Septiembre, 2014

GRUPO DE TRABAJO 5
Informe final

Índice de contenidos

1 Resultados en breve 3

1.1 Resumen ejecutivo 3

2 Introducción 3
2.1 Estructura del CSRIC IV 9
2.2 Miembros del equipo del Grupo de Trabajo 5 9

3 Objetivo, alcance y metodología 10
3.1 Objetivo 10
3.2 Alcance 10
3.3 Metodología 11
3.3 Métrica 12
3.4 Barreras a la participación 13
3.4.1 Barreras a la participación: Consideraciones 13
3.4.1.1 Barreras tecnológicas 13
3.4.1.2 Barreras del cliente/mercado 14
3.4.1.3 Barreras operativas 14
3.4.1.4 Barreras financieras 14
3.4.1.5 Barreras legales/políticas 14
3.4.1.6 Barreras - Ataques DDoS basados en el servidor 15
4 Antecedentes 16
5 Análisis, resultados y conclusiones 17
5.1 Análisis 17
5.2 Hallazgos 19
5.3 Conclusiones 20
6 Recomendaciones 20
7 Agradecimientos 21
8 Apéndices 21

1 Resultados en resumen

1.1 Resumen ejecutivo

Los sectores de infraestructuras críticas se han visto atacados por un aluvión de ataques DDoS, algunos de los cuales han emanado de centros de datos y proveedores de alojamiento. [1] Los ataques DDoS que se originan en los centros de datos y los proveedores de alojamiento son especialmente problemáticos debido al gran ancho de banda y a los recursos computacionales de los que dispone un atacante. Esto hace que la prevención, la detección y la mitigación sean más importantes, aunque más difíciles. Este grupo de trabajo ha examinado y formulado recomendaciones al Consejo sobre las mejores prácticas a nivel de red y otras medidas que los proveedores de comunicaciones y la FCC pueden adoptar para mitigar los efectos de los ataques DDoS procedentes de grandes centros de datos y sitios de alojamiento. Estas recomendaciones incluyen métodos y procedimientos técnicos/operativos para facilitar la aplicación de las recomendaciones por parte de los interesados. Aunque este informe se centra en los proveedores de comunicaciones, hay que tener en cuenta que para mitigar con éxito los ataques DDoS será necesario que se tomen medidas en todo el ecosistema de Internet, incluidas las de los proveedores de alojamiento, los proveedores de equipos, los propietarios y operadores de infraestructuras críticas, otras partes interesadas que dependen de Internet e incluso, potencialmente, los propios usuarios finales. El Grupo de Trabajo 5 también reconoce que, aunque en gran medida fuera del ámbito de este informe, los ataques DDoS basados en servidores no son sólo un problema nacional; es un problema global. En última instancia, las medidas adoptadas por el ecosistema de Internet incluyen consideraciones internacionales.

En este informe final, el Grupo de Trabajo 5 ha proporcionado recomendaciones que los proveedores de comunicaciones pueden adoptar para mitigar la incidencia y el impacto de los ataques DDoS desde los centros de datos y los proveedores de alojamiento, en particular los dirigidos a los sistemas de información de los sectores de infraestructuras críticas. [2] Las recomendaciones son principalmente en forma de Mejores Prácticas (BPs) de mitigación de DDoS basadas en el servidor que se encuentran en el Apéndice E. Además, se incluyen aquí varias recomendaciones procesables para avanzar en el trabajo de prevención, detección y mitigación de los ataques DDoS basados en el servidor.

El Grupo de Trabajo 5 también evaluó el nivel de esfuerzo de los PSI en la aplicación de los PB en comparación con el impacto de la aplicación de las mejores prácticas específicas para determinar el subconjunto de mejores prácticas que tienen un alto impacto pero un nivel relativamente bajo de esfuerzo para su aplicación. El grupo de trabajo también se centró en la identificación de los obstáculos para la aplicación de las BP, basándose en las lecciones aprendidas de los estudios de casos de los subgrupos de ISP, expertos en seguridad de Internet y comunidad financiera, así como en otros obstáculos basados en las experiencias reales de los miembros en la mitigación de los ataques DDoS. El Grupo de Trabajo también desarrolló una taxonomía para su uso en la aplicación de las mejores prácticas. Por último, el grupo abordó posibles medidas de eficacia destinadas a medir los resultados satisfactorios de las BP voluntarias a nivel de red para mitigar los ataques DDoS basados en el servidor.

2 Introducción

Este informe final documenta los esfuerzos llevados a cabo por el Grupo de Trabajo 5 del CSRIC IV y proporciona las mejores prácticas que los proveedores de comunicaciones pueden seguir para mitigar los ataques DDoS basados en el servidor, lanzados desde los servidores que normalmente se encuentran en los centros de datos y los proveedores de alojamiento. El informe final también ofrece recomendaciones sobre las acciones que la FCC puede llevar a cabo para ayudar a mitigar los

1 http://www.eweek.com/security/ddos-attacks-on-major-banks-causing-problems-for-clientes/
2 http://www.dhs.gov/critical-infrastructure-sectors

ocurrencia y el impacto de los ataques DDoS basados en el servidor.

El Grupo de Trabajo 5 ha reunido a un equipo de más de 40 miembros, entre los que se encuentran representantes de ISP, instituciones financieras, proveedores de alojamiento, organizaciones sin ánimo de lucro, asociaciones, instituciones académicas, gobiernos federales y estatales, y expertos en seguridad para cumplir con el encargo del CSRIC IV. Los esfuerzos del Grupo de Trabajo 5 del CSRIC IV han aprovechado y complementado otras actividades relacionadas con las redes de bots, entre ellas

- Recomendaciones de mitigación de DDoS del CSRIC II3 y CSRIC III4
- Grupo de trabajo sobre mensajería, programas maliciosos y lucha contra el uso de móviles (M3AAWG)[5]
- Grupo de Trabajo Anti-Botnet de la Online Trust Alliance (OTA)6
- Alianza de Seguridad en la Nube (CSA) [7]
- Grupo de redes industriales (IBG)[8]

El Grupo de Trabajo 5 estudió la estructura básica de un ataque DDoS típico y los diferentes tipos de ataques DDoS que se ven en los entornos de red actuales. La figura 1 muestra un ataque DDoS ilustrativo basado en un servidor. Los recientes ataques DDoS han aprovechado las vulnerabilidades de las empresas de alojamiento web y otros grandes centros de datos para lanzar ataques DDoS contra sistemas informáticos y sitios web. Estos ataques pueden originarse a nivel nacional o internacional con objetivos nacionales o internacionales. La prevención, detección y mitigación de estos ataques es compleja y requiere la cooperación y el intercambio de información entre los ISP y los operadores de red, los centros de datos y los proveedores de alojamiento, los fabricantes de infraestructuras (es decir, la cadena de suministro) y los propietarios y operadores de infraestructuras críticas. El Grupo de Trabajo utilizó la interacción del ecosistema descrita anteriormente como base para decidir qué estudios de casos se llevarían a cabo y qué mejores prácticas de la industria se considerarían para esta tarea de mitigación que aborda los ataques DDoS basados en el servidor.

3 http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-consejo-ii
4 http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-consejo-iii
5 http://www.maawg.org/m3aawg-san-francisco-meeting-addresses-latest-messaging-security-ranging-mobile-malware-ddos-attacks
6 https://otalliance.org/resources/botnets
7 https://cloudsecurityalliance.org/
8 http://www.ustelecom.org/blog/industry-botnet-group-takes-multi-party-approach-fight-cibercrimen

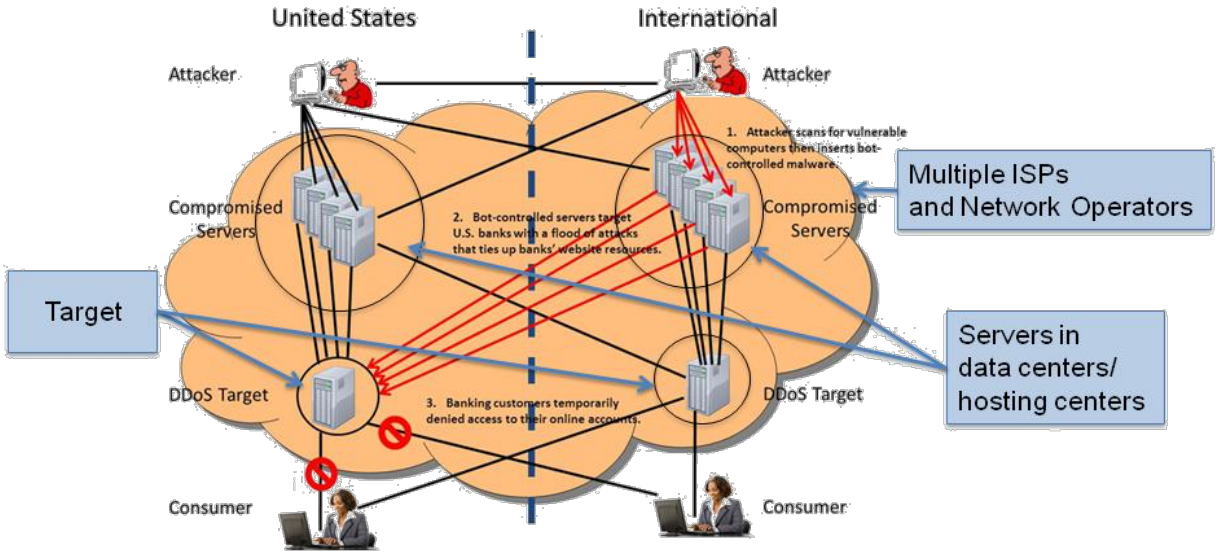


Figure 1 - Example of Server Based DDoS Attack

1

El Grupo de Trabajo 5 también llevó a cabo un análisis de las deficiencias para determinar dónde faltaban las mejores prácticas, pero eran necesarias, para alinearse con las fases del ciclo de vida de la respuesta a incidentes de un ISP en la protección y respuesta a los ataques DDoS basados en el servidor. En los casos en los que se identificaron lagunas, el Grupo de Trabajo formuló recomendaciones sobre nuevas prácticas recomendadas.

El Grupo de Trabajo 5 aplicó el ciclo de vida de la respuesta a incidentes como una forma de mapear las mejores prácticas y recomendaciones sobre DDoS. Este mapeo, junto con las recomendaciones priorizadas en cada área, ayudará a los ISP a identificar las mejores prácticas y recomendaciones más importantes y efectivas en cada área. El Grupo de Trabajo ha adaptado el "Ciclo de vida de los incidentes" de Arbor Network a "Las seis fases de la preparación y respuesta a los ataques DDoS" para los fines de este informe final, véase la Figura 2 a continuación.

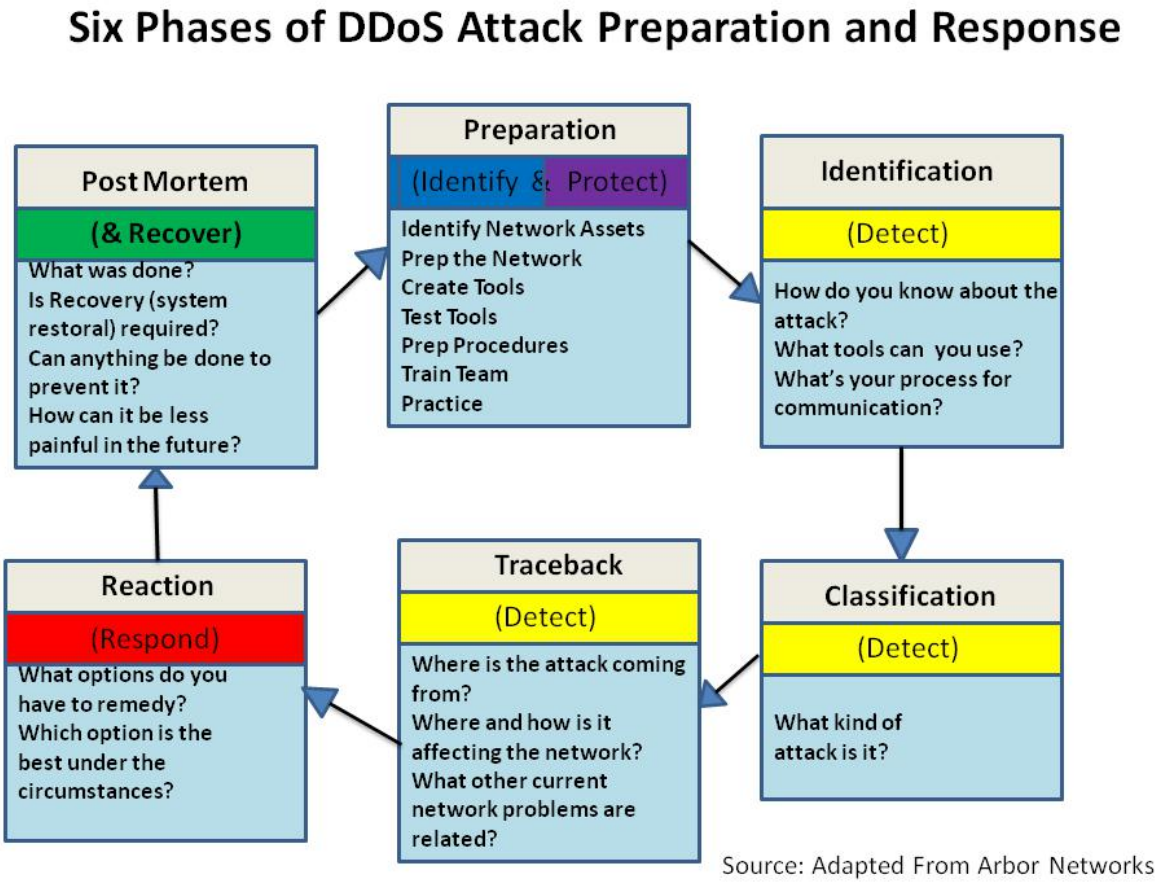


Figura 2. Seis fases de preparación y respuesta a los ataques DDoS.

Junto con el modelo de las Seis Fases, se creó una taxonomía de actividades (Apéndice A) con el fin de proporcionar orientación sobre cómo se podrían utilizar las mejores prácticas en cada fase. El modelo de las Seis Fases es un método de preparación y respuesta a los ataques coherente con el Marco de Ciberseguridad del NIST. [9] El modelo operativo de las Seis Fases se relaciona con el Marco de Ciberseguridad del NIST de la siguiente manera: La Fase de Preparación implementa la Función de Identificación del NIST para identificar los activos de la red a proteger y proporciona la Función de Protección del NIST preparando la red y creando herramientas de detección y mitigación de DDoS. Las fases de Identificación, Clasificación y Rastreo se relacionan con la Función NIST de Detección. La fase de reacción se relaciona con la función NIST Responder, y la fase Post Mortem con la función NIST Recuperar. Esta relación se muestra en la Figura 3.

9http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

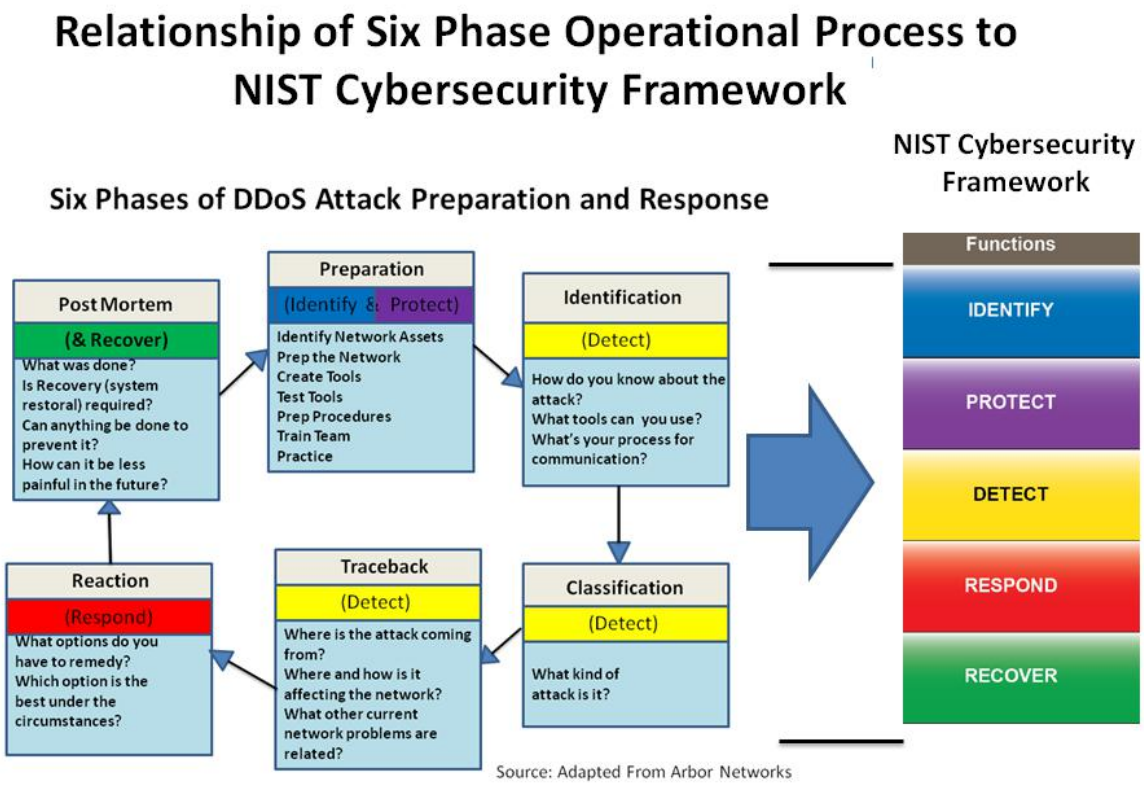


Figura 3. Relación del Proceso Operativo de Seis Fases con el Marco de Ciberseguridad del NIST.

A efectos del análisis, el Grupo de Trabajo utilizó la siguiente definición de ataque DDoS "un ataque de denegación de servicio (**DoS)** o de denegación de servicio distribuido (**DDoS)** es un intento de impedir que los usuarios legítimos accedan a información o servicios10 (US-CERT)". Un ataque de denegación de servicio distribuido consiste en que dos o más sistemas o atacantes realizan el ataque al mismo tiempo al mismo objetivo. Los siguientes son tipos de ataques DDoS:

- Ataques volumétricos
  - Inundación directa de paquetes
    - Los ordenadores comprometidos y de control remoto (bots) envían el tráfico de ataque directamente a la víctima intentando llenar los circuitos con tráfico malicioso.
    - Pueden participar de cientos a decenas de miles de bots.
    - Las herramientas estándar de los ISP manejan bastante bien la mayoría de estos tipos de ataques.
    - Los paquetes pueden ser falsos o no falsos.

  - Ataques de amplificación reflexiva
    - Los bots falsifican su dirección IP de origen para que sea la dirección IP de la víctima.
    - Envíe el tráfico a los servicios donde la respuesta será mucho mayor que la pregunta.

10 http://www.us-cert.gov/ncas/tips/ST04-015

        - Los servidores DNS son grandes amplificadores de este tipo de ataques.
        - Son posibles factores de amplificación de más de 200 veces.
        - Los paquetes deben ser falsificados.

- Ataques a la capa de aplicación
    - El software malicioso de los bots está diseñado para enviar tráfico al servidor web o a otro servidor de aplicaciones que parece provenir de los recursos informáticos de un cliente y consumidor legítimo.
    - Menor volumen de tráfico.
    - Se requiere más trabajo de los atacantes para lograr sus objetivos.
    - El tráfico cifrado es más difícil de mitigar.
    - La mitigación completa necesita mirar los paquetes no encriptados. Una cierta mitigación puede producirse sólo con los paquetes encriptados
    - Por lo general, los paquetes no pueden ser falsificados.
    - Ataques al servicio de nombres de dominio (DNS)
        - El DNS es uno de los dos servicios críticos de Internet, sin el cual fallan casi todas las aplicaciones de Internet (correo, web, etc.). El DNS es las páginas blancas de Internet.
        - En lugar de atacar directamente a la víctima, los atacantes atacarán los servicios de DNS del ISP de la víctima, derribando el tráfico de la víctima.
        - El ataque no sólo afecta al tráfico de la víctima, sino que puede afectar a muchos otros clientes del ISP aunque no sean el objetivo del ataque.

- Ataques de agotamiento del Estado
    - Dispositivos que mantienen el estado de las conexiones, como servidores, cortafuegos y sistemas de detección/prevención de intrusiones que tienen capacidades de estado limitadas.
- Ataques al plano de control
    - Protocolos de enrutamiento como Border Gateway Protocol (BGP) y Open Shortest Path First (OSPF).

El Grupo de Trabajo utilizó los tipos de ataque mencionados para identificar las mejores prácticas de mitigación de los ataques DDoS basados en el servidor, así como para debatir las herramientas y técnicas generales de mitigación de dichos ataques, formando un marco para las recomendaciones del Grupo de Trabajo.

2.1 Estructura del CSRIC IV

Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones (CSRIC) IV									
Comité de Dirección del CSRIC									
Silla o Copresidentes: Trabajando Grupo 1	Silla o Copresidentes: Trabajando Grupo 2	Silla o Co-Sillas: Trabajando Grupo 3	Silla o Co-Sillas: Trabajando Grupo 4	Silla o Co-Sillas: Trabajando Grupo 5	Silla o Co-Sillas: Trabajando Grupo 6	Silla o Co-Sillas: Trabajando Grupo 7	Silla o Copresidentes: Trabajando Grupo 8	Silla o Co-Sillas: Trabajando Grupo 9	Silla o Co-Sillas: Trabajando Grupo 10
Trabajando Grupo 1: Siguiente Generación 911	Trabajando Grupo 2: Inalámbrico Emergencia Alertas	Trabajando Grupo 3: EAS	Trabajando Grupo 4: Ciberseguridad Mejores prácticas	Trabajando Grupo 5: Servidor - Con base en DDoS Ataques	Trabajando Grupo 6: A largo plazo Núcleo de Internet Protocolo Mejoras	Trabajando Grupo 7: Legado Mejor Practica Actualizaciones	Trabajando Grupo 8: Submarino Cable Aterrizaje Sitios	Trabajando Grupo 9: Infraestructura Compartir Durante Emergencias	Trabajando Grupo 10: CPE Alimentación de

Tabla 1 - Estructura de los grupos de trabajo del CSRIC IV.

2.2 Miembros del equipo del Grupo de Trabajo 5

El Grupo de Trabajo 5 está formado por los miembros que se indican a continuación.

Nombre	Empresa
Peter Fonash (Copresidente)	DHS
Michael Glenn (Copresidente)	CenturyLink
Paul Diamond (Co-Editor)	CenturyLink
Robert Thornberry (Co-Editor)	Bell Labs, Alcatel-Lucent
Vernon Mosley (Enlace con la FCC)	FCC
Jared Allison	Verizon
Don Blumenthal	Registro de Interés Público
Chris Boyer	AT&T
Matt Carothers	Cox Communications
Roy Cormier	Nsight
Dave DeCoster	Shadowserver
John Denning	FSSCC
Roland Dobbins	Redes Arbóreas
Martin Dolly	ATIS
David Fernández	Tecnologías Prolexic
Mark Ghassemzadeh	ACS
Darren Grabowski	NTT
Sam Grosby	Wells Fargo
Rodney Joffe	Neustar
John Levine	CAUCE
Gregory Lucak	Windstream
John Marinho	CTIA
Dan Massey	IEEE
Ron Mathis	Intrado
Bill McInnis	Identidad en Internet
Chris Morrow	Google
Michael O'Reirdan	MAAWG
Eric Osterweil	VeriSign, Inc.
Wayne Pacine	Junta de Gobernadores de la Reserva Federal
Glen Pirrotta	Comcast

R.H. Powell	Akamai
Nick Rascona	Sprint
Chris Roosenraad	Time Warner Cable
Craig Spiezle	Alianza para la Confianza en Línea
Joe St Sauver	Universidad de Oregón/Internet2
Kevin Sullivan	Microsoft
Bernie Thomas	CSG Internacional
Matt Tooley	NCTA
Errol Weiss	FSSCC
Pam Witmer	Comisión de Servicios Públicos de PA

Cuadro 2 - Lista de miembros del Grupo de Trabajo 5.

