network-security
18 https://www.fortinet.com/lat/products/ddos/fortiddos.html y https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiddos.pdf
19 https://www.checkpoint.com/products/ddos-protector/

2. En una misma dirección IP pública no deben convivir servicios protegidos por la solución DDoS de la nube y servicios que no, ya que ataques dirigidos a esos servicios podrían colapsar el sistema y de nada serviría la protección de la nube.
3. No reutilizar direcciones IP ya usadas, es fácil recurrir en Internet al histórico de direcciones IP de los dominios para conocer cuál tenía asignada el dominio y lanzar ataques de DDoS sobre dicha dirección IP que, aunque este bien configurada para no atender peticiones, puede verse saturada procesándolas.