3 Objetivo, alcance y metodología

3.1 Objetivo

Este Grupo de Trabajo se encargó de examinar y hacer recomendaciones al Consejo sobre las mejores prácticas a nivel de red y otras medidas para mitigar los efectos de los ataques DDoS desde grandes centros de datos y sitios de alojamiento. El objetivo del Grupo de Trabajo era organizar un grupo de trabajo con una amplia gama de experiencia y conocimientos, e incluir participantes tanto del gobierno como de la industria. Los objetivos del Grupo de Trabajo 511 son:

Objetivos del GT5

Descripción:

Los sectores de infraestructuras críticas, incluido el sector financiero, se han visto asaltados por un aluvión de ataques DDoS procedentes de centros de datos y proveedores de alojamiento. Este Grupo de Trabajo examinará y hará recomendaciones al Consejo sobre las mejores prácticas a nivel de red y otras medidas para mitigar los efectos de los ataques DDoS procedentes de grandes centros de datos y sitios de alojamiento. Estas recomendaciones deben incluir métodos y procedimientos técnicos y operativos para facilitar la aplicación por parte de los interesados de la(s) solución(es) recomendada(s).

Entregable:

Medidas recomendadas que los proveedores de comunicaciones pueden adoptar para mitigar la incidencia y el impacto de los ataques DDoS desde los centros de datos y los proveedores de alojamiento, en particular los dirigidos a los sistemas de información de los sectores críticos.

3.2 Alcance

Desde hace varios años, el volumen, el tamaño y el alcance de los ataques DDoS han aumentado rápidamente, lo que ha supuesto un reto para los proveedores de servicios de Internet debido al mayor volumen observado en

11 http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_5_7_14.pdf

sus redes. Los ataques recientes se han basado en inquilinos infectados dentro de grandes centros de alojamiento de datos. [12] Para abordar el problema de los ataques DDoS basados en los servidores, el Grupo de Trabajo 5 empleó un enfoque holístico (por ejemplo, múltiples partes interesadas representadas en todo el ecosistema) centrado en las medidas que los operadores de red podrían adoptar para prevenir y mitigar los ataques DDoS. El enfoque holístico era necesario, ya que las causas y los impactos de los ataques DDoS deben ser abordados por todo el ecosistema de redes y alojamiento para que sean eficaces. Abordar este vector de ataque se ha convertido en una prioridad para todas las partes interesadas del ecosistema.

El enfoque del Grupo de Trabajo 5 fue ser lo más inclusivo posible sin repetir o duplicar los esfuerzos realizados por otros grupos que abordan otros aspectos del problema de los ataques DDoS basados en el servidor. Además, el enfoque del Grupo de Trabajo 5 fue centrarse en los esfuerzos que darían lugar a acciones recomendadas específicamente para los ataques DDoS basados en el servidor, es decir, muchas de las mejores prácticas revisadas fueron reconocidas como valiosas, eran buenas prácticas *en general*, pero no eran específicas para los ataques DDoS basados en el servidor y por lo tanto no se incluyeron en el ámbito de la tarea del Grupo de Trabajo 5. Una excepción fueron las recomendaciones para protegerse de los ataques de denegación de servicio al sistema de nombres de dominio (DNS). Los ataques DNS repetidos y recientes han sido especialmente atroces, por lo que las mejores prácticas de mitigación se incluyeron en el trabajo del Grupo de Trabajo 5. [13]

3.3 Metodología

El Grupo de Trabajo 5 comenzó identificando subgrupos para centrarse adecuadamente en estudios de casos de ataques DDoS basados en servidores y en el análisis de las mejores prácticas del sector. Los cuatro subgrupos siguientes resultaron de ese enfoque: subgrupos de ISP, comunidad financiera, expertos en seguridad de Internet y mejores prácticas.

El subgrupo de Mejores Prácticas identificó las BPs aplicables para los ataques DDoS basados en el servidor, mientras que los subgrupos de ISPs, Comunidad Financiera y Expertos en Seguridad de Internet desarrollaron estudios de casos representativos para los ataques DDoS basados en el servidor. A continuación, el Grupo de Trabajo 5 en general asoció las mejores prácticas a nivel de red a cada área del subgrupo, así como otras medidas para mitigar los efectos de los ataques DDoS desde grandes centros de datos y sitios de alojamiento.

El Grupo de Trabajo 5 celebró conferencias telefónicas quincenales con los miembros de su grupo de trabajo para llevar a cabo la tarea. Además, los subgrupos celebraron conferencias telefónicas quincenales para solicitar aportaciones y revisar los resultados de sus estudios de caso. El Grupo de Trabajo 5 celebró una reunión presencial de dos días en enero de 2014 (Arlington, Virginia), y en abril de 2014 (Longmont, Colorado), y una última reunión presencial en julio de 2014 (Arlington, Virginia), para facilitar el debate sobre los resultados.

El Grupo de Trabajo 5 revisó aproximadamente 600 BPs de ciberseguridad para determinar si estaban o no dentro del ámbito de la tarea del Grupo de Trabajo (es decir, BPs para mitigar los ataques DDoS basados en el servidor). El Grupo de Trabajo redujo la lista aplicable a unos 30 PB destacados. El Grupo de Trabajo llevó a cabo un análisis de deficiencias utilizando las Seis Fases de Preparación y Respuesta a los Ataques DDoS en paralelo con el Marco de Ciberseguridad del NIST. Sobre la base del análisis de las deficiencias, el Grupo de Trabajo también ha redactado varios BP nuevos para su adopción voluntaria por parte de las Comunicaciones de la industria.

12 ¿http://www.darkreading.com/attacks-and-breaches/bank-attackers-used-php-websites-as-launch-pads/d/d-id/1107833?

13 http://www.pcworld.com/article/2040766/possibly-related-ddos-attacks-cause-dns-hosting-cortes.html

El Grupo de Trabajo también identificó los obstáculos para la aplicación de las BP basándose en las experiencias resumidas en los estudios de casos de los subgrupos, así como en la experiencia de los miembros, y consideró medidas de eficacia basadas en los resultados que demuestran si los esfuerzos voluntarios contra los ataques DDoS basados en el servidor están teniendo un efecto favorable. El Grupo de Trabajo también aplicó la taxonomía de las Seis Fases (Apéndice A) como guía para identificar las mejores prácticas candidatas a ser implementadas.

Por último, el Grupo de Trabajo formuló recomendaciones en cuanto a las medidas que la FCC puede adoptar para ayudar a mitigar los efectos de los ataques DDoS, permitiendo una adopción más amplia de las mejores prácticas recomendadas en materia de DDoS en los servidores.

3.3 Métricas

Las medidas de éxito contra los ataques DDoS basados en el servidor son fundamentales para determinar la eficacia de seguir las mejores prácticas recomendadas en este informe. Los miembros del Grupo de Trabajo 5 reconocen que el acuerdo sobre un enfoque coherente y uniforme para medir la eficacia de seguir las BP recomendadas sentará las bases para determinar si se necesitan acciones voluntarias adicionales en todo el ecosistema para abordar de forma holística los ataques DDoS basados en el servidor.

El Grupo de Trabajo 5 también reconoce que puede ser difícil conseguir medidas eficaces. Cada uno de los operadores de red tiene métodos diferentes para hacer frente a los ataques DDoS. El establecimiento de medidas comunes de éxito requiere que los participantes establezcan un enfoque uniforme en la recopilación, interpretación, análisis y notificación de las métricas de los ataques DDoS. Con el fin de medir la eficacia de seguir los BPs recomendados para ataques DDoS basados en el servidor, las métricas deben ser cuidadosamente elegidas para medir el resultado deseado de una manera significativa, medible y repetible. El análisis cuidadoso de las métricas agregadas en todo el ecosistema, y la inferencia con respecto a la eficacia de la aplicación de los BPs recomendados, requiere la participación y la cooperación entre todas las partes interesadas del ecosistema que contribuyen a la recopilación, el análisis, la presentación de informes y la interpretación de las métricas.

Con el fin de involucrar a los participantes del ecosistema más amplio en la formación de un enfoque uniforme para medir la eficacia de la aplicación de los BPs recomendados, el Grupo de Trabajo 5 se ha asociado con el Grupo de Trabajo 4 de CSRIC IV, Mejores Prácticas de Ciberseguridad, con el fin de aprovechar sus más de 100 miembros, para abordar de manera holística las métricas para medir la eficacia de la aplicación de los BPs recomendados, no sólo para los ataques DDoS basados en el servidor, sino también para otros BPs de ciberseguridad recomendados. Los miembros del Grupo de Trabajo 5 se pondrán en contacto con los miembros del Grupo de Trabajo 4 para completar este esfuerzo de métrica holística para su inclusión en el entregable del Grupo de Trabajo 4 en marzo de 2015.

Como parte del esfuerzo del Grupo de Trabajo 4 sobre métricas, el Grupo de Trabajo 5 recomendará posibles métricas de ataques DDoS basados en el servidor que podrían considerarse como casos de prueba para ser considerados por todos los participantes del ecosistema. Estas medidas que los miembros del Grupo de Trabajo 5 identificarán ante el Grupo de Trabajo 4 serán importantes para medir la eficacia de seguir los PB recomendados para los ataques DDoS basados en el servidor en todo el ecosistema y son medidas de prueba conceptualmente sostenibles para que el Grupo de Trabajo 4 establezca un proceso de revisión disciplinado.

3.4 Obstáculos a la participación

Las siguientes secciones abordan los esfuerzos del Grupo de Trabajo 5 con respecto a las barreras para la participación de los operadores de red en la adopción de las mejores prácticas recomendadas presentadas en este documento. Estas secciones se han adaptado en gran medida de la Guía para la Participación en el Código de los ISP del CSRIC III [14], ya que las barreras identificadas al seguir el Código de Conducta Voluntario Anti-Bot para los ISP del CSRIC III son aplicables a las barreras que los operadores de red pueden encontrar al seguir los PB recomendados para los ataques DDoS basados en el servidor del Grupo de Trabajo 5. Además de los operadores de red, los proveedores de alojamiento, en la medida en que se apliquen los PB recomendados, también pueden encontrar obstáculos similares. El trabajo previo realizado por el CSRIC III proporcionó definiciones y un marco adecuados para el enfoque del Grupo de Trabajo 5 sobre las barreras.

Muchas de las mejores prácticas recomendadas en este informe final implican diversos niveles de compromiso y complejidad. Se entiende que los participantes del sector privado compiten internamente por el capital de inversión y los recursos humanos, y que las decisiones de priorizar dichas inversiones dependen cada vez más de proporcionar un sólido argumento comercial a los responsables de la toma de decisiones.

La Guía de Obstáculos está diseñada para fomentar una mayor participación, proporcionando un conjunto estructurado de recursos relacionados con recomendaciones específicas que incluyen las mejores orientaciones disponibles sobre su aplicación.

3.4.1 Barreras a la participación: Consideraciones

La adopción de las mejores prácticas puede suponer un obstáculo en la medida en que las actividades requeridas afecten a los métodos y procedimientos existentes y a los recursos de múltiples organizaciones. Los operadores de redes tendrán que entender no sólo qué cambios pueden ser necesarios, sino qué organizaciones se verán afectadas desde el punto de vista de los procesos, los recursos y el presupuesto. Hay que tener en cuenta la escalabilidad y los niveles de integración interdepartamental, así como el apoyo continuo necesario para aplicar una recomendación. A la hora de abordar los obstáculos, se ha intentado clasificar cada uno de ellos en una de las siguientes categorías:

3.4.1.1 Barreras tecnológicas

Las barreras tecnológicas son barreras en las que las soluciones técnicas actuales pueden ser insuficientes para hacer frente a las amenazas o en las que esas soluciones pueden tener otros efectos secundarios inaceptables. La importancia de las soluciones tecnológicas como barreras depende del grado en que la tecnología sea necesaria para aplicar una recomendación específica. Algunas soluciones pueden requerir un mínimo de recursos técnicos (activos y personas), mientras que otras pueden ser más exigentes, incluyendo niveles de integración de sistemas. La aplicación de una recomendación también puede depender de la situación actual de un operador de red, incluidas las capacidades, recursos y prioridades internas o el acceso a recursos de terceros. Las barreras tecnológicas pueden traducirse directamente en obstáculos financieros

14 http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

barreras. Puede existir una solución técnica, pero el coste de su aplicación en el operador de la red puede ser prohibitivo.

3.4.1.2 Barreras del cliente/mercado

Las barreras de los clientes o del mercado son obstáculos que surgen de la aplicación de soluciones que pueden ser consideradas por los clientes como ineficaces (por ejemplo, que los clientes decidan no participar) o indeseables (por ejemplo, privacidad, términos y condiciones restrictivos). Las actividades de los operadores de red también pueden tener consecuencias en el mercado al aumentar los costes de sus productos, la cantidad de inversión de capital que un operador de red está dispuesto a hacer, la disposición de los clientes a comprar la solución y otras consideraciones en relación con los productos de la competencia. La aplicación de algunas de las mejores prácticas que se ofrecen como servicios de seguridad gestionados será una decisión comercial del operador de red. Tendrá que decidir si desea ofrecer esos servicios y, en caso de hacerlo, si desea implementarlos internamente o a través de un tercero. Por último, tendrán que decidir el alcance, las características, la capacidad y el precio de la oferta de servicios de seguridad gestionados que mejor se adapte al mercado en el que compiten.

3.4.1.3 Barreras operativas

Las barreras operativas son barreras que podrían tener un impacto inaceptable en la misión principal y los recursos de una organización. Las organizaciones que tienen responsabilidades operativas suelen rendir cuentas a través de medidas de rendimiento bien definidas. (por ejemplo, el tiempo medio de transacción de los representantes de atención al cliente). Toda nueva práctica operativa debe aplicarse prestando suficiente atención a:

- desarrollo y métodos y procedimientos operativos actualizados;
- reasignación de recursos existentes o adicionales;
- escalabilidad de las soluciones;
- objetivos de rendimiento operativo, factores críticos de éxito y capacidad para medir los resultados.

3.4.1.4 Barreras financieras

Las barreras financieras se derivan de la incapacidad de cuantificar los costes o beneficios asociados a la aplicación de las recomendaciones específicas. En el entorno económico actual, la ausencia de una justificación comercial específica para la empresa puede ser una barrera importante para su adopción. Las empresas del sector privado tienen la responsabilidad fiduciaria de tomar decisiones basadas en la asignación prudente del capital. Cuando se trata de invertir en tecnologías relacionadas con la seguridad, la mayoría de las empresas se basan en datos cuantificables para priorizar y asignar nuevas inversiones en sistemas, procesos y recursos humanos.

3.4.1.5 Obstáculos legales/políticos

Las leyes que desalientan la colaboración y el intercambio de información entre los operadores de redes, tanto en Estados Unidos como en el extranjero, pueden dar cobertura a los actores maliciosos. disfrazan las redes de bots como tráfico legítimo, lo que coloca a los profesionales de la seguridad en la insostenible posición de entrometerse potencialmente en la expectativa de privacidad del usuario final o de permitir que tenga lugar una actividad delictiva peligrosa y costosa. [16] Además, los operadores de red no siempre pueden detene r el tráfico aunque se

[15] *Ver id.*

reconozca como malicioso. Por ejemplo, el tráfico podría estar entrelazado con la actividad comercial, de manera que el coste de la mitigación sería mayor que el daño que supone la red de bots. Los operadores de red se enfrentan a un equilibrio continuo entre proporcionar protección a sus clientes y, al mismo tiempo, proteger su privacidad y respetar la autonomía que esperan otros operadores de red.

3.4.1.6 **Barreras - Ataques DDoS basados en el servidor**

Los ataques DDoS que se originan en los centros de datos y en los proveedores de alojamiento son especialmente problemáticos debido al gran ancho de banda y a los recursos computacionales de los que dispone un atacante. Esto hace que la prevención, la detección y la mitigación sean más importantes, aunque más difíciles. Los ataques DDoS basados en servidores requieren la participación del ecosistema, incluso en mayor medida que otros tipos de ataques. Estos aspectos de los ataques DDoS basados en el servidor dan lugar a barreras particulares para hacer frente a los ataques. En este informe se ofrecen varias prácticas recomendadas nuevas para abordar estos aspectos, junto con las prácticas recomendadas existentes y actualizadas más destacadas. En general, las siguientes son declaraciones sobre consideraciones particulares a los ataques DDoS basados en servidores:

3.4.1.6.1 Consideraciones tecnológicas:

Algunas de las mejores prácticas identificadas en este documento son difíciles o no son posibles de implementar sin impacto en algunas redes, dependiendo de la arquitectura de la red. Algunas de las mejores prácticas descritas en este documento dependen en parte de la tecnología disponible en algunas plataformas de dispositivos de red, pero no en otras.

3.4.1.6.2 Consideraciones sobre el cliente/mercado:

Algunas de las mejores prácticas, aunque son muy eficaces, son servicios adicionales que los clientes deben adquirir y configurar. Los controles de mitigación de ataques pueden interferir con el tráfico legítimo, lo que puede considerarse inaceptable para un cliente.

3.4.1.6.3 Consideraciones operativas:

Aunque muchas de las mejores prácticas no son difíciles de aplicar en sí mismas, su aplicación a escala de miles de clientes introduce una complejidad significativa en términos de gestión de la configuración y de los sistemas de back-office. Algunas técnicas de mitigación podrían causar daños colaterales a otros clientes del mismo centro de datos, lo que puede ser considerado inaceptable por los operadores de centros de datos. Muchas de las recomendaciones de cambios operativos requieren la coordinación entre los operadores de red y sus clientes para evitar cortes. Esto supone una importante inversión de tiempo y también puede provocar problemas de retención de clientes si éstos no se benefician directamente de la aplicación.

3.4.1.6.4 Consideraciones legales/regulatorias/políticas:

[16] *Véase*, *en general*, Can We Beat Legitimate Cyber Behavior Mimicking Attacks from Botnets, IEEE (2012).

El intercambio de datos entre proveedores puede ser más difícil en algunos países con leyes locales de privacidad estrictas. También pueden existir problemas de responsabilidad en relación con los datos inexactos compartidos durante un ataque.

3.4.1.6.5 Consideraciones financieras:

Muchas de las mejores prácticas de este documento dependen de capacidades y conjuntos de características específicas que no son omnipresentes entre los routers. Su aplicación puede requerir la adquisición de nuevos equipos por parte de los operadores de red, los proveedores de alojamiento o los clientes.
La aplicación de algunas de las mejores prácticas identificadas puede afectar al rendimiento de los equipos de red o de los servidores. Esto, a su vez, puede requerir dispositivos más potentes o más numerosos, encareciendo los servicios para todos los clientes.

4 Antecedentes

Los CSRIC anteriores han recomendado las mejores prácticas que podrían utilizarse para mitigar los ataques DoS y DDoS. El CSRIC II aprobó las recomendaciones del Grupo de Trabajo 8 de su informe final *ISP Network Protection Practices:*[17]

- Mejores prácticas recomendadas (BPs) en áreas de prevención, detección, notificación, mitigación y consideraciones de privacidad
- Se centró en los PB para los PSI que prestan servicios a los consumidores en redes residenciales de banda ancha, pero señaló que muchas de las mejores prácticas identificadas en el informe también serían prácticas valiosas para aplicar en contextos de redes no residenciales y de no consumidores
- Además, recomendó que, en una fecha posterior, la FCC considere si sería valioso un trabajo adicional de mejores prácticas en el contexto no residencial.

El CSRIC II también aprobó las recomendaciones del Grupo de Trabajo 2A de su informe final sobre *mejores prácticas de ciberseguridad:*[18]

- Mejores prácticas de ciberseguridad actualizadas que reflejan el entorno tecnológico actual dentro de la industria de las comunicaciones, y referencias relacionadas por:
  - Analizar las mejores prácticas existentes de NRIC, NIST, SANS, IEEE, etc. relacionadas con la ciberseguridad
  - Recomendar modificaciones y supresiones de las mejores prácticas existentes
  - Identificar las nuevas mejores prácticas de ciberseguridad en las tecnologías existentes y relativamente nuevas dentro de la industria de la comunicación.

El CSRIC III aprobó las recomendaciones del Grupo de Trabajo 7 de su informe final *Código de Conducta Anti-Bot de Estados Unidos para los ISP (ABC para los ISP):*[19]

- Centrado en la amenaza de las redes de bots desde los dispositivos de banda ancha residenciales
- Acciones voluntarias del PSI recomendadas en las áreas de educación, detección, notificación, remediación y colaboració

17 http://www.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf

18 http://www.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf

19 http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf

- Además, recomendó a la FCC que, en colaboración con otros organismos gubernamentales federales y con la industria, facilitara la creación de estudios de casos sobre actividades de mitigación de botnets

El CSRIC III aprobó las recomendaciones del Grupo de Trabajo 4 de su informe final *DNS Best Practices:*[20]

- Se centró en las mejores prácticas para asegurar el DNS y el sistema de enrutamiento de Internet durante el período previo a la implementación de DNSSEC.

El CSRIC III también aprobó las recomendaciones del Grupo de Trabajo 5 de su informe final *Prácticas de implementación de DNSSEC para los ISP:*[21]

- Examinar las mejores prácticas para desplegar y gestionar las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) por parte de los proveedores de servicios de Internet (ISP).
- Recomendar métricas y mediciones adecuadas que permitan evaluar la eficacia del despliegue de DNSSEC por parte de los ISP.

Los recientes ataques DDoS han aprovechado las vulnerabilidades de las empresas de alojamiento web y otros grandes centros de datos para lanzar ataques DDoS contra sistemas informáticos y sitios web. [22] El CSRIC IV reconoció que el trabajo en esta área es oportuno e importante para incidir en estas últimas amenazas DDoS. Sobre la base de los progresos realizados en los anteriores CSRICs centrados en las redes residenciales, el Grupo de Trabajo 5 del CSRIC IV recibió el encargo de recomendar las medidas que los proveedores de comunicaciones pueden adoptar para mitigar la incidencia y el impacto de los ataques DDoS procedentes de los centros de datos y los proveedores de alojamiento, en particular los dirigidos a los sistemas de información de los sectores de infraestructuras críticas.

5Análisis , resultados y conclusiones

5.1 Análisis

Los estudios de caso analizaron una serie de ataques DDoS basados en servidores. Un ataque puede implicar a varios ISP y a varios centros de datos y de alojamiento.

- Anatomía de un ataque DDoS basado en un servidor

Como se muestra en la figura 3, un atacante puede hacerse con el control de los servidores del centro de datos y del alojamiento y aprovechar los considerables recursos informáticos y de red para lanzar un ataque DDoS contra una víctima empresarial. Obsérvese que el objetivo también podría ser parte de la infraestructura de los ISP. Este ataque abruma el acceso al objetivo, negando el acceso de los usuarios legítimos, así como causando

---

20 http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.p df

21 http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%202013.p df

22 ¿http://www.darkreading.com/attacks-and-breaches/bank-attackers-used-php-websites-as-launch-pads/d/d-id/1107833?

daños colaterales al afectar a otras partes a lo largo de la ruta del tráfico DDoS. La mitigación de este tipo de ataques requiere la actuación de todas las partes implicadas:

- Múltiples ISPs
- Proveedores de alojamiento / Centros de datos / Revendedores
- Infraestructura objetivo
- Infraestructura del ISP del atacante originario

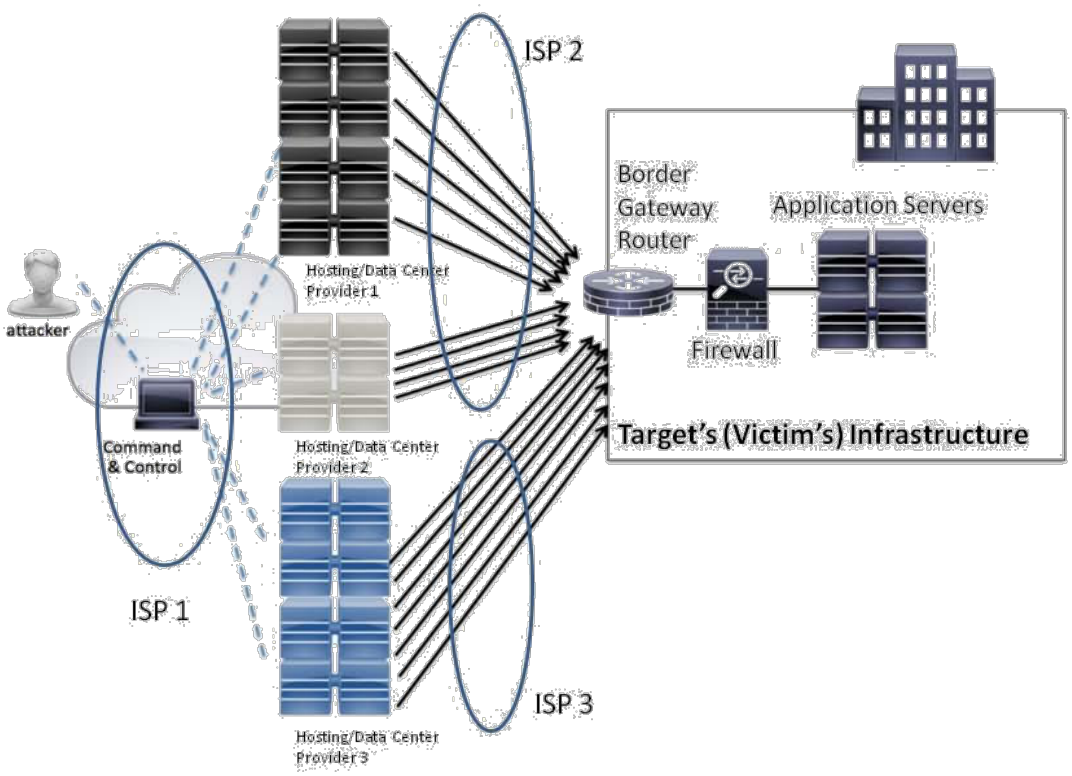


Figura 3 - Un ataque DDoS basado en el servidor.

Fuente:
http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html#_Toc374453043

- Taxonomía de los ataques - Se creó una taxonomía de los tipos de ataques DDoS basados en el servidor para determinar el alcance de las defensas que serían necesarias para mitigar los ataques. La taxonomía de los ataques figura en el Apéndice C.

- Estudios de caso
  - El Grupo de Trabajo 5 identificó tres subgrupos para centrar la atención en los estudios de casos de ataques DDoS basados en servidores de las partes interesadas y un cuarto subgrupo para realizar un análisis de las mejores prácticas del sector. Los subgrupos fueron: ISP, Financiero

Subgrupos de la Comunidad, de los Expertos en Seguridad de Internet y de las Mejores Prácticas.
    - El subgrupo de Mejores Prácticas identificó los BPs aplicables para los ataques DDoS basados en el servidor, mientras que los subgrupos de ISPs, Financiero y Expertos en Seguridad de Internet desarrollaron estudios de casos representativos para los ataques DDoS basados en el servidor. Los casos prácticos se incluyen en el Apéndice D.
- Mejores prácticas recomendadas
    - Las mejores prácticas se incluyen en el Apéndice E

5.2 Conclusiones

Principales conclusiones de los estudios de caso:

1. Los ataques DDoS se están volviendo lo suficientemente grandes como para desbordar la capacidad de absorción de un solo ISP.
2. Los ataques basados en servidores aprovechan los recursos informáticos y de red de los centros de datos para realizar ataques DDoS de un volumen sin precedentes.
3. Debido al aumento del volumen de los ataques DDoS, los daños colaterales (impactos en otras personas que no son objetivo de los ataques DDoS) son comunes: pérdida de paquetes, retrasos, alta latencia para el tráfico de Internet de las partes no implicadas cuyo tráfico simplemente atraviesa las redes saturadas por estos ataques.
4. Los ataques DDoS se utilizan no sólo para interrumpir los servicios, sino para distraer los recursos de seguridad mientras se intentan otros ataques, por ejemplo, transacciones fraudulentas.
5. Los ataques DDoS adaptativos son frecuentes. Los atacantes varían el tráfico de ataque sobre la marcha para evitar su identificación y desafiar y confundir las estrategias de mitigación.
6. Los ataques de reflexión y amplificación siguen siendo comunes, aprovechando los DNS, NTP y otros recursos de red mal configurados con la capacidad de falsificar las direcciones IP de origen (destino).
7. La arquitectura de las redes de bots es cada vez más sofisticada y difícil de rastrear, y los sistemas de mando y control (C2) están cada vez más escalonados, utilizando servidores proxy y redes peer to peer para ofuscar la ubicación del sistema que ejecuta los comandos. Además, algunas redes de bots tienen la capacidad de deteriorar un sistema comprometido después de haber completado un ataque.
8. Los dispositivos están cada vez más repartidos por todo el mundo, lo que dificulta la coordinación del cierre de estos sistemas debido a que los países suelen tener leyes diferentes y a veces contradictorias.
9. El tráfico DDoS se acumula rápidamente, por lo que se necesitan capacidades de mitigación automatizadas para proteger la infraestructura.
10. Con el fin de apoyar las capacidades de mitigación automatizada, es necesario seguir una taxonomía estandarizada para expresar la información necesaria para mitigar los ataques basados en servidores DDoS.
11. Las tecnologías anti-spoofing (antifalsificación) tienen que ser más extendidas para protegerse de los ataques de amplificación.
12. La capacidad de mitigación de DDoS debe desplegarse en toda la red, ya que es difícil predecir dónde se originará el ataque.
13. La mitigación de DDoS requiere múltiples herramientas. Los ISP necesitan la capacidad de filtrado de agujeros negros de destino para proteger sus redes reconociendo que el filtrado de agujeros negros completa la

ataque DDoS al objetivo. Los mitigadores de ataques necesitan múltiples tipos de capacidades menos intrusivas para minimizar la eficacia de los ataques DDoS.

14. Los ataques DDoS deben ser abordados por todo el ecosistema de redes, no sólo por los operadores de redes. Esto incluye a los proveedores de centros de alojamiento y de datos, a los objetivos de los DDoS, a los proveedores de software, a las organizaciones de código abierto, así como a los fabricantes de equipos (toda la cadena de suministro).
15. La mitigación de los DDoS requiere una estrecha colaboración de los objetivos, los proveedores de alojamiento y los operadores de red. A medida que las nuevas técnicas de mitigación de DDoS sean más eficaces, los atacantes seguirán adaptando sus técnicas para encontrar nuevas formas de atacar a sus objetivos.
16. El desarrollo de posibles medidas de éxito para determinar la eficacia de seguir las mejores prácticas voluntarias de ataque DDoS basadas en el servidor debe ser abordado no sólo por los operadores de red, sino por las partes interesadas del ecosistema de Internet en general con el fin de proporcionar interpretaciones significativas y holísticas de la eficacia.

5.3 Conclusiones

En este informe final, el Grupo de Trabajo 5 ha documentado sus conclusiones, ha formulado recomendaciones, ha sugerido las mejores prácticas para hacer frente a los ataques DDoS basados en el servidor, ha abordado los obstáculos para su aplicación y ha sugerido un camino a seguir para abordar de forma holística las medidas de eficacia para seguir los PB recomendados. En este informe final concluimos que será necesario que actúen, no sólo los operadores de red, sino todo el ecosistema de partes interesadas afectadas por los ataques DDoS basados en servidores, para prevenir, detectar y mitigar los ataques.

6 Recomendaciones

1- La FCC anima a los ISP a considerar la implementación voluntaria, de forma prioritaria, de las mejores prácticas recomendadas y de las nuevas recomendaciones (Apéndice E) para hacer frente a los ataques DDoS basados en el servidor, promoviendo la concienciación y los beneficios de estas mejores prácticas.

2- La FCC fomenta el desarrollo de las mejores prácticas para los proveedores de alojamiento con el fin de promover prácticas informáticas seguras, reducir las vulnerabilidades y la amenaza de explotarlas, reduciendo así la incidencia de los ataques DDoS basados en el servidor.

3- La FCC fomenta las relaciones voluntarias del sector privado, en la medida en que no existan ya, entre pares para colaborar en las mejores prácticas de respuesta a los DDoS y en el apoyo a la mitigación.

4- La FCC fomenta el desarrollo de un centro de intercambio de información voluntario para la mitigación de DDoS dentro de la estructura existente de intercambio de información del DHS que puede ser un recurso entre los ISP, los proveedores de alojamiento, los objetivos, las organizaciones de respuesta (CERTS e ISAC) y los gobiernos para mitigar los ataques DDoS en tiempo real.

5- La FCC anima a las partes interesadas del ecosistema a compartir la información de los ataques basados en servidores DDoS entre ellas o a través de un centro de intercambio de información que utilice una taxonomía estandarizada, como la Structured Threat Information eXpression (STIX)[23] o una construcción similar, para ayudar a la mitigación automática de los ataques.

6- FCC fomenta el intercambio de las mejores prácticas de mitigación de DDoS, amenazas, vulnerabilidad,

23 https://stix.mitre.org/

y acciones de respuesta a incidentes entre los operadores de red en el Comm-ISAC.

7 Agradecimientos

Este informe final refleja las inestimables contribuciones de todos los miembros del grupo de trabajo. Los copresidentes del Grupo de Trabajo 5, Michael Glenn de CenturyLink y Peter Fonash de DHS, desean expresar su agradecimiento a todos los miembros del Grupo de Trabajo 5 por su arduo trabajo, su tiempo y sus enormes esfuerzos, que han culminado en este informe final. Los copresidentes desean reconocer los incansables esfuerzos de los editores, Paul Diamond de CenturyLink y Robert Thornberry de Bell Labs, Alcatel Lucent, por su extraordinaria dedicación en la elaboración de los informes provisional y final. Los copresidentes también desean reconocer a las siguientes personas que han liderado los esfuerzos de los importantes subgrupos:

- ISPs - Jared Allison de Verizon y Chris Boyer de AT&T
- Financiero - John Denning del Bank of America y Errol Weiss del Consejo de Coordinación del Sector de Servicios Financieros (FSSCC)
- Internet - Roland Dobbins de Arbor Networks
- Mejores prácticas - Robert Thornberry de Bell Labs, Alcatel-Lucent

Los copresidentes desean agradecer a Vernon Mosley, de la Comisión Federal de Comunicaciones, sus considerables esfuerzos para facilitar la elaboración del informe. Los copresidentes también desean agradecer a los anfitriones de las reuniones presenciales, CenturyLink e Intrado. Y los copresidentes también desean agradecer a John Levine, de CAUCE, la creación y el mantenimiento de la wiki y el listserve del WG5.

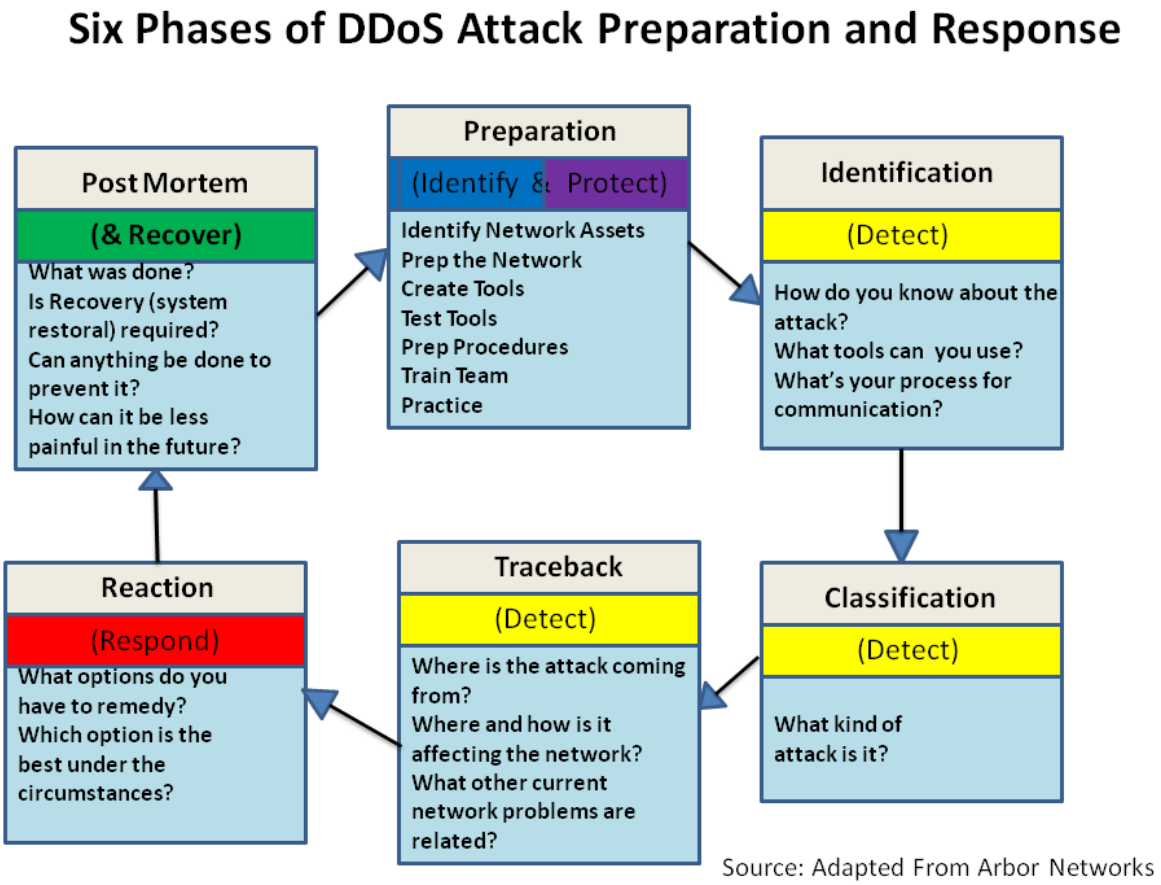
Y los miembros del Grupo de Trabajo 5 desean reconocer el excelente liderazgo de los copresidentes, Michael Glenn y Peter Fonash, por mantener el grupo de trabajo centrado y por crear un entorno de equipo de alto rendimiento en el que contribuir a las recomendaciones de mitigación de ataques DDoS basados en servidores.

8 Apéndices

Apéndice A: Seis fases de preparación y respuesta a ataques DDoS Taxonomía
Apéndice B: Glosario de DDoS basado en el servidor
Apéndice C: Taxonomía de los ataques DDoS
Apéndice D: Estudios de caso de mitigación de ataques DDoS
Apéndice E: Mejores prácticas de mitigación de DDoS basadas en el servidor

Apéndice A: Seis fases de preparación y respuesta a ataques DDoS Taxonomía

.



Source: Adapted From Arbor Networks

Preparación

- Comunicación
  - ISP y Pure Play DDoS Empresa de mitigación (PP)
    - ISP/PP a ISP/PP
    - De ISP/PP a Hosting
    - ISP/PP a la víctima
    - ISP/PP a la Coordinación Central Centro
  - Hospedaje
    - Alojamiento a ISP
    - De alojamiento a alojamiento
    - Acogida a la víctima
    - Acogida en la Coordinación Central Centro
  - Objetivo
    - Víctima a ISP
    - De víctima a anfitrión
    - De víctima a víctima
    - Objetivo a la coordinación central Centro
- Control y visibilidad
  - ISP
    - Netflow
    - Niveles de tráfico
    - Niveles de recursos de la infraestructura del servidor
    - Secuestro de rutas
    - FW, router, registros del servidor
  - Hospedaje
    - Netflow
    - Niveles de tráfico
    - Niveles de recursos de la infraestructura del servidor
    - Señalización del ataque del ISP
    - FW, router, registros del servidor
  - Objetivo
    - Niveles de recursos de la infraestructura del servidor
    - Señalización del ataque del ISP
    - FW, router, registros del servidor

Prevención

ISP

Técnicas anti-spoofing
Reducir las superficies reflectantes
Límites de tarifa / Bloqueo de tráfico

Hospedaje

Técnicas anti-spoofing
Reducir las superficies reflectantes
Límites de tarifa / Bloqueo de tráfico
Plan de minimización de recursos del servidor y procedimientos

Objetivo

Plan de minimización de recursos del servidor y procedimientos

Despliegue y configuración
Herramientas de mitigación

ISP y Pure Play DDoS
Empresa de mitigación
Filtrado

Filtrado CDN (ataques al tráfico web)
BGP Flowspec
Filtrado de agujeros negros (Fuente y Destino)
Depuración de datos de la red

Filtrado del alojamiento

Depuración de datos in situ

Filtrado de objetivos

Depuración de datos in situ

Capacidad y recursos		
	ISP	
		Servidor DNS
		Capacidad de la red DNS
		Enlace, router y estado de BGP
		Protección
	Hospedaje	
		Servidor DNS
		Capacidad de la red DNS
		Enlace, router y estado de BGP
		Protección
		Ancho de banda del enlace ascendente del centro de datos
		FWs, IDS/IPS, capacidades de conmutación
	Objetivo	
		Servidores y enlaces de red
		FWs, IDS/IPS, capacidades de conmutación
		Capacidades de recursos del servidor
Minimizar el Servicio de Ataque		
	ISP	
		Cerrar Resolvers DNS abiertos
		Limitar la velocidad de las consultas DNS
		Limitar la velocidad de los protocolos abiertos (NTP, Echo, etc)
		Desactivar los protocolos innecesarios en infraestructura de red
	Hospedaje	
		Cerrar Resolvers DNS abiertos
		Limitar la velocidad de las consultas DNS
		Limitar la velocidad de los protocolos abiertos (NTP, Echo, etc)
		Desactivar los protocolos innecesarios en infraestructura de red
		Desactivar los protocolos innecesarios en servidor e infraestructura virtual
	Objetivo	

Desactivar los protocolos innecesarios en servidor e infraestructura virtual

Peering y Upstream Cooperativa ISP acuerdos de mitigación

Formal e informal acuerdos de mitigación Identificación de 24/7 contactos operativos en pares o ISPs ascendentes para mitigación de ataques asistencia

Identificación

Control y visibilidad

ISP

Netflow (con router e interfaz información)
Niveles de tráfico
Infraestructura de servidores
Secuestro de rutas
FW, router, registros del servidor
Captura y análisis de paquetes completos

Hospedaje

Netflow (con router e interfaz información)
Niveles de tráfico
Cargas del sistema
Señalización del ataque del ISP
FW, router, registros del servidor
Captura y análisis de paquetes completos

Objetivo

Cargas del sistema
Señalización del ataque del ISP
FW, router, registros del servidor
Captura y análisis de paquetes completos

Confirmar con el objetivo (cliente) que el el tráfico es realmente un ataque el tráfico.

Clasificación

Tipo de ataque

¿Ataque volumétrico?

Inundación directa de paquetes
Reflexión/Amplificación

¿Ataque a la capa de aplicación?
Estado o recurso
¿Ataque de agotamiento?

¿Ataque de avión de control?

¿Ataque específico Ipv6?

Rastreo

Identificación de la fuente
IPs

Identificación de la entrada
interfaces del router

Identificación de DDoS
Rutas de paquetes

Cargas de tráfico intermedias

Identificación de los reflejos
Superficie (routers, servidores, etc)

Identificación del router de entrada
interfaces para la suplantación de identidad
paquetes

Reacción

Determinar la mejor herramienta o conjunto de herramientas para mitigar la ataque

Analizar el tráfico residual
ir a la sintonía fina del objetivo
filtros de mitigación y
cambios en el tráfico de ataques y métodos

Supervisar los métodos de filtrado para minimizar los falsos positivos errores de tráfico

¿Se necesita la ayuda de los compañeros o de los proveedores de la cadena de suministro para ¿Mitigar el ataque?

Post Mortem

¿Cómo de rápido fue el
ataque identificado y
¿clasificado?

¿Fueron eficaces las herramientas
en la mitigación del ataque?

¿Hay algún otro
medidas preventivas
que se pueden poner en marcha para
¿prevenir futuros ataques?

¿Hay algún otro
medidas de mitigación que
se puede poner en marcha para
mitigar más eficazmente
¿futuros ataques?

¿Fueron las comunicaciones
¿conforme a los plazos y a la eficacia?

Fueron mutuos ISP
acuerdos de asistencia
¿es necesario? ¿Eficaz?

Apéndice B: Glosario de DDoS basado en servidor del CSRIC IV WG5

(Este glosario combina los glosarios de los informes finales del CSRIC III WG7 como base).

I. Condiciones:

1. Filtrado de agujeros negros / Enrutamiento de agujeros negros

Es una técnica que se utiliza para eliminar el tráfico de red basándose en la dirección IP de origen o de destino. El filtrado/enrutamiento de agujeros negros se utiliza normalmente para mitigar un ataque DoS o DDoS por parte de un operador de red. La técnica puede desplegarse en routers de borde, de frontera o de núcleo para eliminar eficazmente el tráfico de ataque cerca de los puntos de entrada de la red para minimizar los efectos de un ataque en la red o en el tráfico de otros clientes.

2. Bot

Un "bot" malicioso (o potencialmente malicioso) (derivado de la palabra "robot", en lo sucesivo denominado simplemente "bot") se refiere a un programa que se instala en un sistema con el fin de permitir que ese sistema realice automáticamente (o de forma semiautomática) una tarea o conjunto de tareas normalmente bajo el mando y control de un administrador remoto (a menudo denominado "bot master" o "bot herder").
Los sistemas informáticos y otros dispositivos de usuario final que han sido "botteados" también suelen ser conocidos como "zombis".
Los bots maliciosos se instalan normalmente de forma subrepticia, sin el consentimiento del usuario, o sin que éste sepa lo que podría hacer el sistema del usuario una vez instalado el bot.
Los bots se utilizan a menudo para enviar correo electrónico no deseado ("spam"), para reconocer o atacar otros sistemas, para espiar el tráfico de la red o para alojar contenidos ilegales como software pirata, material de explotación infantil, etc.
Muchas jurisdicciones consideran que la infección involuntaria de hosts de usuarios finales es un ejemplo de intrusión informática ilegal.

3. Botnet

Las redes de bots son redes de dispositivos informáticos de usuario final conectados a Internet e infectados con malware de bots, que son controlados a distancia por terceros con fines nefastos.
Una red de bots está bajo el control de un determinado "molestador" o "botmaster". Una red de bots puede tener sólo un puñado de hosts bots, o millones.

4. Proveedor de comunicaciones

Los proveedores de comunicaciones están formados por los proveedores de servicios de Internet, los proveedores de servicios, los operadores de redes, los operadores de centros de alojamiento, los operadores de centros de datos y el ecosistema de fabricantes que apoya a estos proveedores.

5. Cliente (o "Cliente directo")
La parte que contrata el servicio con un ISP. Distinga el "cliente" de un "usuario autorizado": por ejemplo, una cafetería puede contratar el servicio de Internet de un ISP. La cafetería sería el cliente del ISP. La cafetería puede optar por ofrecer el uso gratuito de su conexión (si

permitido por la Política de Uso Aceptable del ISP, o AUP) a quienes le compran café -- los compradores de café serían entonces usuarios autorizados de la conexión adquirida por la cafetería, pero no el cliente directo del ISP.

6. Centro de datos

Una instalación dedicada a albergar grandes cantidades de recursos informáticos y de red en un entorno que proporciona energía y capacidades de red de alta disponibilidad.

7. Depuración de datos

Enrutamiento del tráfico de ataque DoS o DDoS a un sistema o servicio que trata de diferenciar el tráfico de red "bueno" del tráfico de ataque y que abandona el tráfico de ataque mientras pasa el tráfico bueno. Los depuradores de datos pueden desplegarse en las redes de los operadores de red o en las instalaciones de los clientes. Para el tráfico de ataque mayor que el ancho de banda de las instalaciones del cliente, se necesitan depuradores de datos basados en la red para mitigar eficazmente el ataque.

8. Ataque de denegación de servicio (DoS) o de denegación de servicio distribuido (DDoS)

A El ataque de denegación de servicio (DoS) o de denegación de servicio distribuido (DDoS) es un intento de impedir que los usuarios legítimos accedan a información o servicios24 (US-CERT)". Un ataque de denegación de servicio distribuido consiste en que dos o más sistemas o atacantes realizan el ataque al mismo tiempo al mismo objetivo.

9. Detección

La detección es el proceso por el que un proveedor de servicios o un usuario final se da cuenta de que un determinado sistema o dispositivo ha sido infectado con software malicioso. Un proveedor de servicios puede detectar que un sistema se ha infectado de muchas maneras diferentes, incluso como resultado de recibir quejas de terceros sobre el spam, el escaneo de la red o los ataques que se han originado en ese sistema. Los usuarios finales pueden detectar las infecciones del sistema mediante herramientas de software u otros medios.

10. Ecosistema

Este término se utiliza a menudo para describir la interrelación de varios participantes en Internet: fabricantes de hardware, desarrolladores de software, proveedores de servicios de Internet y proveedores de diversos contenidos, aplicaciones y servicios de Internet que hacen que la red funcione y sea útil para los usuarios finales.
El ecosistema de Internet incluye proveedores de sistemas operativos, organizaciones centradas en el usuario final, proveedores de contenidos, aplicaciones y servicios de Internet, proveedores de servicios de Internet, proveedores de búsquedas, usuarios finales, departamentos de TI, empresas de alojamiento, proveedores de blogs, proveedores de seguridad, investigadores, gobiernos, empresas de servicios financieros y otras partes.
La llamada "economía sumergida" también se describe a menudo como un "ecosistema", con múltiples participantes que desempeñan diversas funciones especializadas. Por ejemplo, algunos participantes pueden especializarse en escribir malware, mientras que otros pueden "cosechar" direcciones de correo electrónico de páginas web y listas de correo, mientras que otros pueden especializarse en la distribución de malware a esas direcciones de correo electrónico cosechadas. El ecosistema de malware también incluirá normalmente a la población de víctimas potenciales seleccionadas y a los organismos encargados de hacer cumplir la ley que trabajan en la lucha contra la ciberdelincuencia.

[24] http://www.us-cert.gov/ncas/tips/ST04-015

11. Usuario final

Usuario final: En un contexto informático y de redes, el usuario final es la persona que, en última instancia, hace un uso autorizado de un producto o servicio.

A menudo, el usuario final puede no ser la misma persona que ha comprado el producto o servicio. Por ejemplo, el propietario de una cafetería puede comprar la conectividad para que la utilicen sus clientes; en ese caso, los clientes de la cafetería, y no el propietario, representan los verdaderos "usuarios finales", aunque no hayan contratado directamente a un ISP para la conectividad que utilizan.

Una parte, como un hacker/cracker que hace uso de un producto o servicio sin la autorización del comprador, se consideraría normalmente un intruso cibernético y no un "usuario final" per se.

12. Centro de alojamiento / Proveedor de alojamiento

Los centros de alojamiento ofrecen varios tipos de servicios de alojamiento que pueden ir desde el alojamiento gestionado que utiliza recursos informáticos, de red y de gestión proporcionados por el operador del centro de alojamiento, hasta el alojamiento en coubicación que permite a los inquilinos proporcionar su propio equipo alojado en los racks del operador de alojamiento.

13. ISP

Un proveedor de servicios de Internet (PSI) es una empresa que proporciona acceso a Internet al público, a las empresas y a otras organizaciones. Esas conexiones pueden ser por cable, DSL, satélite, inalámbricas, de acceso telefónico u otras tecnologías. Los ISP a veces se conocen también como "proveedores de acceso".

Una empresa que proporciona acceso a Internet únicamente a sus propios empleados no se consideraría normalmente un PSI. Del mismo modo, un operador de red que sólo proporciona acceso a Internet al por mayor para otros ISP se consideraría normalmente un proveedor de servicios de red (NSP), en lugar de un ISP.

14. Malware

"Malware" es la abreviatura de "software malicioso".

Los bots maliciosos son un tipo de malware. Otras formas de malware incluyen categorías de software conocidas como virus, troyanos, gusanos, rootkits, crimeware, registradores de pulsaciones de teclas, dialers, spyware, adware, etc. Los factores que distinguen esos diferentes tipos de malware son menos importantes que la comprensión de por qué el malware puede ser visto como "malicioso".
El malware suele violar uno o varios de los siguientes principios fundamentales:
(a) Consentimiento: El malware puede instalarse aunque el usuario no lo haya pedido conscientemente.
(b) Honestidad: El malware puede pretender hacer una cosa, mientras que en realidad hace algo completamente diferente.
(c) Privacidad-Respeto: El malware puede violar la privacidad de un usuario, quizás capturando sus contraseñas o la información de su tarjeta de crédito.

(d) No es intrusivo: El malware puede molestar a los usuarios mostrando anuncios, cambiando la página de inicio del navegador, haciendo que los sistemas sean lentos o inestables y propensos a fallar, o interfiriendo con el software de seguridad ya instalado.
(e) Inocuidad: El malware puede ser un software que perjudica a los usuarios (como el que daña nuestro sistema, envía correos electrónicos de spam o desactiva el software de seguridad).
(f) Respeto a la gestión del usuario: Si el usuario intenta eliminar el software, éste puede reinstalarse o anular las preferencias del usuario.

Todo se resume en "el software que los usuarios no quieren".
Los usuarios pueden instalar malware sin saberlo al abrir un archivo adjunto contaminado recibido por correo electrónico o al visitar una página web con contenido malicioso. Los sistemas también pueden ser infectados directamente por un atacante remoto como resultado de que los atacantes se dirijan a una vulnerabilidad conocida que pueda ser explotada de forma remota, o por el usuario que monta un CD, DVD o unidad de disco duro infectado.

15. Mitigación

La mitigación es el proceso de gestionar o controlar los efectos asociados a un bot. Por ejemplo, si un sistema está infectado con un bot de spam, y está arrojando correo electrónico comercial no deseado, la mitigación puede consistir en filtrar el spam que se está emitiendo desde ese dispositivo.
La mitigación también puede implicar el bloqueo, la limitación del acceso o la limitación de la velocidad de los servicios en los dispositivos que pueden ser utilizados en un ataque DDoS reflexivo.
Hay que tener en cuenta que la mitigación no suele implicar el arreglo de la condición subyacente (eso sería "remediación"); la mitigación sólo maneja los síntomas asociados a una condición.

16. Operador de red

Una organización que proporciona servicios de red para el acceso a Internet en el ámbito alámbrico o inalámbrico. Los ISP, las empresas de telecomunicaciones, las empresas de cable y los proveedores de alojamiento pueden ser ejemplos de operadores de red si prestan estos servicios.

17. Notificación

La notificación es un proceso por el que los ISP se comunican con sus usuarios finales en relación con la posible infección del dispositivo del usuario final por un malware bot o con la forma en que un abonado puede prevenir o identificar dicha infección. La notificación también puede implicar un proceso por el que se dirige a los usuarios finales a herramientas que permitirán el autodescubrimiento de las infecciones por bots. La notificación puede adoptar diferentes formas, incluida la notificación directa por parte del ISP al usuario final, o la notificación indirecta a través de las herramientas de autodescubrimiento disponibles o de un tercero. La notificación puede hacerse a través de múltiples canales potenciales, incluyendo (pero no limitado a) el correo electrónico, el correo postal, una llamada telefónica, una notificación en el navegador, una herramienta de autodescubrimiento basada en la web o un mensaje SMS.

18. Prevención

La prevención es el proceso de endurecimiento de un sistema o servicio para que sea menos vulnerable al compromiso y la explotación. Por ejemplo, en muchos sistemas, la prevención puede implicar:

- Parchear el sistema operativo y todas las aplicaciones con las correcciones de seguridad disponibles

- Instalar o habilitar un cortafuegos
- Uso de software antivirus
- Asegurarse de que el sistema tiene una copia de seguridad periódica
- Utilizar contraseñas seguras
- Desactivar o impedir el acceso a servicios de red innecesarios
- Animar a los usuarios a utilizar de forma segura los servicios de Internet (por ejemplo, el correo electrónico, la navegación por la web, etc.)

19. Ataque DDoS reflexivo

Un ataque DDoS que falsifica la dirección de origen de los paquetes IP de ataque con la dirección IP de la víctima y envía los paquetes IP a los hosts intermedios. Cuando el host intermedio responde a estos paquetes, los paquetes de respuesta se envían a la dirección IP de la víctima, inundándola con tráfico procedente de los hosts intermedios. Normalmente, en este tipo de ataque se utilizan hosts y protocolos intermedios en los que el paquete de respuesta es mayor que el paquete de solicitud, lo que amplifica el tráfico de red enviado a la víctima.

20. Remediación

La remediación es el proceso por el que pasa un usuario final para limpiar un ordenador infectado para que deje de estarlo. En los casos fáciles, esto puede implicar la instalación y ejecución de un producto antivirus. En los casos más difíciles, la reparación puede implicar una intervención más sustancial hasta "destruir y pavimentar" el sistema, es decir, formatearlo y reinstalarlo desde cero, o al menos desde la última copia de seguridad limpia conocida. Una vez que el sistema esté limpio o se haya reinstalado, normalmente se endurecerá para protegerlo de una nueva infección.

21. Servidor

Un servidor de red es un ordenador diseñado para procesar solicitudes y entregar datos a los ordenadores cliente a través de una red local o de Internet. Los servidores de los centros de datos y de los centros de alojamiento suelen tener conexiones de gran ancho de banda a la red y disponen de importantes recursos informáticos para procesar un gran número de solicitudes en un corto periodo de tiempo.

22. Spam

Correo electrónico no deseado y no solicitado, a menudo de carácter comercial, que se envía normalmente a un gran número de destinatarios de forma prácticamente idéntica. El spam suele ser enviado por "afiliados" que reciben el pago de la persona que gestiona el programa de afiliación cuando los destinatarios compran el producto anunciado por el spam.

II. El ciclo de vida de la infección:

1. Limpio: A los efectos del Código de Conducta Anti-Botnet voluntario del ISP, un ordenador u otro dispositivo en red se considerará "limpio" cuando (a) no presente síntomas de infección discernibles externamente (como el envío de spam, la participación en un ataque de denegación de servicio distribuido o el contacto con un host de comando y control conocido), y (b) una revisión del ordenador u otro dispositivo en red con un programa antivirus comercial o de código abierto/gratuito generalmente aceptado (utilizando las definiciones más recientes disponibles) no encuentre ninguna infección, y (c) el ordenador u otro dispositivo parezca funcionar normalmente en todos los aspectos.

Se presumirá que un sistema recién adquirido arranca en estado limpio "al sacarlo de la caja", salvo prueba en contrario.

2. Vulnerable: Un ordenador u otro dispositivo conectado a la red se considerará "vulnerable" cuando tenga uno o varios fallos o desconfiguraciones que lo hagan potencialmente susceptible de ser comprometido, infectado o utilizado como medio de reflexión en un ataque DoS o DDoS. Un ejemplo común de un dispositivo vulnerable es uno que no ha sido parcheado, o que utiliza una contraseña fácil de adivinar para el acceso. Nótese que un sistema puede ser "limpio" y "vulnerable" simultáneamente, como en el caso de que un sistema vulnerable esté protegido por un control compensatorio (como un cortafuegos), permitiendo así que el sistema no se infecte o comprometa a pesar de la presencia de una o más vulnerabilidades.

3. Infectado: Un ordenador infectado o un dispositivo de red infectado es aquel al que se le ha instalado un software malicioso o un firmware malicioso sin autorización conocida. Ese software malicioso o firmware malicioso puede denominarse virus, troyano, gusano, rootkit, registrador de pulsaciones de teclas, dialer, crimeware, spyware, adware, etc. Una definición completa de "malware" se puede encontrar en el glosario que aparece en el Apéndice A del "ABC para los ISP" de la FCC CSRIC.

4. Aislado: Un sistema infectado o comprometido puede ser aislado para evitar que genere tráfico de Internet no deseado. Los hosts aislados a menudo se colocan en "jardines amurallados" donde se limitan a acceder a un conjunto estrictamente limitado de recursos necesarios para la reparación, o sólo se les permite acceder a servicios de seguridad (como el servicio de telefonía VoIP para uso de emergencia).

5. Fuera de línea: Un sistema fuera de línea es aquel en el que no se permite el acceso a la red a/desde ese host en absoluto. Conceptualmente, piense en un host conectado a ethernet en el que se ha desconectado el cable de ethernet (o se ha desactivado el puerto de conmutación de ethernet), aunque obviamente se utilizan procesos técnicos diferentes en el caso de las conexiones de módem de cable, DSL
conexiones, acceso inalámbrico, acceso por módem, etc.

6. Desinfectado: Un sistema se considerará "desinfectado" cuando, habiendo sido infectado, haya vuelto a un estado "limpio" (como se ha definido anteriormente). El primer paso en la desinfección de un sistema suele ser la instalación y ejecución de un producto antivirus (si es que no había uno instalado y actualizado). En algunos casos, puede ser necesario formatear y reinstalar el sistema desde cero para superar el malware persistente particularmente bien escondido.

7. Endurecido: Un sistema reforzado es aquel que ha sido configurado sistemáticamente para eliminar las vulnerabilidades (o posibles vulnerabilidades) del sistema. Por ejemplo, entre otras cosas, un sistema reforzado tendrá parches actualizados, tendrá deshabilitados todos los servicios innecesarios, requerirá el cifrado de todo el tráfico de red sensible, utilizará sistemas de seguridad fuertes.
contraseñas o autenticación multifactor, hará un registro seguro en un host de registro fuera del sistema, etc.

8. Reinfectado: Un sistema que ha sido desinfectado pero NO endurecido suele reinfectarse rápidamente.

9. Comprometidos: Mientras que muchos sistemas vulnerables pueden verse comprometidos como resultado de una infección con malware, otros sistemas vulnerables pueden verse comprometidos como resultado de contraseñas débiles o configuraciones erróneas (como archivos críticos que pueden ser modificados involuntariamente por partes no autorizadas). Un sistema comprometido no es digno de confianza.

10. Gestionado: Un "host gestionado" es aquel que se administra de forma centralizada, en lugar de ser autogestionado administrado por el/los usuario/s del sistema.

11. Monitorizado: Un host monitorizado es aquel que es continuamente (o al menos periódicamente) escrutado en busca de cosas como tráfico de red anómalo o cambios no autorizados en archivos críticos del sistema. La monitorización puede tener lugar a través de sistemas de seguridad de red, como Snort, o a través de sistemas basados en el host, como Tripwire.

12. Reemplazar: Mientras que la mayoría de los usuarios intentan desinfectar y endurecer un sistema infectado, algunos pueden optar por reemplazar ese sistema por uno nuevo. El sistema anterior puede ser vendido o entregado a un tercero, que puede obtener el sistema junto con el malware instalado en él.

13. Compartido: Un sistema compartido es aquel que es utilizado por varios individuos. Un ejemplo común de un dispositivo compartido sería un dispositivo familiar utilizado por uno o varios padres, así como por los hijos u otros miembros de la familia. Un dispositivo compartido suele ser más propenso a las infecciones (u otros problemas de seguridad) que un sistema utilizado por una sola entidad.

14. Huérfano: Un dispositivo huérfano o un programa huérfano es uno más antiguo para el que el proveedor ya no publica ni siquiera parches de seguridad/estabilidad críticos. Los sistemas o programas huérfanos generalmente no pueden ser reforzados.

III. Funciones del ecosistema

1. Cliente: En el contexto del ABC de los ISP, la persona que paga a un ISP por el servicio de Internet.

2. Propietario del sistema: La persona que es propietaria de un determinado ordenador u otro dispositivo.

3. Usuario del sistema: Persona a la que el propietario del sistema permite intencionadamente utilizar su ordenador u otro dispositivo.

4. Persona de apoyo: En el caso de los ordenadores residenciales, una persona de apoyo puede ser un miembro de la familia o un amigo que ayuda al propietario o usuario del sistema a utilizar y mantener su ordenador. Una persona de apoyo también puede ser un especialista en soporte informático comercial contratado a tal efecto por el propietario o usuario del ordenador.

5. Equipo de seguridad/abuso del ISP: La persona o grupo de un proveedor de servicios de Internet que se ocupa de las quejas sobre un cliente.

6. Proveedor: La empresa que fabrica y comercializa un sistema informático o un programa de software. Se puede hablar de un vendedor de sistemas operativos, de un vendedor de software de aplicación, de un vendedor de hardware o de un vendedor de software antivirus, por ejemplo.

7. Aplicación de la ley: Un oficial de policía, un sheriff, un agente federal u otra persona juramentada con el poder de investigar delitos, reunir pruebas y realizar detenciones.

8. Regulador: Funcionario estatal o federal encargado de gestionar las prácticas empresariales u otras actividades para garantizar la equidad fundamental o el cumplimiento de la normativa. Un ejemplo de regulador sería la Comisión Federal de Comercio de Estados Unidos. Los reguladores suelen emplear sanciones civiles (como multas administrativas o demandas civiles) en lugar de sanciones penales (como el arresto/encarcelamiento).

9. Usuario no autorizado: Una persona que utiliza un ordenador u otro dispositivo sin la intención permiso del propietario del sistema, o alguien que utiliza el acceso autorizado en exceso de su autorización

10. Autor del malware: El programador o equipo de programación que diseña y codifica una pieza de malware, como un bot.

11. Botmaster: Un botmaster es una persona que opera una red de ordenadores con bots, a menudo utilizándolos para enviar spam o atacar a otros ordenadores. El botmaster normalmente envía órdenes a "sus" o "sus" bots a través de un host de comando y control, por ejemplo, un servidor bajo su control.

12. Afiliado: En este contexto, un afiliado es una persona que ayuda a comercializar un determinado producto o servicio a cambio de una compensación, normalmente utilizando modelos de pago por impresión, pago por clic, pago por instalación o reparto de ingresos:
(a) Pago por impresión (PPI): los afiliados suelen ser propietarios de sitios web a los que se les paga en función del número de veces que se muestra un banner de un sitio web u otro anuncio a los visitantes
(b) Pago por clic: en este modelo, se paga a los afiliados cuando alguien hace clic en un anuncio
(c) Pago por instalación: en este modelo, los afiliados reciben una remuneración cuando un programa que se les ha suministrado se instala en un nuevo sistema, ya sea de forma subrepticia o con el consentimiento consciente del usuario (quizás como parte de una oferta de "acceso patrocinado" para un programa o sitio que, de otro modo, habría que comprar)
(d) Reparto de ingresos: en este modelo, los afiliados reciben un porcentaje de las ventas asociadas a los clientes que recomiendan.

13. Vendedor de listas: Un vendedor de listas es alguien que recopila y distribuye listas de direcciones de correo electrónico. Por ejemplo, un spammer que quiera hacer publicidad no deseada de un casino online ilegal podría comprar una lista de direcciones de correo electrónico que se sabe que están asociadas a jugadores online.

14. Empresa de alojamiento a prueba de balas: Una empresa de alojamiento a prueba de balas es aquella que acepta alojar un sitio web u otra presencia en línea a pesar de las quejas que puedan derivarse de esa actividad, normalmente a cambio de que la parte alojada pague un precio superior. Las empresas de alojamiento a prueba de balas pueden utilizarse para alojar sitios web con publicidad de spam, software malicioso, material de abuso infantil u otros contenidos que probablemente sean inaceptables para las empresas de alojamiento habituales.

15. Registradores de nombres de dominio a prueba de balas: Un registrador de dominios a prueba de balas es aquel que permite a un spammer o a otro ciberdelincuente registrar un nombre de dominio y mantenerlo, a pesar de las quejas que puedan estar asociadas a ese nombre de dominio. Este servicio se presta normalmente a cambio de una prima sobre las tarifas de registro de nombres de dominio del mercado.

16. Procesador de pagos: Cuando un afiliado realiza una venta, el pago se realiza normalmente con tarjeta de crédito. La entidad que procesa esa transacción con tarjeta de crédito se conoce como "procesador de pagos".

17. Distribuidor directo: Un expedidor directo es una entidad que gestiona el cumplimiento de los pedidos para un programa de afiliados. Por ejemplo, un transportista especializado en productos farmacéuticos ilegales puede empaquetar y enviar los pedidos obtenidos por un spammer de píldoras.

18. Cambio de moneda en línea: Algunos afiliados pueden ser pagados utilizando una moneda online en lugar de a través de un cheque enviado por correo o un depósito directo. Los cambiadores de divisas online hacen posible que algunos compren una divisa online a cambio de dinero en efectivo, o viceversa.

19. Informador de abusos: tercero que informa de un incidente de abuso a un ISP, o a través de un centro de intercambio de información (como un equipo de respuesta a incidentes de seguridad informática).

Apéndice C: Taxonomía de los ataques DDoS

1 Ataques DDoS - Ataque a la disponibilidad 1.1 Definición de ataques DDoS

A efectos del análisis, el grupo de trabajo utilizó la siguiente definición de ataque DDoS "un **ataque de denegación de servicio (DoS)** o de denegación de servicio distribuido (**DDoS) es** un intento de impedir que los usuarios legítimos accedan a información o servicios25 (US-CERT)". Un ataque de denegación de servicio distribuido consiste en que dos o más sistemas o atacantes realizan el ataque al mismo tiempo al mismo objetivo.

1.2 1.2 Objetivos de los ataques DDoS
- 1.2.1 Ataques contra la capacidad
- 1.2.2 Ataques contra el Estado

1.3 Herramientas de ataque DDoS
- 1.3.1 Redes de bots
  - 1.3.1.1 Botnets de clientes
  - 1.3.1.2 Botnets de servidor
  - 1.3.1.3 Botnets participativos
  - 1.3.1.4 Otras redes de bots
- 1.3.2 Arneses de ataque
- 1.3.3 Aplicaciones de generación de tráfico

2 Ataques DDoS IPv4 e IPv6

2.1 Ataques DDoS volumétricos
- 2.1.1 Inundación directa de paquetes
  - 2.1.1.1 ICMP e ICMPv6
  - 2.1.1.2 UDP
  - 2.1.1.3 TCP
    - 2.1.1.3.1 SYN-Flood
    - 2.1.1.3.2 RST-Inundación
    - 2.1.1.3.3 ACK-Inundación
    - 2.1.1.3.4 RST-Inundación
    - 2.1.1.3.5 Inundación nula
    - 2.1.1.3.6 Inundación SYN/ACK
    - 2.1.1.3.7 Inundación del árbol XMAS
    - 2.1.1.3.8 Inundación por combinación de banderas no válida
    - 2.1.1.3.9 Inundación del puerto 0
  - 2.1.1.4 Paquetes fragmentados
    - 2.1.1.4.1 UDP
    - 2.1.1.4.2 TCP
  - 2.1.1.5 Protocolo 0
  - 2.1.1.6 Inundación GRE (encapsulación de enrutamiento general)
  - 2.1.1.7 Inundación ESP (IPsec Encapsulating Security Payload)
  - 2.1.1.8 Inundación RTP
  - 2.1.1.9 Otros protocolos "no estándar" inundan
- 2.1.2 Reflexión/Amplificación
  - 2.1.2.1 Reflejo/amplificación UDP

[25] http://www.us-cert.gov/ncas/tips/ST04-015

2.1.2.1.1 Reflejo/amplificación del DNS
2.1.2.1.1.1 Reflejo/Amplificación del DNS con recursores DNS abiertos y servidores autoritativos
2.1.2.1.1.2 Reflejo/amplificación del DNS con Sólo servidores autorizados
2.1.2.1.2 Reflejo/Amplificación SNMP
2.1.2.1.3 Reflejo/amplificación NTP
2.1.2.1.4 Reflexión/amplificación de la carga
2.1.2.1.5 Reflexión/amplificación del TFTP
2.1.2.1.6 Reflejo/amplificación RADIUS
2.1.2.1.7 Reflexión/amplificación del SIP
2.1.2.1.8 Otros ataques de reflexión/amplificación UDP
2.1.2.2 Reflejo/amplificación del TCP
2.1.2.2.1 Reflexión SYN/ACK
2.1.2.2.2 Reflexión RST
2.2 Ataques DDoS en la capa de aplicación
2.2.1 HTTP
2.2.1.1 GET
2.2.1.2 POST
2.2.1.3 CGI
2.2.1.4 Variantes HTTP "lentas
2.2.2 SSL/TLS
2.2.2.1Malformación de SSL/TLS
2.2.2.2 Negociación SSL/TLS
2.2.2.3 Ataques encapsulados HTTP/S
2.2.3 DNS
2.2.3.1 Inundaciones de peticiones DNS autoritativas
2.2.3.2 Inundaciones de peticiones DNS recursivas
2.2.3.3 Ataques de delegación de zona autorizada
2.3.4 SIP
2.2.4.1 Inundaciones INVITE
2.2.4.2 INFO Inundaciones
2.2.4.3 NOTIFICAR INUNDACIONES
2.2.4.4 REINVITACIÓN DE INUNDACIONES
2.3.5 ssh
2.2.5.1 Negociación SSH
2.2.5.2 Forzar el inicio de sesión
2.3.6 Aplicaciones de nivel intermedio y secundario
2.2.6.1 Subsistemas AAA
2.2.6.2 Bases de datos
2.2.6.3 Sistemas de generación de imágenes
2.2.6.4 Otras aplicaciones de nivel intermedio y secundario
2.2.7Otras aplicaciones
2.3 Ataques DDoS de agotamiento de estado
2.3.1 El papel del Estado en los ataques DDoS
2.3.2 Ataques DDoS de conexión TCP
2.3.2.1 Agotamiento de la conexión
2.3.2.2 Agotamiento de la conexión directa
2.3.2.3 Agotamiento de la conexión de segundo orden en la capa de aplicación

2.4.3 Agotamiento del estado en las Middleboxes/Middleblades Stateful
2.3.3.1 Cortafuegos con estado
2.3.3.2 IDS/'IPS'
2.3.3.3 Balanceadores de carga
2.3.3.4 NATs/CGNs/Proxies
2.4 Ataques DDoS en el plano de control
2.4.1 Enrutamiento
2.4.1.1 BGP4 Y MP-BGP
2.4.1.2OSPF y OSPFv3
2.4.2 Otros ataques al plano de control
3 Ataques DDoS específicos
de IPv6 3.1 Cabeceras
de extensión
3.1.1 ICMPv6
3.1.1.1 Descubrimiento de vecinos
3.1.1.2 Anuncio del router

4 Ataques en varias etapas
4.1 Inundación seguida de ataques de mecanismos de mitigación

Apéndice D: Estudios de caso de mitigación de ataques DDoS

Estudios de caso del subgrupo ISP

I. Antecedentes

Los proveedores de servicios de Internet (ISP) han estado mitigando activamente la *denegación de servicio distribuida (DDoS)*[26] durante varios años. En las primeras versiones más comunes del ataque, los ordenadores personales conectados a los servicios de banda ancha domésticos comenzaron a experimentar infecciones de malware que transformaban las máquinas en los llamados *zombis* (ahora denominados *bots*). Utilizando servidores comprometidos por separado para el control, los atacantes podían entonces ordenar a grandes grupos de bots que enviaran volúmenes de datos a alguna víctima, normalmente un sitio web. El sitio web se vería entonces abrumado por los datos entrantes, y sería incapaz de procesar las solicitudes normales autorizadas.

Desde aproximadamente 1999 hasta 2011, los volúmenes de datos dirigidos a la mayor parte de la infraestructura de los ISP, y la habilidad con la que los adversarios elaboraron los volúmenes de datos, estuvieron dentro de unos umbrales manejables. *Ha habido muy pocos ataques importantes que afecten al servicio en cualquier parte de la infraestructura de los grandes ISP durante ese período de doce años*. Esto incluye los ataques a la infraestructura de servicios de nombres de dominio de los principales ISP de nivel 1. Los ataques durante este período fueron generalmente del tamaño de varios Gigabit por segundo.

Además, durante este mismo periodo de tiempo, algunos ISP desarrollaron nuevos servicios de seguridad gestionados para clientes empresariales con el fin de ayudarles a mitigar los ataques DDoS en su propia infraestructura. Varias instituciones financieras estadounidenses están suscritas actualmente a estos servicios, que suelen implicar la detección en tiempo real de ataques basados en soluciones volumétricas o en aplicaciones. Por ejemplo, un ataque DDoS podría detectarse volumétricamente sobre la base de picos de tráfico utilizando herramientas de recopilación de datos y luego redirigir el tráfico utilizando el protocolo de pasarela de frontera (BGP) hacia cortafuegos especialmente diseñados que filtran el ataque. A continuación, el tráfico filtrado se "tuneliza" hacia el sitio del cliente a través de la infraestructura del ISP.

A finales de 2012, los ISP empezaron a ver ataques a mayor escala por parte de adversarios que creaban un volumen de entrada suficiente como para desbordar la capacidad de entrada de la infraestructura de depuración de algunos ISP. Además, la red de bots que desencadenaba el ataque era única en el sentido de que utilizaba servidores en conexiones de red a menudo de gran tamaño como bots, en lugar de PCs comprometidos en conexiones de banda ancha de consumidores. Más adelante, en el tercer trimestre, este mismo adversario lanzó una serie de "ataques telegrafiados" contra sitios web bancarios con sus advertencias publicadas rutinariamente en *pastebin*. Estos ataques alcanzaron tamaños sin precedentes, a menudo dirigidos de nuevo a los DNS. En respuesta, los ISP hicieron varios ajustes en tiempo real para mejorar su infraestructura, plataformas de depuración y capacidad de sitios DNS27.

Este estudio de caso pretende ofrecer una explicación y una propuesta de prácticas que los PSI pueden adoptar

---

[26] Un **ataque de denegación de servicio (DoS)** o **de denegación de servicio distribuido (DDoS)** es un intento de impedir que los usuarios legítimos accedan a la información o a los servicios26 (US-CERT).

[27] Se trata de un proceso continuo de ingeniería de tráfico. Muchos ISP supervisan continuamente los flujos de tráfico para garantizar una capacidad adecuada. Este mismo proceso se aplica a los enlaces de datos en la infraestructura de depuración DDoS de los ISP.

en respuesta a ataques DDoS a gran escala en el futuro.

II. Taxonomía simplificada de los ataques DDoS para los ISP

Mientras que el grupo de trabajo más amplio ha desarrollado una taxonomía detallada de los ataques DDoS, el subgrupo de ISP consideró necesario desarrollar una versión simplificada para utilizarla en el estudio de caso. El subgrupo también discutió un modelo para clasificar los ataques DDoS en dos dimensiones:

1. Tipo de ataque: volumétrico o de aplicación
2. Dirección del ataque: de *norte a sur* o de *este a oeste*.
    a. *Norte-Sur* es un ataque que se origina fuera de la red del ISP y tiene como objetivo un cliente del ISP o una infraestructura dentro de la red del ISP.
    b. *El ataque de sur a norte es un ataque que se origina dentro de la red del ISP y tiene como objetivo una entidad o infraestructura externa dentro de la red del ISP.*
    c. *Este-Oeste* representa un ataque que se origina en un cliente y tiene como objetivo otro cliente

Ejemplos:

1. Infraestructura del cliente o del ISP atacada desde el exterior - de norte a sur
2. Los clientes con puertas de enlace domésticas con errores inundan los servidores DNS de los ISP - de sur a norte
3. Clientes que inundan paquetes hacia un objetivo externo - también de sur a norte
4. Los clientes se atacan entre sí - de este a oeste

El subgrupo sugirió que separáramos a los clientes que se atacan entre sí de los que atacan a la infraestructura o a objetivos externos, ya que a veces requieren estrategias de detección y mitigación diferentes. Por ejemplo, si dos clientes de la misma región se atacan mutuamente, es posible que el tráfico no atraviese ninguno de los routers de los que los ISP recopilan datos de flujo y no llegue a los centros de depuración del borde de los ISP.

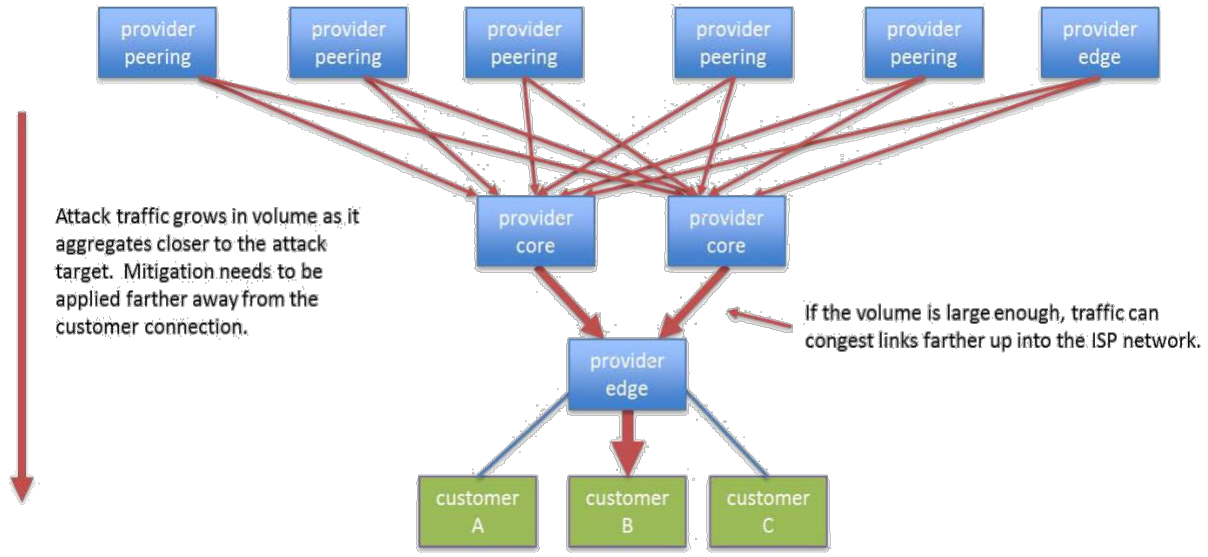
III. Ejemplos de ataques DDoS sufridos por los ISP

A. Ataque DoS volumétrico basado en el servidor contra un gran cliente

Antecedentes: Este ataque utilizó paquetes UDP/80 (tráfico basura) en gran volumen para agotar el ancho de banda del objetivo. El ataque tardó aproximadamente 10 minutos en alcanzar un volumen máximo de más de 70 Gbps. En ese momento fue uno de los mayores ataques vistos en la red del ISP. Las IPs atacantes se contaban por miles.

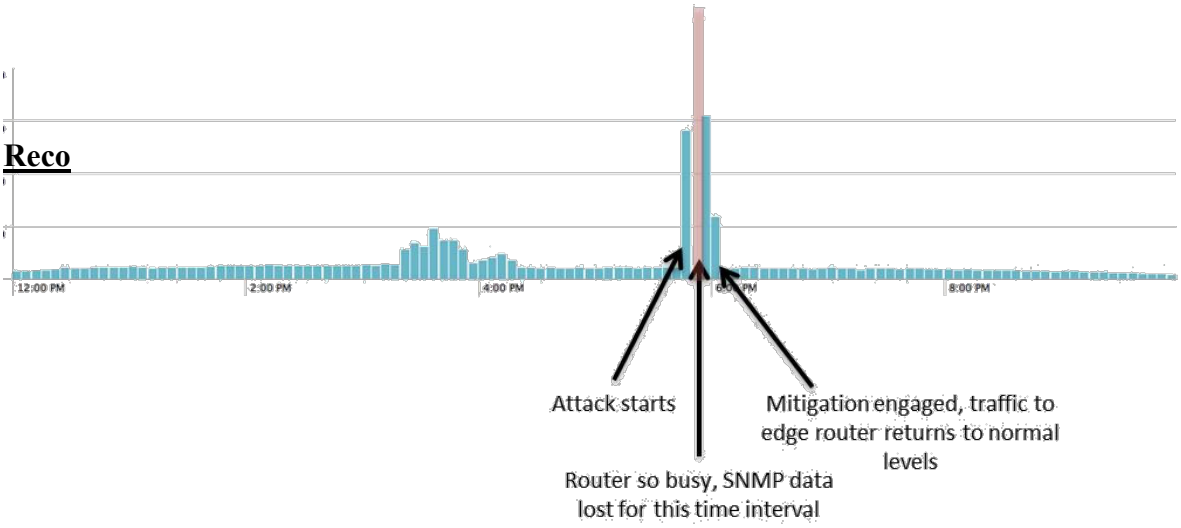
Medidas de mitigación:

1. El ataque fue identificado junto con una IP objetivo por el servicio de detección de DoS del cliente.
2. El cliente contrató el servicio de mitigación del DoS, el tráfico fue redirigido a los centros de mitigación del DoS. El tráfico de ataque se eliminó y se entregó el tráfico legítimo.



En el caso de los ataques de mayor envergadura (de 10 a 100 Gbps), existe el riesgo de que se produzca un impacto colateral en los clientes que no son objeto del ataque. Los daños colaterales a menudo pueden evitarse si el ataque se detecta y se mitiga rápidamente.

Reco



Prácticas recomendadas:

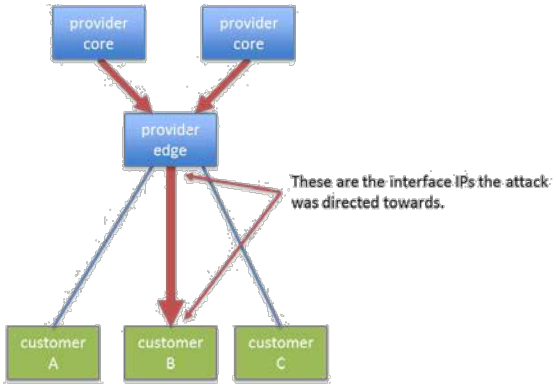
1. El enrutamiento de agujeros negros debe configurarse en los routers de los ISP en caso de que se ataque a un cliente que no esté suscrito a ningún servicio de mitigación de DoS.
2. La instrumentación de la red y las alarmas basadas en el sondeo SNMP, el flujo de red, las sondas o una tecnología similar son fundamentales para detectar rápidamente los problemas de saturación del ancho de banda (15 minutos o menos).
3. La recopilación de flujos de red o alguna tecnología similar debería desplegarse para identificar los objetivos de los ataques y los protocolos objetivo.
4. Los proveedores que ofrezcan servicios de mitigación/limpieza de ataques deben diseñar la infraestructura de manera que el tráfico de ataque no se concentre en una sola zona o centro.

B. Ataque dirigido a las IP de los ISP y de la infraestructura del cliente

Antecedentes: Este ataque volvió a utilizar paquetes UDP/80 (tráfico basura) en gran volumen para agotar el ancho de banda del objetivo. Sin embargo, en este caso el ataque se dirigió primero a la IP de la interfaz del router del cliente y luego a la del ISP.

Medidas de mitigación:

1. El ataque fue identificado junto con una IP de destino a través de netflow.
2. La subred /30 entre el ISP y el cliente fue bloqueada.
3. Posteriormente se aplicaron filtros en los routers fronterizos de los ISP para limitar el tráfico destinado a la infraestructura de los ISP.



Prácticas recomendadas:

- Limitar el tráfico a la infraestructura punto a punto del ISP tanto como sea posible, ya sea mediante el filtrado o el enrutamiento.
- No utilice IPs de infraestructura punto a punto para NAT, terminación de túneles u otro tipo de tráfico que requiera que las IPs sean anunciadas y enrutadas cuando de otra manera no sería necesario.
- Implementar la detección como se sugiere en el Estudio de Caso 1 para que estos ataques puedan ser identificados rápidamente. Tenga en cuenta que cuando una dirección ISP es el objetivo del ataque, el cliente nunca verá el tráfico.

Desafíos potenciales:

- El filtrado en cada punto de entrada del ISP puede ser poco práctico.
- Volver a direccionar una red a un espacio que no está enrutado puede ser una tarea difícil y que requiere mucho tiempo.

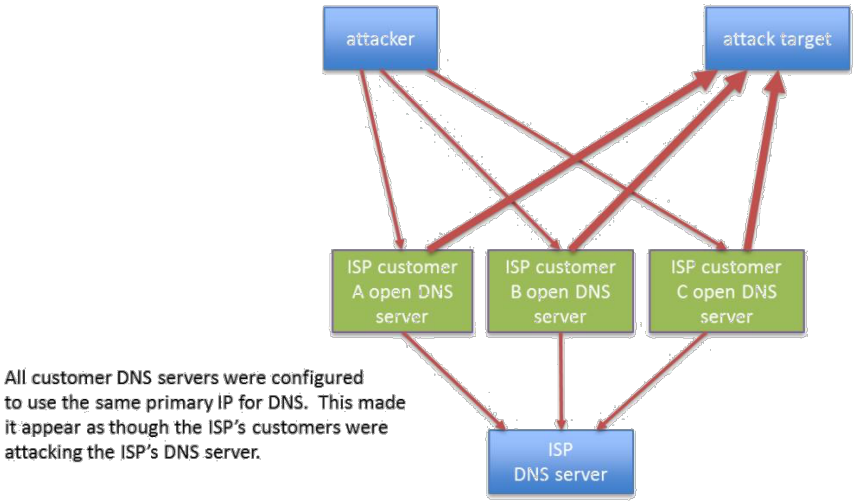
C. Daños colaterales del ataque por reflexión del DNS

Antecedentes: Este ataque volvió a utilizar paquetes UDP/53 falsos (consultas DNS) en gran volumen hacia servidores DNS recursivos sin filtrar para magnificar el ataque y agotar el ancho de banda del objetivo. En este caso, el ISP corría el riesgo de sufrir un impacto adverso a pesar de que el ataque no estaba dirigido al ISP en absoluto.

Medidas de mitigación:

1. El ataque fue identificado junto con una IP de destino a través de netflow, así como el registro configurado en el servidor DNS.
2. Las consultas de los clientes se enrutaron a través de un servicio de mitigación del DoS.

3. El ISP hizo un seguimiento posterior para conseguir que el equipo del cliente se filtrara correctamente.



Prácticas recomendadas:

- Configurar servicios de mitigación de ataques para infraestructuras críticas como los servicios DNS. Algunos ejemplos de mitigación son la depuración del tráfico y la limitación de la velocidad del servicio.
- Ampliar la capacidad de mitigación según sea necesario para los servicios de infraestructura.
- Distribuir los servicios críticos utilizando tecnologías como anycast o redes de distribución de contenidos cuando sea posible.
- Proporcionar una gestión fuera de banda para las infraestructuras críticas de manera que un ataque no impida el acceso a los equipos necesarios para mitigarlo.
- Limitar la exposición de los servicios sólo a aquellos que necesitan acceder a ellos (por ejemplo, DNS, NTP, etc.).
- Evite el uso de equipos configurados con servicios no protegidos, como DNS sin filtrar y cadenas de comunidad SNMP conocidas.
- Aplicar controles anti-spoofing cuando sea práctico y posible, por ejemplo, en redes residenciales y centros de alojamiento.

Desafíos potenciales:

- El suministro de capacidad de mitigación puede ser una "carrera armamentística" con los atacantes.
- Algunos servicios no pueden filtrarse eficazmente sin un impacto colateral inaceptable.
- El anti-spoofing (BCP 38) no es posible para muchos clientes de tránsito.

D. DDoS originado en el gateway/router de casa

- **Antecedentes:** Un determinado proveedor de puertas de enlace domésticas tenía un error que hacía que inundara las solicitudes de DNS a la velocidad de la línea cuando el módem que tenía delante se reiniciaba. El ISP aumentó la velocidad de la banda ancha en su mayor mercado, lo que obligó a reiniciar el módem. Aproximadamente 250 puertas de enlace domésticas empezaron a inundar las solicitudes de DNS, lo que provocó la caída del grupo de DNS del ISP.

- •

- Problemas descubiertos:

- No hay capacidad de mitigación DDOS tan profunda en la red del ISP. Los centros de depuración de datos se sitúan en el borde de la red del ISP.

- Los servidores DNS devolvían información de autoridad adicional y opcional con cada respuesta, lo que provocaba un efecto de amplificación
- Las funciones de limitación de velocidad no se utilizaron en los equilibradores de carga del ISP
- El ISP tenía dificultades para gestionar los servidores DNS a través de las interfaces de consulta, que estaban saturadas debido a la inundación de DNS del módem de banda ancha.

- Medidas de mitigación:

1. Utilización de herramientas de seguridad fuera de banda que capturan paquetes DNS. Configuró las herramientas para contar el número de paquetes vistos durante un periodo de tiempo determinado y generar alertas sobre los clientes que superan esos umbrales.
2. Se introdujeron las alertas en el sistema de gestión de abusos existente y se desconectó a los clientes
3. Automatización del proceso para su uso futuro

Recomendaciones:

- Para cualquier servicio, asegúrate de que devuelve la menor cantidad de información posible para que no se pueda utilizar fácilmente como amplificador.
- Asegúrese de que los servidores sigan siendo accesibles cuando sean atacados, separando las interfaces de gestión de las de servicio.
- Utilizar las funciones de seguridad (como la limitación de velocidad) disponibles en el hardware de red existente.
- La mitigación puede llevarse a cabo fuera de la línea utilizando monitores pasivos que señalan a otras herramientas para que realicen alguna acción.

E. Enrutamiento nulo

Antecedentes: El enrutamiento nulo es la forma más simple de mitigación de DDOS, pero también la que tiene más daños colaterales. Es un martillo que deja caer todo el tráfico destinado a una dirección IP determinada.

Pros:

- Simple y rápido de aplicar
- Deja caer el tráfico en el borde de la red en los enlaces más grandes

Contras:

- Arroja todo el tráfico hacia una IP determinada y no sólo el tráfico malicioso
-

Casos de uso:

- Cliente residencial (u otra IP dinámica) bajo ataque. El ISP puede simplemente eliminar todo el tráfico destinado a la IP objetivo y dar al cliente una nueva
- Ataque de salida. Si una dirección IP de otro ISP está bajo ataque, y ese ISP indica que no hay necesidad legítima de que nuestros clientes lleguen a ella, el primer ISP puede descartar los paquetes antes de que salgan de su red. Ejemplo: el router de otro ISP está siendo atacado. Los clientes del primer ISP no tienen ninguna razón para enviar paquetes directamente a ese router, por lo que anulan el enrutamiento de su ip en nuestra red.

IV. Técnicas de mitigación del ISP (Herramientas/Controles técnicos) Hay dos fases principales para responder a los ataques

DDoS:

Fase 1: Detección

Los ataques DDoS pueden ser detectados por los ISP utilizando métodos volumétricos o basados en la aplicación. Por ejemplo, en el caso de las soluciones basadas en el volumen, los ISP establecerían una línea de base contra la que se pueden determinar las anomalías del tráfico de ataque. Otro medio para detectar los ataques es directamente por parte de los clientes, que también suelen observar por su cuenta aumentos graduales en los volúmenes de tráfico de entrada, y se pondrán en contacto con los ISP en consecuencia.

Detección:

Tipo	De norte a sur	De sur a norte	De este a oeste
Volumétrico	- Basado en Netflow soluciones - Utilización control de Llamada de la - víctima	- Basado en Netflow soluciones Llamada de la - víctima	- Llamada de la víctima
Aplicación[28]	- Basado en DPI soluciones - Basado en el host soluciones Llamada de la - víctima	Soluciones basadas en DPI - Soluciones basadas en host Llamada de la - víctima	- Llamada de la víctima

Fase 2: Mitigación

La fase de mitigación de la actividad de respuesta DDOS tiene como objetivo contrarrestar los efectos de la acción maliciosa. La mitigación suele consistir en (1) filtrar el tráfico malicioso, o (2) reducir la intensidad del ataque degradando el origen de la red de bots. Esta segunda acción puede llevarse a cabo de diversas maneras, como ponerse en contacto con los propietarios de los ordenadores y servidores infectados antes, durante y después de un ataque. Por lo tanto, el objetivo principal de las actividades de seguridad DDoS de los ISP implica todos los intentos posibles de bloquear, desviar, filtrar y ralentizar con éxito el tráfico de ataque incrustado en el flujo normal de tráfico de entrada dirigido a un sitio víctima. Dado que la mayoría de los ataques DDoS son muy variados (a diferencia de los recientes ataques bancarios, que siguieron una cadencia más rutinaria), el proceso de decisión puede ser muy dinámico y suele depender del análisis en tiempo real.

Mitigación:

En general, se suele preferir la técnica de mitigación más sencilla que resuelva el problema. Sin embargo, desde el punto de vista del servicio, se prefieren las técnicas de mitigación más específicas a las que son más contundentes y tienen un mayor impacto en el tráfico legítimo. Como se ha señalado anteriormente, la acción apropiada en una situación determinada depende de las características específicas del ataque y del objetivo.

Las rutas de agujeros negros son la mitigación preferida en el caso de que el servicio o el cliente bajo

[28] Los ataques DDoS en la capa de aplicación pueden ser más difíciles de detectar y, en algunos casos, pueden requerir herramientas más intrusivas que las tradicionales basadas en el volumen, como el uso de la inspección profunda de paquetes (DPI), y también pueden complicarse por el uso de SSL u otro tipo de cifrado.

ataque no sufrirá ninguna degradación o interrupción al perder todo el tráfico hacia el objetivo. Por ejemplo, en el caso de que la dirección de destino nunca necesite recibir ningún tráfico de Internet, una ruta blackhole de esa IP es la respuesta más sencilla. Además, un ataque saliente también podría mitigarse mediante el enrutamiento de agujero negro del objetivo del ataque. Si se requieren servicios de la dirección de destino, pero el ataque utiliza un protocolo o servicio diferente, entonces un filtro de paquetes como una ACL de router puede ser eficaz. Los ataques volumétricos no triviales -los dirigidos a servicios necesarios- suelen requerir servicios de depuración más especializados o soluciones DPI. Estos servicios están diseñados para permitir el paso de la mayor parte del tráfico legítimo y bloquear la mayor parte del tráfico de ataque.

Tipo	De norte a sur	De sur a norte	De este a oeste
Volumétrico	- • Fregado centro/rampa de salida - • ruta del agujero negro - • router ACL - • BGP Flowspec	- • Suspender el ataque servicio - • Control de otros dispositivos, como el bloqueo de puertos de un módem - • ruta del agujero negro - • router ACL	• Suspender el servicio del atacante • Otro control de dispositivos, como el bloqueo de puertos en un módem • ruta del agujero negro • router ACL
Aplicación	- • Fregado centro/rampa de salida - • Basado en DPI soluciones - • Basado en el host soluciones	- • Soluciones basadas en DPI - • Soluciones basadas en host - • Suspender el ataque servicio - • Control de otros dispositivos, como el bloqueo de puertos de un módem	• Suspender el servicio del atacante • Otro control de dispositivos, como el bloqueo de puertos en un módem • Soluciones basadas en host

V. Recomendaciones adicionales

- Los ISPs revisan el conjunto de recomendaciones *ABC para ISPs* para la mitigación de malware publicado por CSRIC III en 2012 dado que muchos ataques DDoS han emanado de usuarios finales infectados.
- Se deben desarrollar mejores prácticas similares para los proveedores de alojamiento en términos de procesos de notificación y de recepción de abusos para alertar a los inquilinos infectados de los centros de alojamiento ante los ataques basados en los centros de datos.
- Los ISP revisan el BCP 38 y otras alternativas para gestionar potencialmente la suplantación de direcciones IP

Estudio de caso del Subgrupo Financiero

Estudio de caso:

Desde finales de 2012 hasta mediados de 2013, las instituciones financieras estadounidenses (USFI) sufrieron continuos ataques de denegación de servicio distribuido (DDoS) contra sus redes. Los análisis indican que algunos de los ataques se originan en un actor de la amenaza de un estado nacional. Estos ataques muestran evidencias de planificación previa y siguen evolucionando en complejidad.

Se cree que los ataques DDoS contra las USFI formaban parte de una estrategia de ataque más amplia y presagian ataques más graves. Las USFIs atacadas representan un componente significativo de la actividad económica estadounidense, son emblemáticas de la estabilidad económica de Estados Unidos y, si se ven comprometidas, podrían suponer un riesgo sistémico para el sector financiero. Los grupos que se atribuyen el mérito han amenazado con más ataques.

¿Qué es un ataque DDOS?

Un ataque DDoS es un ciberataque coordinado con la intención de interrumpir la disponibilidad de un sistema o aplicación de procesamiento de información consumiendo el ancho de banda de la red o abrumando el sistema objetivo con conexiones de datos simultáneas procedentes de múltiples fuentes autónomas. El modelo distribuido ha dado lugar a las redes de bots, que son colecciones de hosts infectados con malware que tienen la capacidad de lanzar ataques DDoS a voluntad del adversario que los controla para cambiar significativamente la velocidad de los ataques.

Tipos de DDoS utilizados:

- Inundación UDP
- Inundación TCP
- Ataques a la función de búsqueda
- Archivo grande GET
- Ataques a nivel de infraestructura
- Ataques al portal de autenticación

Pasos en ataque:

- Puerto 80 SYN Flood con algo de UDP para saturar el ancho de banda de la red si es posible.
- Atacar servidores DNS con paquetes UDP/TCP malformados.
- Atacar los puertos DNS de los servidores web.
- Ataque a las conexiones SSL.
- Las URL (última táctica) cambian del sitio principal a los sitios secundarios.
- Ataques postales HTTP/HTTPS (funciones de búsqueda).
- Puertos 80/443/53

Herramientas:

- Los atacantes utilizan scripts de ataque personalizados enviando tráfico a los puertos 80, 443, 53, 1800

Técnicas de adaptación:

- Volumen significativo (ancho de banda/paquetes) morfología constante (puerto/protocolo).

- Personalización sobre la marcha de los ataques para abordar la mitigación.
- Capacidad de comprometer y luego utilizar servidores infectados con malware con conexiones de gran ancho de banda.
- Capacidad de añadir a los bots y añadir nuevos clientes para evadir los filtros/las listas negras de IP.

Mientras que los ataques en 2012/13 se centraron principalmente en ataques de ancho de banda (Capa 3 y 4), los actores de la amenaza cambiaron y evolucionaron sus capacidades para llevar a cabo ataques más complicados de Capa 7. Mediante el uso de SSL, los actores de las amenazas diseñaron ataques para que el tráfico atacante pareciera tráfico legítimo en un intento de camuflar sus actividades nefastas y engañar a las defensas de la red. Además, los ataques evolucionaron desde objetivos únicos, en los que los atacantes "se quedaban" en un objetivo durante horas o días, hasta ataques contra varias USFI simultáneamente o en rápida sucesión.

Controles técnicos:

1. Limitación de la velocidad del protocolo portador
2. Bloqueo de la IP de origen del transportista
3. Filtrado de agujeros negros de la dirección IP de destino o del protocolo
4. Filtrado de los equilibradores de carga mediante scripts personalizados
5. Cortafuegos de aplicaciones web locales
6. Depuración de datos basada en BGP de terceros
7. Depuración de datos de terceros basada en el DNS
8. Normas del SIP
9. Bloques de red basados en las características de la capa 3 o 4
10. Equipo de detección/mitigación de DDoS in situ
11. Bloqueo del operador basado en la geografía de la IP de origen
13. Limitación de la velocidad de conexión
15. Filtro de tiempo de vida (TTL) de paquetes/sesión in situ
16. Filtrado de puertos/protocolos in situ

Tendencias emergentes

- La arquitectura de las redes de bots es cada vez más sofisticada y difícil de rastrear, y los sistemas C2 (de mando y control) están cada vez más escalonados y utilizan servidores proxy para ocultar la ubicación del sistema que ejecuta los comandos.
- Los dispositivos están cada vez más repartidos por todo el mundo, lo que dificulta la coordinación del cierre de estos sistemas debido a que los países suelen tener leyes diferentes y a veces contradictorias.
- Las redes de bots se están volviendo extremadamente sofisticadas, y algunas tienen la capacidad de borrar todo el disco duro de un sistema comprometido después de haber completado un ataque.
- Las herramientas DDoS son/seguirán siendo más sofisticadas, con capacidades multitarea y multihilo que proporcionarán el potencial para lanzar ataques a múltiples objetivos y servicios simultáneamente.
- Las redes sociales, como Twitter, podrían utilizarse para redirigir y configurar a los zombis como nuevos vectores de ataque.
- Con la proliferación de dispositivos móviles, los adversarios comprometerán e instalarán botnets y los aprovecharán para realizar ataques DDoS.

- Los atacantes han desarrollado la capacidad de monitorear activamente las acciones defensivas y adaptar continuamente sus ataques para intentar vencer la mitigación. Los atacantes han demostrado la capacidad de aumentar los bots, añadiendo nuevos clientes para evadir los filtros/las listas negras de IP.

Estudios de caso del subgrupo de expertos en seguridad de Internet

Caso práctico nº 1: Ataque DDoS saliente/cruzado lanzado por los servidores de un centro de datos de Internet (IDC)

Servidores comprometidos en un IDC debido a versiones vulnerables de software; no hay root, ni tráfico de falsificación.

- Vectores de ataque múltiples y cambiantes: HTTP, HTTP/S, inundaciones de consultas DNS malformadas; GETs a través de HTTP y HTTP/S que consumen el ancho de banda de tránsito saliente en las redes objetivo. Impacto colateral para los usuarios legítimos de los servidores, los operadores de IDC y los operadores de redes de tránsito.

- Alto número de paquetes por segundo (pps) / bits por segundo (bps) por fuente

Caso de estudio #2: Ataque de reflexión/amplificación de DNS aprovechando los recursores de DNS abiertos.

El atacante falsifica la dirección IP del objetivo del ataque, enviando consultas DNS para registros DNS de gran tamaño previamente identificados (registros ANY, registros TXT de gran tamaño, etc.), bien a servidores DNS recursivos abiertos que puedan ser objeto de abuso, o bien directamente a servidores DNS autoritativos.

El atacante elige el puerto UDP al que quiere dirigirse - con DNS, esto se limita normalmente a UDP/53 o UDP/1024-65535. El puerto de destino es UDP/53

Los servidores "responden" directamente al objetivo del ataque o a los servidores recursivos DNS intermedios abiertos con grandes respuestas DNS - el objetivo del ataque verá flujos de respuestas DNS no solicitadas desglosadas en fragmentos iniciales y no iniciales.

El tamaño de las respuestas suele ser de 4096 - 8192 bytes (puede ser menor o mayor), dividido en múltiples fragmentos.

El tamaño de los paquetes que recibe el objetivo del ataque suele ser de ~1500 bytes debido a las MTU de Ethernet predominantes, y son muchas.

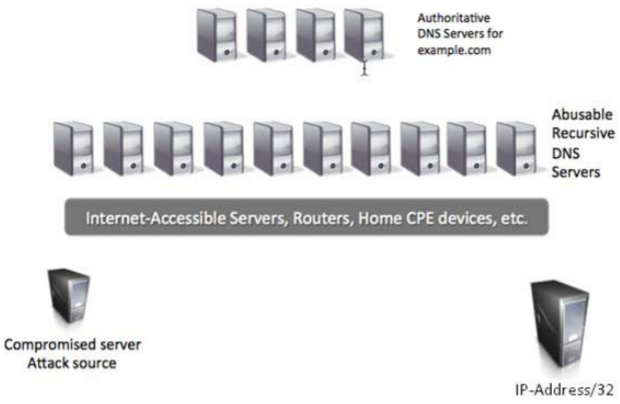
A medida que convergen estos múltiples flujos de respuestas DNS fragmentadas, el volumen de ataque puede ser enorme: el mayor ataque verificado de este tipo hasta ahora es de ~200gb/seg. Los ataques de 100gb/seg son habituales.

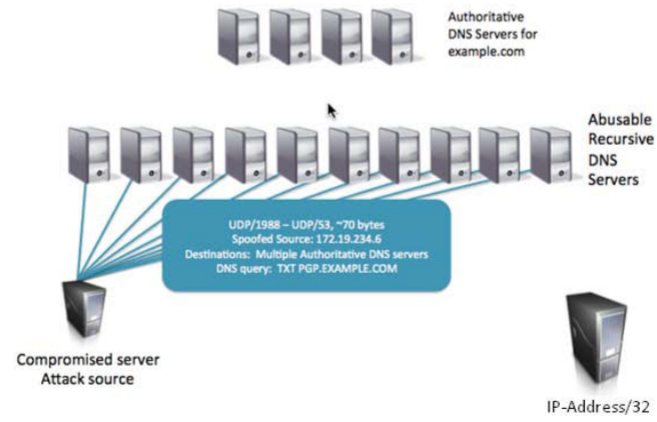
El ancho de banda de tránsito de Internet del objetivo, junto con el ancho de banda central de los pares/sobrecarga del objetivo, así como el ancho de banda central de las redes intermediarias entre los distintos servicios DNS de los que se abusa y el objetivo, están saturados.

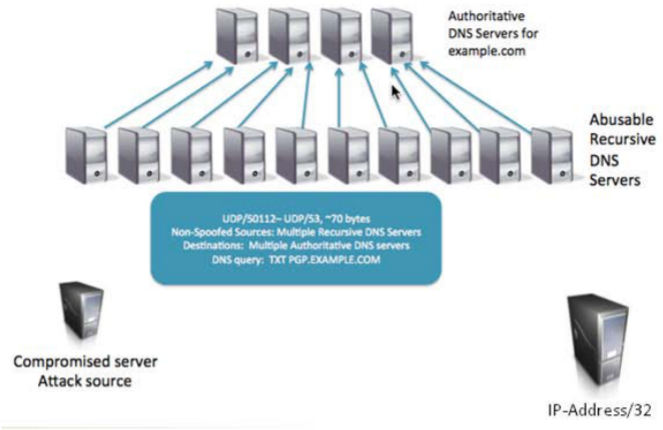
En la mayoría de los ataques que implican servidores DNS recursivos abiertos intermedios son reflectores, entre ~20.000 - 30.000 DNS recursivos abusables son aprovechados por los atacantes. En algunos ataques se han observado hasta 50.000 servidores DNS recursivos abiertos abusables.

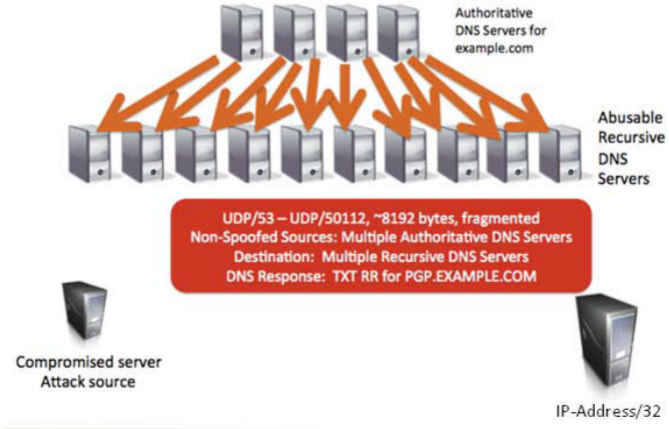
En los ataques que aprovechan directamente los servidores DNS autorizados, los atacantes utilizan cientos o miles de estos servidores.

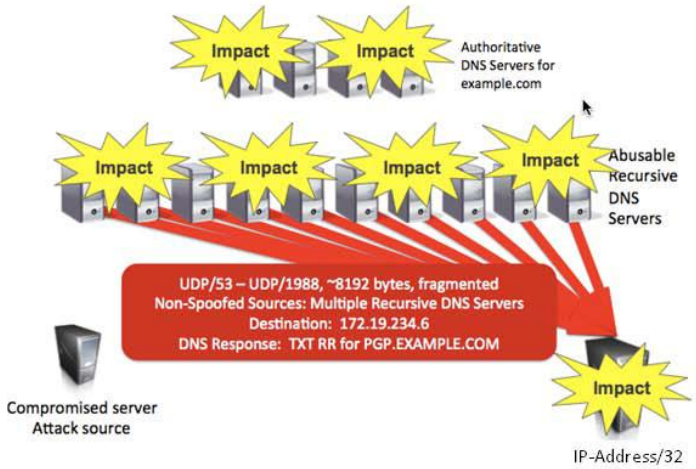
Muchos de los servidores DNS autorizados más conocidos son anycasted, con múltiples instancias desplegadas en Internet.






Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/50112– UDP/53, ~70 bytes
Non-Spoofed Sources: Multiple Recursive DNS Servers
Destinations: Multiple Authoritative DNS servers
DNS query: TXT PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32


Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/53 – UDP/50112, ~8192 bytes, fragmented
Non-Spoofed Sources: Multiple Authoritative DNS Servers
Destination: Multiple Recursive DNS Servers
DNS Response: TXT RR for PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32



Estudio de caso nº 3: Servidor web de la red empresarial de punto final atacado por reflexión/amplificación de ntp.

El atacante falsifica la dirección IP del objetivo del ataque, envía monlist, showpeers u otras consultas administrativas de nivel 6/-7 de NTP a múltiples servicios NTP abusables que se ejecutan en servidores, routers, dispositivos CPE domésticos, etc.

El atacante elige el puerto UDP al que quiere dirigirse -normalmente, UDP/80 o UDP/123, pero puede ser cualquier puerto a elección del atacante- y lo utiliza como puerto de origen. El puerto de destino es UDP/123.

Los servicios NTP "responden" al objetivo del ataque con flujos no suplantados de paquetes de ~468 bytes procedentes de UDP/123 hacia el objetivo; el puerto de destino es el puerto de origen que el atacante eligió al generar las consultas NTP monlist/showpeers/etc.

A medida que convergen estos múltiples flujos de respuestas NTP no falsificadas, el volumen de los ataques puede ser enorme
- el mayor ataque verificado de este tipo hasta ahora es de más de 400gb/seg. Los ataques de 100gb/seg son habituales.

Debido al gran volumen de los ataques, el ancho de banda de tránsito de Internet del objetivo, junto con el ancho de banda central de los pares/subidas del objetivo, así como el ancho de banda central de las redes intermediarias entre los diversos servicios NTP de los que se está abusando y el objetivo, se satura con tráfico de ataque no falsificado.

En la mayoría de los ataques, los atacantes aprovechan entre ~4.000 y ~7.000 servicios NTP abusables. En algunos ataques se han observado hasta 50.000 servicios NTP.

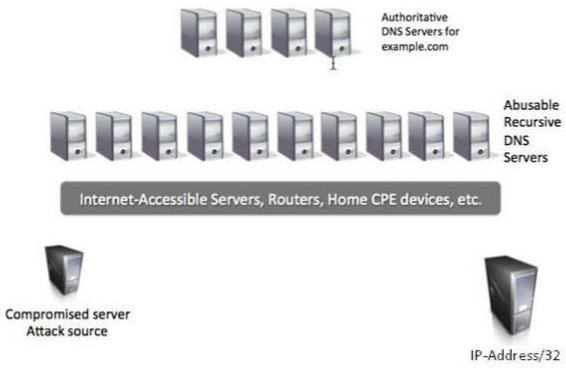
Servidores, servicios, aplicaciones, acceso a Internet, etc., en la red de destino abrumados e indisponibles por el mero volumen de tráfico: decenas o cientos de gb/seg. frecuentes.

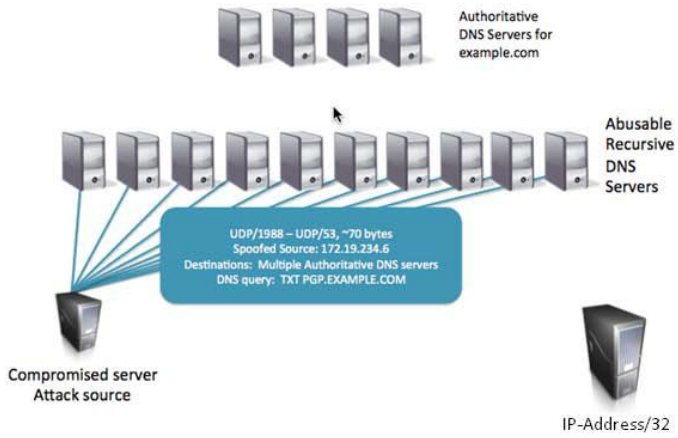
Saturación completa de los enlaces de peering/tránsito de la red de destino.

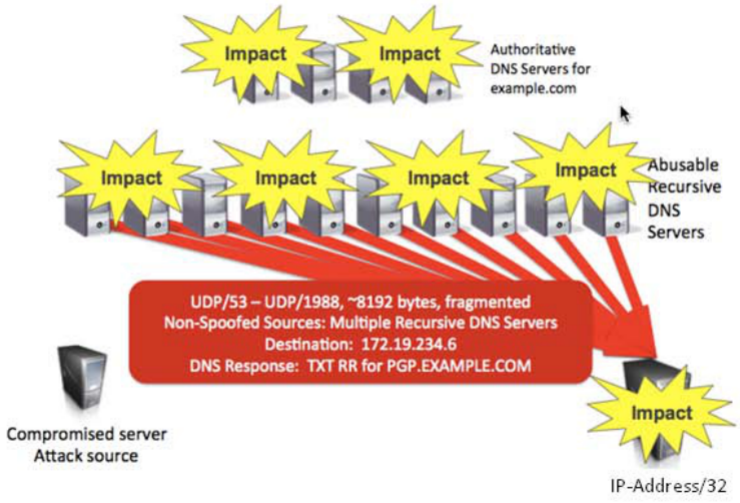
Saturación total o casi total de los enlaces de peering/enlaces de tránsito/enlaces centrales de las redes intermedias entre los reflectores/amplificadores NTP y la red de destino - incluyendo las redes de los pares/proveedores de tránsito directos de la red de destino

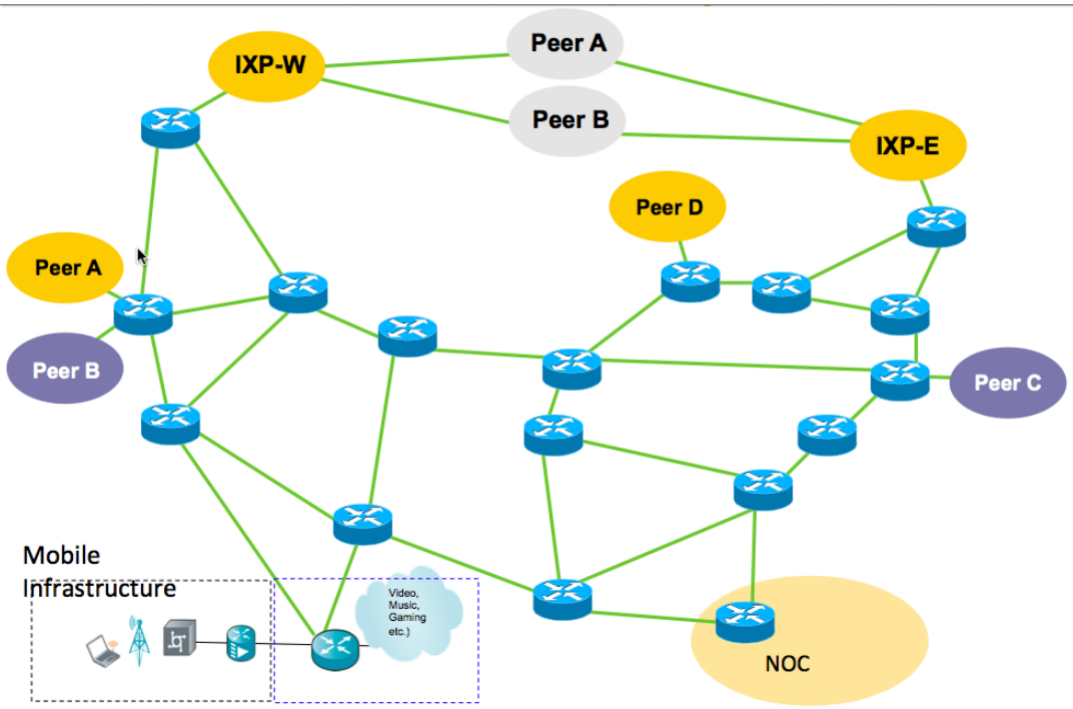
Daños colaterales generalizados: pérdida de paquetes, retrasos, alta latencia para el tráfico de Internet de las partes no implicadas que simplemente atraviesan las redes saturadas por estos ataques.

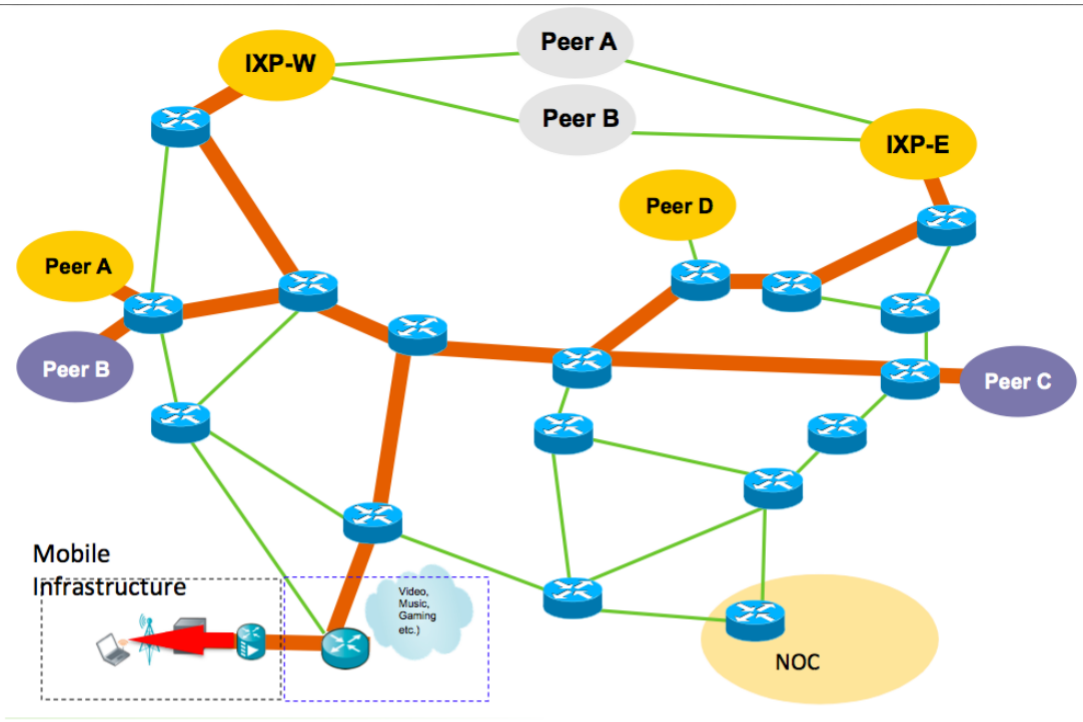
Indisponibilidad de servidores/servicios/aplicaciones, acceso a Internet para transeúntes topológicamente próximos a la red objetivo.

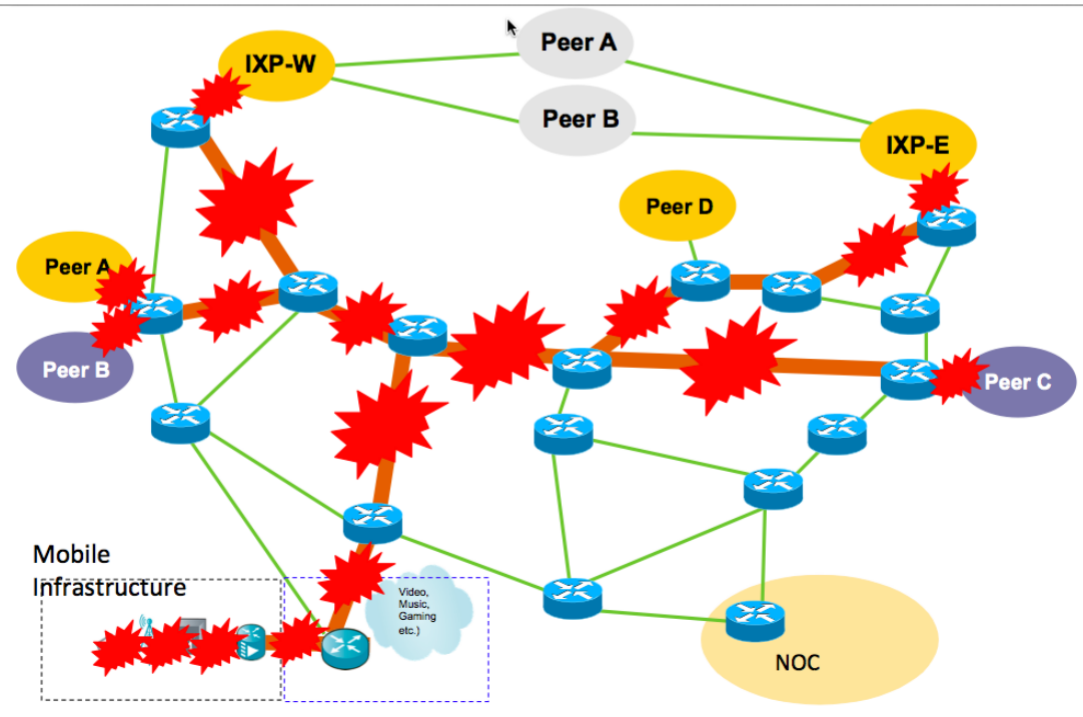

Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
Internet-Accessible Servers, Routers, Home CPE devices, etc.
Compromised server
Attack source
IP-Address/32


Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/1988 – UDP/53, ~70 bytes
Spoofed Source: 172.19.234.6
Destinations: Multiple Authoritative DNS servers
DNS query: TXT PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32


Impact
Impact
Authoritative DNS Servers for example.com
Impact
Impact
Impact
Impact
Abusable Recursive DNS Servers
UDP/53 – UDP/1988, ~8192 bytes, fragmented
Non-Spoofed Sources: Multiple Recursive DNS Servers
Destination: 172.19.234.6
DNS Response: TXT RR for PGP.EXAMPLE.COM
Compromised server
Attack source
Impact
IP-Address/32


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile Infrastructure
Video, Music, Gaming etc.)
NOC


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile
Infrastructure
Video,
Music,
Gaming
etc.)
NOC


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile
Infrastructure
Video,
Music,
Gaming
etc.)
NOC

Apéndice E: Mejores prácticas

Introducción a las mejores prácticas

Las mejores prácticas son declaraciones que describen la orientación de la industria para sí misma sobre el mejor enfoque para abordar un problema. Son el resultado de una cooperación sin parangón en el sector, que cuenta con una amplia experiencia y considerables recursos. El objetivo principal de las Mejores Prácticas es proporcionar orientación a partir de la experiencia y los conocimientos del sector. La aplicación de las Mejores Prácticas debe ser voluntaria. La decisión de aplicar o no una práctica recomendada específica se deja en manos de la organización responsable (por ejemplo, el proveedor de servicios, el operador de red o el proveedor de equipos). Además, la aplicabilidad de cada Buena Práctica para una circunstancia determinada depende de muchos factores que deben ser evaluados por personas con la experiencia y los conocimientos adecuados en el mismo ámbito al que se refiere la Buena Práctica.

Las Mejores Prácticas recomendadas por el Grupo de Trabajo 5 del CSRIC IV pretenden servir de orientación. La decisión de implantar o no una Buena Práctica específica debe dejarse en manos de la organización responsable (por ejemplo, el proveedor de servicios, el operador de red o el proveedor de equipos). La aplicación obligatoria de estas Buenas Prácticas no es coherente con su propósito. La aplicación adecuada de estas Mejores Prácticas sólo puede ser realizada por personas con suficiente conocimiento de la arquitectura de la infraestructura de red específica de la empresa para entender sus implicaciones. Aunque las Buenas Prácticas están escritas para que sean fácilmente comprensibles, su significado a menudo no es evidente para aquellos que carecen de este conocimiento y experiencia previos. La aplicación adecuada requiere la comprensión del impacto de las Mejores Prácticas en los sistemas, procesos, organizaciones, redes, suscriptores, operaciones comerciales, cuestiones de costes complejos y otras consideraciones. Con estas importantes consideraciones sobre el uso previsto, a las partes interesadas del sector les preocupa que las autoridades gubernamentales puedan imponerlas inadecuadamente como reglamentos u órdenes judiciales. Dado que estas Mejores Prácticas se han desarrollado como resultado de una amplia cooperación de la industria que involucra una vasta experiencia y considerables recursos voluntarios, tal uso indebido de estas Mejores Prácticas puede poner en peligro la voluntad de la industria de trabajar juntos para proporcionar dicha orientación en el futuro. [29]

[29] Estos principios se han extraído del trabajo del Grupo de discusión 3B de la RNIC VII, Informe final sobre la fiabilidad de la red pública de datos, apartados 2.3.2 y 3.4.2.

El WG5 ha identificado las siguientes categorías de buenas prácticas para mitigar los problemas de los servidores
Ataques DDoS:

Preparación
Identificación
Clasificación
Rastreo
Reacción
Post mortem y recuperación

Las siguientes Buenas Prácticas abordan los ataques DDoS basados en el servidor.

Operadores de red

Preparación

Número de BP: Nuevo BP2
Filtrado de agujeros negros basado en el destino / Filtrado de agujeros negros basado en el destino activado a distancia:
Los operadores de red deberían desplegar el filtrado de agujeros negros basado en el destino (BHF) para proteger sus redes de los ataques DDoS. Los operadores de red deberían, cuando sea factible, proporcionar un filtrado de agujeros negros en el destino iniciado por el cliente (RTBHF) para el espacio IP de un cliente.
Referencia/Comentarios de BP:
El RFC 4778 es útil como respuesta inicial para controlar el ataque mientras se verifica su impacto y se reconfigura la red.
Tenga en cuenta que una vez que el filtrado Black Hole está en su lugar, completa el ataque DDoS dejando caer todo el tráfico hacia el destino. El tráfico hacia el destino puede reanudarse asignando nuevas direcciones IP al destino y anunciando los nuevos registros DNS..
Fase: Preparación (Despliegue de herramientas de mitigación, operador de red, filtrado de alojamiento)
Orientación para la aplicación: Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): M

Número de BP: Nuevo BP8
Despliegue de tecnologías anti-spoofing:
Los operadores de redes y los proveedores de alojamiento deberían, siempre que sea posible, desplegar tecnologías anti-spoofing para evitar que el tráfico falsificado se origine en sus redes.
Referencia/Comentarios de BP:
Relacionado con BP 9-7-0408
Hay que tener en cuenta que el despliegue puede no ser factible en algunas redes multi-homed debido a la necesidad de enrutamiento asimétrico.
Fase: Preparación (proteger, operador de red, proveedores de alojamiento)

Orientación para la aplicación: Eficacia (H/M/L):
Redes domésticas individuales: H
Redes multihomologadas: M a L

Dificultad de aplicación: (H/M/L):
Redes domésticas individuales: L
Redes multihomes: H

Número BP: Nuevo BP16
Implantar la depuración de datos de la red:
Los operadores de red deben emplear, cuando sea posible, centros de depuración de datos de red para filtrar el tráfico de ataques DDoS. Esto puede lograrse "desviando" el tráfico de ataque DDoS sospechoso a un centro de depuración de la red, donde el tráfico de ataque puede ser filtrado, y "desviando" el tráfico legítimo de vuelta al objetivo.

Referencia/Comentarios de BP:

Es importante dimensionar la capacidad de la red y de los centros de depuración para acomodar el tráfico de ataques, de manera que se minimicen los posibles daños colaterales causados por grandes oleadas de tráfico. Fase: Preparación (despliegue de herramientas de mitigación, operador de red)

Orientación para la aplicación: Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-8-8047

Protéjase contra los ataques de denegación de servicio del DNS (sistema de nombres de dominio):

Los operadores de red deben proporcionar protección DoS de DNS proporcionando una defensa en profundidad para prevenir ataques que harían que el DNS no estuviera disponible, implementando técnicas de protección como:

1) Aumentar la resistencia del DNS a través de la redundancia y las conexiones de red robustas, por ejemplo, desplegar múltiples servidores con diversas conectividades de red para cada servicio, de manera que cualquier servidor o sitio no afecte a los demás. Despliegue anycast para mejorar la redundancia de sus servidores DNS. Anycast puede utilizarse para proporcionar un servicio DNS desde una única dirección IP DNS utilizando múltiples servidores DNS en la red, mejorando así la capacidad de recuperación de DNS. Tenga en cuenta que Anycast aborda la redundancia de la red y no proporciona el equilibrio de carga entre los nodos DNS.
2) Disponer de servidores de nombres separados para el tráfico interno y externo, así como para las infraestructuras críticas, como las redes de OAM&P y de señalización/control,
3) Siempre que sea posible, separe los servidores DNS de caché o recursivos de los servidores DNS autoritativos,
4) Proteja la información del DNS protegiendo los servidores de nombres maestros con reglas de filtrado/cortafuegos debidamente configuradas, implemente maestros secundarios para toda la resolución de nombres y utilice listas de control de acceso para limitar las solicitudes de transferencia de zonas a las partes autorizadas.
5) Configurar la instrumentación de la red para alertar a los equipos de operaciones de los proveedores sobre volúmenes de tráfico anómalos.
6) Diseñar el filtrado de la red DNS en las arquitecturas DNS para permitir el filtrado a nivel de red y de aplicación de tráfico DNS específico (dominios, tipos de consulta, IPs de origen, tasas de consulta, etc.) durante un ataque; esto debe ser configurado de antemano. Esta configuración debe minimizar la interferencia con el tráfico DNS legítimo.
7) Disponer de conectividad de gestión fuera de banda para los servidores DNS, de modo que los servidores puedan ser gestionados durante un ataque.
8) Separar los servidores DNS de caché de los servidores autoritativos.
9) No utilice servidores DNS orientados a Internet para las operaciones de la red interna, sistemas de administración, mantenimiento y aprovisionamiento.
10) Proporcionar un servidor DNS robusto y una capacidad de ancho de banda superior al tráfico máximo de la conexión de red

Referencia/Comentarios de BP:

RFC-2870, ISO/IEC 15408, ISO 17799, US-CERT "Securing an Internet Name Server" (http://www.cert.org/archive/pdf/dns.pdf).
Fase: Preparación (capacidad y recursos, operador de la red)

Orientación para la aplicación:Eficacia (H/M/L):H
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-8-8753A - Nuevo BP (antes BP 9-8-8563)
Actualizado a:
Gestión de la vulnerabilidad - Notificación:

Cuando se descubra una vulnerabilidad o un exploit DoS o DDoS, los operadores de red, los proveedores de alojamiento y los vendedores de hardware/software deben notificar el problema a los propietarios/operadores de los sistemas afectados para garantizar que el software, las configuraciones o los equipos se actualicen para remediar la vulnerabilidad. Si no es posible una reparación a corto plazo, los propietarios/operadores deben considerar la posibilidad de mitigar el sistema o la red para minimizar la probabilidad de explotación de los ataques DDoS.

Referencia/Comentarios de BP:

Instituto Sans, "Gestión de la vulnerabilidad: Herramientas, retos y mejores prácticas". 2003. Pg.
12 - 13.
Preparación (Proteger) BP
Fase: Preparación (proteger, operador de red, proveedores de alojamiento)
Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-9-8068

Los proveedores de servicios, los operadores de redes, los proveedores de alojamiento, la seguridad pública y los proveedores de equipos deben elaborar y poner en práctica un plan de comunicaciones como parte del plan más amplio de respuesta a incidentes, en el que se identifique a los actores clave y se incluya el mayor número posible de los siguientes elementos: nombres de contacto, números de teléfono de la empresa, números de teléfono del domicilio, números de buscapersonas, números de fax, números de teléfono móvil, direcciones del domicilio, direcciones de Internet, números de puente permanente, etc. Los planes de notificación deben elaborarse antes de que se produzca un suceso/incidente cuando sea necesario. El plan también debe incluir canales de comunicación alternativos (por ejemplo, buscapersonas alfa, Internet, teléfonos por satélite, VOIP, líneas privadas, teléfonos inteligentes) equilibrando el valor de cualquier método alternativo con los riesgos de seguridad y pérdida de información introducidos.

Referencia/Comentarios de BP:

Vía de comunicación de banda ancha alternativa para la coordinación y la gestión. Fase: Preparación (comunicación, operador de red, proveedor de alojamiento)
Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): L

Número de BP: 9-8-8753
Actualizado a:
Gestión de la vulnerabilidad:

Los operadores de redes, los proveedores de alojamiento y los vendedores de hardware y software deben asegurarse de que pueden gestionar las vulnerabilidades de seguridad de los productos que gestionan o mantienen para los clientes. Esta gestión puede ser pasiva, como el simple mantenimiento de una lista de clientes a los que han distribuido el producto, o activa, como el escaneo de vulnerabilidades y la presentación de informes. Además, los productos, servicios, hardware y software deben ser probados para detectar vulnerabilidades antes de su despliegue significativo.

Referencia/Comentarios de BP:

Instituto Sans, "Gestión de la vulnerabilidad: Herramientas, retos y mejores prácticas". 2003. Pg.
12 - 13.
Preparación (Proteger) BP
Fase: Preparación (proteger, operador de red, proveedores de alojamiento)
Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-8-8912

Comunicar la aplicación de las medidas de protección y conocimiento de la situación con otros operadores de la red:

Los operadores de red deben hacer esfuerzos razonables para comunicarse con otros operadores y proveedores de software de seguridad, enviando y/o recibiendo informes de abuso a través de métodos manuales o automatizados. Esto es especialmente importante en el caso de los ataques DDoS para notificar a las fuentes de tráfico DDoS su participación en el ataque. Este intercambio de información y colaboración es necesario para ayudar a prevenir futuros ataques. Estos esfuerzos pueden incluir información como la aplicación de "medidas de protección", como la notificación de abusos (por ejemplo, spam) a través de bucles de retroalimentación (FBL) utilizando formatos de mensajes estándar como el Formato de Notificación de Abusos (ARF). Siempre que sea posible, los operadores de red deben participar en los esfuerzos de otros participantes de la industria y otros miembros del ecosistema de Internet con el objetivo de implementar un intercambio de información más sólido y estandarizado en el área de la detección de botnets entre los proveedores del sector privado.

Referencia/Comentarios de BP:

Hay que tener en cuenta que la creación de mecanismos de comunicación con otros Operadores de Red debe realizarse con antelación a un ataque para que los canales de comunicación estén disponibles durante un ataque si es necesario.
Para más información, consulte el siguiente documento:
http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf
Las vulnerabilidades pueden notificarse de forma estandarizada utilizando la información proporcionada en
http://nvd.nist.gov/
http://puck.nether.net/mailman/listinfo/nsp-security
https://ops-trust.net/
https://www2.icsalabs.com/veris/
https://stix.mitre.org/
Fase: Preparación (comunicación, operador de red)
Post mortem y recuperación
Orientación para la aplicación:Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): M

Tenga en cuenta que las mejores prácticas de esta agrupación se dirigen principalmente a los ISP que prestan servicio a los consumidores finales en redes de banda ancha residenciales, pero también pueden ser aplicables a otros usuarios y redes.

Número de BP: 9-8-8917

Notificación a los usuarios finales:

Los operadores de red y los proveedores de alojamiento deberían desarrollar y mantener métodos de notificación críticos para comunicar a sus clientes que su ordenador, servidores y/o red han sido probablemente infectados con malware. Esto debería incluir una gama de opciones para adaptarse a un grupo diverso de clientes y tecnologías de red. Una vez que el Operador de Red ha detectado un probable problema de seguridad del usuario final, deben tomarse medidas para informar al usuario de Internet de que puede tener un problema de seguridad. Un Operador de Red o Proveedor de Alojamiento debe decidir el método o métodos más apropiados para proporcionar la notificación a sus clientes o usuarios de Internet, y debe utilizar métodos adicionales si el método elegido no es efectivo. La gama de opciones de notificación puede variar en función de la gravedad y/o criticidad del problema.

Los ejemplos de los diferentes métodos de notificación pueden incluir, pero no se limitan a: correo electrónico, llamada telefónica, correo postal, mensajería instantánea (IM), servicio de mensajería corta (SMS), y la notificación del navegador web.

Referencia/Comentarios de BP:

Una decisión del Operador de Red y del Proveedor de Alojamiento sobre el método más apropiado o métodos de notificación a uno o varios de sus clientes o usuarios de Internet depende de una serie de factores, desde las capacidades técnicas del operador de la red, a los atributos técnicos de la red del Operador de Red, consideraciones de coste, los recursos disponibles del servidor, los recursos disponibles de la organización, el número de hosts infectados detectados en un momento dado, y la gravedad de las posibles amenazas, entre
muchos otros factores. El uso de múltiples métodos de notificación simultánea es razonable para un operador de red, pero puede ser difícil para un falso proveedor de antivirus. Tenga en cuenta que el uso de las Notificaciones ciegas, es decir, las Notificaciones sin seguimiento, han resultado ser menos eficaz que los métodos que verifican o requieren la acción del usuario. La práctica recomendada 9-8-8921 establece información sobre cómo hacer frente a la infección de malware.

Fase: Preparación (comunicación, operador de red, proveedor de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): L

Dificultad de aplicación: (H/M/L): M

Tenga en cuenta que las mejores prácticas de esta agrupación se dirigen principalmente a los ISP que prestan servicios a los consumidores finales en redes de banda ancha residenciales, pero también pueden ser aplicables a otros usuarios y redes.

Número de BP: 8-9-8074

Actualizado

Ataque de denegación de servicio (DoS) - Objetivo:

Siempre que sea posible, los operadores de red, los proveedores de alojamiento y las redes de destino, así como los equipos de los proveedores de equipos, deberían ser capaces de sobrevivir a aumentos significativos tanto en el número de paquetes como en la utilización del ancho de banda. Siempre que sea posible, los proveedores de equipos y software deberían desarrollar características efectivas de supervivencia al DoS/DDoS para sus líneas de productos..

La infraestructura que soporta los servicios de misión crítica debe estar diseñada para un aumento significativo del volumen de tráfico y debe incluir dispositivos de red capaces de filtrar y/o limitar la velocidad del tráfico. Los ingenieros de red deben comprender las capacidades de los dispositivos y cómo emplearlos para obtener el máximo efecto. Siempre que resulte práctico, los sistemas de misión crítica deben desplegarse en una configuración de clústeres que permita el equilibrio de carga del exceso de tráfico y estar protegidos por un dispositivo de protección DoS/DDoS especialmente diseñado. Los operadores de infraestructuras críticas deben desplegar hardware y software de supervivencia al DoS siempre que sea posible.

Referencia/Comentarios de BP:

Nota: Esta Buena Práctica podría afectar a las operaciones del 9-1-1.
Por ejemplo, defensa contra ataques SYN Flood, CERT/CC ® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks - http://www.cert.org/advisories/CA-1996-21.html. Relacionado con NRIC BP 8753A.

Tenga en cuenta que, los operadores de red, los proveedores de alojamiento, los objetivos y los proveedores de equipos deben determinar qué servicios son de misión crítica en la aplicación de esta Buena Práctica.
Fase: Preparación (capacidad y recursos, operador de red, proveedor de alojamiento, objetivo)

Orientación para la aplicación:Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-9-8725

Actualizado a:

Protección DoS de señalización:

Los operadores de red deben establecer umbrales de alarma para varios indicadores de tráfico para asegurar que se reconocen las condiciones de DoS/DDoS. Los ejemplos incluyen la comparación de las líneas de base de los niveles de tráfico normales en los puntos clave de la red con los niveles de tráfico actuales, y la comparación de la línea de base de la información de flujo de red tanto para los niveles de tráfico como para los protocolos con los niveles de tráfico actuales.

Referencia/Comentarios de BP:

Nota: Esta mejor práctica podría afectar a las operaciones del 9-1-1.

Los umbrales de alarma están destinados a reconocer las condiciones de DoS que pueden ser una amenaza para la infraestructura del operador.
Fase: Preparación (Control y visibilidad, operador de la red)

Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): M

Número de BP: Nuevo BP3

Enrutamiento de los sumideros:

Los operadores de red deben desplegar el Sinkhole Routing para dirigir el tráfico de ataque a otras partes de la red para su análisis (sinkholing) y su caída (offramping).

Referencia/Comentarios de BP:

Fase: Preparación (Despliegue de herramientas de mitigación, operador de red, filtrado de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

El RFC 4778 puede utilizarse junto con Anycast para proporcionar redundancia.

Número de BP: Nuevo BP4
Filtrado de agujeros negros basado en la fuente:

Los operadores de red deberían desplegar el filtrado de agujeros negros basado en la fuente (SBBHF) o mecanismos dinámicos similares que activen el filtrado en toda la red basado en la información de la cabecera del paquete de origen para proteger sus redes de los ataques DDoS. Tenga en cuenta que esto puede no ser tan eficaz si se utiliza un gran número de direcciones IP de origen en el ataque, por ejemplo, un ataque de botnet, o el tráfico de ataque utiliza direcciones IP falsas para la ofuscación.

Referencia/Comentarios de BP:

Greene, Barry Raveendran. "Fase 1 - Preparar las herramientas y técnicas, utilizando el enrutamiento IP como herramienta de seguridad". ISP Security Bootcamp Singapore 2003. 31 de julio de 2003 ftp://ftp-eng.cisco.com/cons/isp/security/ISP-Security-Bootcamp-Singapore-2003/H-Preparation-Tools-v3-0.pdf
Fase: Preparación (Despliegue de herramientas de mitigación, operador de red, filtrado de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): M

Número de BP: Nuevo BP5
Despliegue de la distribución automática de los filtros de tráfico:

Los operadores de red deben desplegar sistemas, como BGP Flowspec, que distribuyan automáticamente los filtros de tráfico a los dispositivos pertinentes en caso de un ataque DOS/DDoS. Estos sistemas pueden permitir que el tráfico de ataque a un objetivo sea filtrado (scrubbed) mientras se permite el tráfico legítimo.

Referencia/Comentarios de BP:

RFC 5575, RFC 4360
Fase: Preparación (Despliegue de herramientas de mitigación, operador de red, filtrado de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): H

Tenga en cuenta que actualmente no todos los proveedores de routers son compatibles con esta tecnología.

Número de BP: Nuevo BP9
Priorización del tráfico para garantizar que el tráfico crítico, por ejemplo, el plano de control, no se vea afectado por el ataque DDOS basado en el servidor:

Los operadores de red deben priorizar el plano de control y otro tráfico crítico sobre el tráfico de tránsito para garantizar que el tráfico de ataques DDoS no afecte al funcionamiento del protocolo de enrutamiento.

Referencia/Comentarios de BP:

Fase: Preparación (capacidad y recursos, operador de la red)
Orientación para la aplicación: Eficacia (H/M/L): H

Dificultad de aplicación: (H/M/L): M

Número de BP: Nuevo BP14
Evitar que los servicios DNS sean utilizados en ataques de reflexión:

Los operadores de red deben aplicar protecciones para evitar que sus servicios DNS sean

utilizados como parte de un ataque de reflexión, si resulta práctico. Estas protecciones pueden incluir, pero no están limitadas a:

1. Limitar los servidores DNS recursivos para que sólo respondan a las consultas del menor conjunto práctico de subredes IP necesarias para el servicio.
2. Implementar procesos de instrumentación y alarma para detectar dominios, IPs y servidores que estén siendo abusados en un ataque.
3. Configure los controles para permitir la mitigación de ataques específicos, como los límites de la tasa de consulta, la eliminación de dominios específicos o el filtrado de los tipos de consulta que se pueden aplicar cuando se detecta un ataque.
4. Tener capacidad de detección de anomalías de tráfico y de respuesta.
5. Implantar sistemas de validación de protocolos DNS, cuando proceda, para descartar el tráfico DNS ilegítimo o malicioso.

Referencia/Comentarios de BP:

Esta BP sustituye a la BP 9-8-8118

Obsérvese que, dado que el número de servidores DNS bajo el control del Operador de Red es bajo en comparación con el número total de servidores DNS desplegados, el impacto de la aplicación de esta Buena Práctica sólo por parte de los Operadores de Red en el problema general de los servidores DNS abiertos que se utilizan en los ataques de reflexión es bajo.

Fase: Preparación (proteger, operador de red, capacidad y recursos, operador de red)

Orientación para la aplicación:	Eficacia (H/M/L): L Dificultad de aplicación: (H/M/L): M

Identificación

Número de BP: 9-8-8916

Actualizado a:

La detección de bots y la correspondiente notificación deben ser oportunas:

Los operadores de red y los proveedores de alojamiento deben asegurarse de que la detección de bots y la correspondiente notificación a los clientes de alojamiento se realicen a tiempo, ya que estos problemas de seguridad son sensibles al tiempo. Si se requiere un análisis complejo y se necesitan múltiples confirmaciones para confirmar que un bot está realmente presente, entonces es posible que el malware pueda causar algún daño, ya sea en el host infectado o en el sistema objetivo remoto (más allá del daño de la infección inicial) antes de que pueda ser detenido. Así pues, un operador de red o un proveedor de alojamiento debe equilibrar el deseo de confirmar definitivamente una infección de malware, lo que puede llevar un largo período de tiempo, con la capacidad de predecir la fuerte probabilidad de una infección de malware en un período de tiempo muy corto. Este desafío "definitivo-vs. probable" es difícil y, en caso de duda, los operadores de redes y los proveedores de alojamiento deberían pecar de precavidos y comunicar una probable infección de malware, al tiempo que toman medidas razonables para evitar las notificaciones de falsos positivos.

Referencia/Comentarios de BP:

La implementación de la notificación por parte del operador de red necesita equilibrar la certeza de una infección detectada con la incertidumbre de una detección transitoria de tráfico malicioso para minimizar la posibilidad de notificaciones falsas-positivas que podrían convertirse en una molestia para los clientes y llegar a ser inmanejables por el operador de red.

Puede encontrar más información en el Código de Conducta Anti-Bot de los Estados Unidos (ABC) para el servicio de Internet
Proveedores (ISP):
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

Fase: Identificación (supervisión y visibilidad, operador de red, proveedor de alojamiento)
Orientación para la aplicación: Eficacia (H/M/L): L (sólo notificación)
Dificultad de aplicación: (H/M/L): M

Tenga en cuenta que las mejores prácticas de esta agrupación se dirigen principalmente a los ISP que prestan servicio a los consumidores finales en redes de banda ancha residenciales, pero también pueden ser aplicables a otros usuarios y redes.

Número de BP: Nuevo BP6
Utilice el análisis de datos de Netflow para analizar los ataques DDoS:

Cuando sea posible, los operadores de red y los proveedores de alojamiento deberían permitir, recopilar y analizar los datos de Netflow para ayudar a la identificación y clasificación de los ataques DDoS. Los datos deben estar disponibles después del ataque para permitir un análisis posterior. Los datos de Netflow deben conservarse de acuerdo con la política de conservación de datos del operador de red.

Referencia/Comentarios de BP:

Los datos de Netflow pueden ser útiles para identificar ataques de spoofing.
Fase: Identificación (supervisión y visibilidad, operador de red, proveedores de alojamiento)
Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): M

Número de BP: 9-8-8913
Mantener los métodos para detectar la infección de bots/malware:

Los operadores de redes deben mantener métodos para detectar posibles infecciones de malware en los equipos de los clientes. Los métodos de detección pueden variar mucho debido a una serie de factores. Los métodos, herramientas y procesos de detección pueden incluir, entre otros, los siguientes: retroalimentación externa, observación de las condiciones y el tráfico de la red, como el análisis del ancho de banda y/o del patrón de tráfico, firmas, técnicas de comportamiento y supervisión forense de los clientes a un nivel más detallado.

Referencia/Comentarios de BP:

Puede encontrar más información en:
http://teamcymru.org
http://shadowserver.org
http://abuse.ch
http://cbl.abuseat.org
Código de Conducta Anti-Bot de los Estados Unidos (ABC) para los proveedores de servicios de Internet (ISP):
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf
Tenga en cuenta que las mejores prácticas de esta agrupación se dirigen principalmente a los ISP que prestan servicio a los consumidores finales en redes de banda ancha residenciales, pero también pueden ser aplicables a otros usuarios y redes.
Fase: Identificación (Control y visibilidad, operador de la red)

Dificultad de aplicación: (H/M/L): H

Número de BP: 9-8-8914

Utilice un enfoque de detección de bots por niveles:

Los operadores de redes deben utilizar un enfoque escalonado para la detección de botnets que primero aplique las características de comportamiento del tráfico de los usuarios (lanzar una red amplia), y luego aplique técnicas más granulares (por ejemplo, detección de firmas) al tráfico marcado como un problema potencial.

Referencia/Comentarios de BP:

Esta técnica debería ayudar a minimizar la exposición de la información del cliente en la detección de bots al no recoger información detallada hasta que sea razonable creer que el cliente está infectado.

El análisis del tráfico de usuarios mediante un enfoque de red amplia puede incluir tanto la información externa como otros enfoques internos.

Este enfoque es útil para limitar la necesidad de herramientas más sofisticadas, como la inspección profunda de paquetes y las firmas. Una vez que se sospecha del tráfico de bots maliciosos (una red amplia), entonces se puede hacer un análisis más detallado del tráfico.

Puede encontrar más información en el Código de Conducta Anti-Bot de los Estados Unidos (ABC) para el servicio de Internet
Proveedores (ISP):
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf
Fase: Identificación (Control y visibilidad, operador de la red)
Orientación para la aplicación: Eficacia (H/M/L): M

Dificultad de aplicación: (H/M/L): H

Tenga en cuenta que las mejores prácticas de esta agrupación se dirigen principalmente a los ISP que prestan servicio a los consumidores finales en redes de banda ancha residenciales, pero también pueden ser aplicables a otros usuarios y redes.

Clasificación

Número de BP: Nuevo BP 18

Clasificar los ataques DoS/DDoS:

Los operadores de red, los proveedores de alojamiento y los objetivos de DDoS, cuando sea posible, deben tener procesos y/o capacidades para analizar y clasificar un ataque DoS/DDoS. La clasificación de los ataques puede ayudar a determinar las mejores mitigaciones para el ataque y ayudar a identificar las mejoras necesarias para proporcionar una protección futura.

Referencia/Comentarios de BP:

Ejemplo de clasificación:
¿Ataque volumétrico?
- Inundación directa de paquetes
- Reflexión/Amplificación

¿Ataque a la capa de aplicación?
¿Ataque de estado o de agotamiento de recursos?
¿Ataque de avión de control?
¿Ataque específico Ipv6?

¿Fecha?
Fase: Clasificación (tipo de ataque, operador de red, proveedor de alojamiento, objetivo), post mortem y recuperación (operador de red, proveedor de alojamiento, objetivo)
Orientación para la aplicación:Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

Rastreo

Número de BP: 9-8-0507:
Rastrear el ataque:
Los operadores de red deben disponer de procesos y/o capacidades para analizar y determinar el origen del tráfico malicioso y, a continuación, rastrear y eliminar los paquetes en la fuente o más cerca de ella. Las referencias proporcionan varias técnicas posibles. (El tráfico malicioso es aquel tráfico como los ataques de denegación de servicio distribuido (DDoS), los ataques smurf y fraggle, diseñados y transmitidos con el propósito de consumir recursos de una red de destino para bloquear el servicio o consumir recursos hasta el estado de desbordamiento que podría causar caídas del sistema).
Referencia/Comentarios de BP:
"Practical Network Support for IP Trace back" por Stefan Savage et.al., Dept. of Computer Science and Engineering, Univ of Washington, Tech Report UW-CSE-2000-02-01 con una versión publicada en los Proceedings of the 2000 ACM SIBCOMM pp256-306 Stockholm, Sweden, August 2000.
Fase: Rastreo (operadores de red)
Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): H

Reacción

Número de BP: 9-9-8065
Los operadores de red y los proveedores de alojamiento deben establecer un proceso para la entrega de información a los miembros de las fuerzas del orden e identificar un punto de contacto (POC) para las actividades de coordinación.
Referencia/Comentarios de BP:
Ninguna.
Fase: Reacción (operador de red, proveedores de alojamiento)
Orientación para la aplicación:Eficacia (H/M/L): L
Dificultad de aplicación: (H/M/L): L

Post mortem y recuperación

Número de BP: 9-9-8762
Recuperación de un ataque DoS:
Actualizado a:
Los operadores de red y los proveedores de alojamiento deberían, siempre que sea posible, cooperar con otros organizaciones durante y después de incidentes cibernéticos significativos para compartir información sobre los pasos
de caracterizar el ataque, sobre las técnicas para identificar, filtrar y aislar el origen puntos del ataque, y sobre las medidas adoptadas para desviar el tráfico legítimo y disuadir o defenderse de ataques DoS similares.
Referencia/Comentarios de BP:
IETF RFC2350, CMU/SEI-98-HB-001. Nota: Esta mejor práctica podría afectar al 9-1-1 operaciones.
Actualizado para añadir:
Esta buena práctica está orientada a la recuperación de la infraestructura del operador ante un ataque DoS. Fase: Reacción (operador de red, proveedores de alojamiento); Post Mortem (operador de red, proveedores de alojamiento)
Orientación para la aplicación: Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): M

Número de BP: 9-8-8515
Actualizado a:
Recuperación por uso indebido o consumo indebido de recursos del sistema:
Si se detecta un uso indebido o no autorizado de un sistema bajo su control (por ejemplo, la detección de la participación en un ataque DDoS), los operadores de red, los proveedores de alojamiento o los objetivos deben, cuando sea práctico, realizar un análisis forense del sistema, llevar a cabo un análisis post-mortem, aplicar controles para evitar futuros ataques y/o aplicar cuotas de recursos del sistema.
Referencia/Comentarios de BP:
IETF RFC2350, CMU/SEI-98-HB-001.
Fase: Post Mortem (operador de red, proveedor de alojamiento, objetivo)
Orientación para la aplicación: Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

Proveedores de alojamiento

Preparación

Número de BP: Nuevo BP10
Actualizar periódicamente la tecnología con las actualizaciones de seguridad o las nuevas versiones proporcionadas por
Proveedores:

Los proveedores de alojamiento deben tomar medidas razonables para proporcionar software y plug-ins actualizados a sus clientes (en los casos en que los proveedores de alojamiento ofrezcan software). El software proporcionado a los clientes debe ser apoyado activamente por el proveedor para las correcciones de seguridad. Deben proporcionarse herramientas, procesos o instrucciones de parcheo a los clientes para ayudarles a mantener su software actualizado con parches de seguridad. Siempre que sea posible, seleccione software que proporcione actualizaciones de seguridad automáticas y proporcione a los clientes instrucciones sobre cómo activar las actualizaciones.

Referencia/Comentarios de BP:

TBD
Fase: Preparación (Proteger, Proveedor de Alojamiento)

Orientación para la aplicación: Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-8-8753 (repetido desde la sección de operadores de red)
Actualizado a:
Gestión de la vulnerabilidad:

Los operadores de redes, los proveedores de alojamiento y los vendedores de hardware y software deben asegurarse de que pueden gestionar las vulnerabilidades de seguridad de los productos que gestionan o mantienen para los clientes. Esta gestión puede ser pasiva, como el simple mantenimiento de una lista de clientes a los que han distribuido el producto, o activa, como el escaneo de vulnerabilidades y la presentación de informes. Además, los productos, servicios, hardware y software deben ser probados para detectar vulnerabilidades antes de su despliegue significativo.

Referencia/Comentarios de BP:

Instituto Sans, "Gestión de la vulnerabilidad: Herramientas, retos y mejores prácticas". 2003. Pg.
12 - 13.
Preparación (Proteger) BP
Fase: Preparación (proteger, operador de red, proveedores de alojamiento)
Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-8-8753A - Nuevo BP (Anteriormente BP 9-8-8563) (Repetido de la Sección de Operadores de Red)
Actualizado a:
Gestión de la vulnerabilidad - Notificación:

Cuando se descubra una vulnerabilidad o un exploit DoS o DDoS, los operadores de red, los proveedores de alojamiento y los vendedores de hardware/software deben notificar el problema a los propietarios/operadores de los sistemas afectados para garantizar que el software, las configuraciones o los equipos se actualicen para

remediar la vulnerabilidad. Si no es posible remediarla a corto plazo, los propietarios/operadores deben considerar la posibilidad de mitigar el sistema o la red para minimizar la probabilidad de explotación del ataque DDoS.

Referencia/Comentarios de BP:

Instituto Sans, "Gestión de la vulnerabilidad: Herramientas, retos y mejores prácticas". 2003. Pg.
12 - 13.

Preparación (Proteger) BP

Fase: Preparación (proteger, operador de red, proveedores de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): H

Dificultad de aplicación: (H/M/L): H

Número de BP: 9-8-8917 (repetido desde la sección de operadores de red)

Notificación a los usuarios finales:

Los operadores de red y los proveedores de alojamiento deberían desarrollar y mantener métodos de notificación críticos para comunicar a sus clientes que su ordenador, servidores y/o red han sido probablemente infectados con malware. Esto debería incluir una gama de opciones para adaptarse a un grupo diverso de clientes y tecnologías de red. Una vez que el Operador de Red ha detectado un probable problema de seguridad del usuario final, deben tomarse medidas para informar al usuario de Internet de que puede tener un problema de seguridad. Un Operador de Red o Proveedor de Alojamiento debe decidir el método o métodos más apropiados para proporcionar la notificación a sus clientes o usuarios de Internet, y debe utilizar métodos adicionales si el método elegido no es efectivo. La gama de opciones de notificación puede variar en función de la gravedad y/o criticidad del problema.

Los ejemplos de los diferentes métodos de notificación pueden incluir, pero no se limitan a: correo electrónico, llamada telefónica, correo postal, mensajería instantánea (IM), servicio de mensajería corta (SMS), y la notificación del navegador web.

Referencia/Comentarios de BP:

Una decisión del Operador de Red y del Proveedor de Alojamiento sobre el método más apropiado o
métodos de notificación a uno o varios de sus clientes o usuarios de Internet
depende de una serie de factores, desde las capacidades técnicas del operador de la red, a los atributos técnicos de la red del Operador de Red, consideraciones de coste, los recursos disponibles del servidor, los recursos disponibles de la organización, el número de hosts infectados detectados en un momento dado, y la gravedad de las posibles amenazas, entre muchos otros factores. El uso de múltiples métodos de notificación simultánea es razonable para un operador de red, pero puede ser difícil para un falso proveedor de antivirus. Tenga en cuenta que el uso de las Notificaciones ciegas, es decir, las Notificaciones sin seguimiento, han resultado ser menos eficaz que los métodos que verifican o requieren la acción del usuario. La práctica recomendada 9-8-8921 establece información sobre cómo hacer frente a la infección de malware.

Fase: Preparación (comunicación, operador de red, proveedor de alojamiento)

Orientación para la aplicación: Eficacia (H/M/L): L

Dificultad de aplicación: (H/M/L): M

Tenga en cuenta que las mejores prácticas de esta agrupación se dirigen principalmente a los ISP que prestan servicios a los consumidores finales en redes de banda ancha residenciales, pero también pueden ser aplicables a otros usuarios y redes.

Número de BP: 9-8-8901

Actualizado a:

Apoyo de los proveedores de alojamiento a los recursos educativos para la higiene informática / informática segura:

Los Proveedores de Alojamiento deben proporcionar, poner a disposición, identificar o apoyar los recursos tutoriales, educativos y de autoayuda de terceros para sus clientes con el fin de educarlos sobre la importancia de la informática segura y ayudarlos a practicarla. Los clientes de los Proveedores de Alojamiento deben saber cómo proteger los dispositivos y las redes de los usuarios finales del acceso no autorizado a través de varios métodos, incluyendo, pero no limitado a:

1) Utiliza un software de seguridad legítimo que te proteja de los virus y spywares;
2) Asegúrese de que cualquier descarga o compra de software sea de una fuente legítima;
3) Utilice cortafuegos;
4) Mantener actualizados los parches de seguridad del sistema operativo, las bases de datos, las aplicaciones y los complementos de las aplicaciones;
5) Educar a los clientes sobre la importancia de la gestión de la vulnerabilidad y el escaneo.
6) Elimine y deje de utilizar el software que no se mantiene con parches de seguridad;
7) Analice regularmente los servidores en busca de software malicioso, programas espía y otros programas potencialmente no deseados;
8) Mantenga todas las aplicaciones, los complementos de las aplicaciones y el software del sistema operativo actualizados y utilice sus funciones de seguridad;
9) Utilizar contraseñas seguras y/o autenticación de 2 factores; y
10) No compartas nunca las contraseñas.
11) Proporcionar información de contacto para informar de los problemas.

Referencia/Comentarios de BP:

Puede encontrar más información en:

Alianza Nacional de Ciberseguridad - http://www.staysafeonline.org/ OnGuard Online - http://www.onguardonline.gov/default.aspx Departamento de Seguridad Nacional -

StopBadware - http://www.stopbadware.org/home/badware_prevent Seguridad de Comcast.net - http://security.comcast.net/ Seguridad de Verizon -

http://www.verizon.net/central/vzc.portal?_nfpb=X&_pageLabel=vzc_help_safety Sitio de Qwest Incredible Internet Security: http://www.incredibleinternet.com/ Microsoft- http://www.microsoft.com/security/pypc.aspx Fase: Preparación (educación, proveedores de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): L

Dificultad de aplicación: (H/M/L): L

Tenga en cuenta que las mejores prácticas de esta agrupación se dirigen principalmente a los ISP que prestan servicio a los consumidores finales en redes de banda ancha residenciales, pero también pueden ser aplicables a otros usuarios y redes.

Número de BP: 9-9-8068 (repetido desde la sección de operadores de red)

Los proveedores de servicios, los operadores de redes, los proveedores de alojamiento, la seguridad pública y los proveedores de equipos deben elaborar y poner en práctica un plan de comunicaciones como parte del plan más amplio de respuesta a incidentes, en el que se identifique a los actores clave y se incluya el mayor número posible de los siguientes elementos: nombres de contacto, números de teléfono de la empresa, números de teléfono del domicilio, números de buscapersonas, números de fax, números de teléfono móvil, direcciones del domicilio, direcciones de Internet, números de puente permanente, etc. Los planes de notificación deben elaborarse antes de que se produzca un suceso/incidente cuando sea necesario. El plan también debe incluir canales de comunicación alternativos (por ejemplo, buscapersonas alfa, Internet, teléfonos por satélite, VOIP, líneas privadas, teléfonos inteligentes) equilibrando el valor de cualquier método alternativo con los riesgos de seguridad y pérdida de información introducidos.

Referencia/Comentarios de BP:

Vía de comunicación de banda ancha alternativa para la coordinación y la gestión. Fase: Preparación (comunicación, operador de red, proveedor de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): H
Dificultad de aplicación: (H/M/L): L

Número de BP: 8-9-8074 (repetido desde la sección de operadores de red) Actualizado Ataque de denegación de servicio (DoS) - Objetivo: (Repetido de la sección de operadores de red)

Cuando sea posible, los operadores de redes, los proveedores de alojamiento, las redes de destino y los equipos de los proveedores de equipos deben ser capaces de sobrevivir a aumentos significativos tanto en el número de paquetes como en la utilización del ancho de banda. Siempre que sea posible, los proveedores de equipos y software deben desarrollar características efectivas de supervivencia al DoS/DDoS para sus líneas de productos. La infraestructura que soporta los servicios de misión crítica debe estar diseñada para aumentos significativos en el volumen de tráfico y debe incluir dispositivos de red capaces de filtrar y/o limitar la tasa de tráfico. Los ingenieros de red deben conocer las capacidades de los dispositivos y cómo emplearlas con el máximo efecto. Siempre que resulte práctico, los sistemas de misión crítica deben desplegarse en una configuración de clústeres que permita equilibrar la carga del exceso de tráfico y estar protegidos por un dispositivo de protección DoS/DDoS especialmente diseñado. Los operadores de infraestructuras críticas deben desplegar hardware y software de supervivencia al DoS siempre que sea posible.

Referencia/Comentarios de BP:

Nota: Esta Buena Práctica podría afectar a las operaciones del 9-1-1.
Por ejemplo, defensa contra ataques SYN Flood, CERT/CC ® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks - http://www.cert.org/advisories/CA-1996-21.html. Relacionado con NRIC BP 8753A.

Tenga en cuenta que, los operadores de red, los proveedores de alojamiento, los objetivos y los proveedores de equipos deben determinar qué servicios son de misión crítica en la aplicación de esta Buena Práctica.
Fase: Preparación (capacidad y recursos, operador de red, proveedor de alojamiento, objetivo)

Orientación para la aplicación:Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

Número de BP: Nuevo BP8 (repetido de la sección de operadores de red)
Despliegue de tecnologías anti-spoofing:

Los operadores de redes y los proveedores de alojamiento deberían, siempre que sea posible, desplegar tecnologías anti-spoofing para evitar que el tráfico falsificado se origine en sus redes.

Referencia/Comentarios de BP:

Relacionado con BP 9-7-0408

Hay que tener en cuenta que el despliegue puede no ser factible en algunas redes multi-homed debido a la necesidad de enrutamiento asimétrico.

Fase: Preparación (proteger, operador de red, proveedores de alojamiento)

Orientación para la aplicación:
Eficacia (H/M/L):H
Dificultad de aplicación: (H/M/L):
Redes domésticas individuales: L
Redes multihomes: H

Número de BP: Nuevo BP1
Protección de la red basada en aplicaciones:

Los proveedores de alojamiento y las fuentes de ataque deberían considerar la posibilidad de utilizar sistemas de detección de intrusiones basados en aplicaciones de red y/o en el host, cortafuegos u otros dispositivos de seguridad, configurados para denegar el tráfico por defecto, para protegerse contra el tráfico de red entrante o saliente malicioso o no autorizado en sus centros de alojamiento o en los servidores.

Referencia/Comentarios de BP:

Guía GB973 - 4 /DSD 2011 #8 (Modificado)
Guía GB973 - 5 /DSD 2011 #9 (Modificado)

Por ejemplo: Utilizar la función de control de frontera, por ejemplo, controladores de frontera de sesión o dispositivos similares, para evitar la negación / degradación de la comunicación VOIP mediante el bloqueo de las tormentas de registro de las granjas de servidores (puntos finales no autorizados) y el bloqueo de los intentos de fuzzing del protocolo.

Tenga en cuenta que es importante asegurarse de que la protección de la aplicación desplegada no es en sí misma vulnerable a un ataque DoS/DDoS. Si su diseño o configuración lo hace vulnerable al ataque, el dispositivo puede hacer que la aplicación sea más susceptible a un ataque DDoS. Fase: Preparación (prevención, proveedor de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): M

Identificación

Número de BP: Nuevo BP11
Supervisión del entorno de alojamiento en busca de tráfico malicioso o DDoS:

Los proveedores de alojamiento, siempre que sea posible, deben supervisar sus entornos para detectar tráfico de red malicioso o DDoS para identificar las fuentes y los métodos de los ataques.

Dificultad de aplicación: (H/M/L): M

Número de BP: 9-8-8916 (repetido desde la sección de operadores de red)

Actualizado a:

La detección de bots y la correspondiente notificación deben ser oportunas:

Los operadores de red y los proveedores de alojamiento deben asegurarse de que la detección de bots y la correspondiente notificación a los clientes de alojamiento se realicen a tiempo, ya que estos problemas de seguridad son sensibles al tiempo. Si se requiere un análisis complejo y se necesitan múltiples confirmaciones para confirmar que un bot está realmente presente, entonces es posible que el malware pueda causar algún daño, ya sea en el host infectado o en el sistema objetivo remoto (más allá del daño de la infección inicial) antes de que pueda ser detenido. Así pues, un operador de red o un proveedor de alojamiento debe equilibrar el deseo de confirmar definitivamente una infección de malware, lo que puede llevar un largo período de tiempo, con la capacidad de predecir la fuerte probabilidad de una infección de malware en un período de tiempo muy corto. Este desafío "definitivo-vs. probable" es difícil y, en caso de duda, los operadores de redes y los proveedores de alojamiento deberían pecar de precavidos y comunicar una probable infección de malware, al tiempo que toman medidas razonables para evitar las notificaciones de falsos positivos.

Referencia/Comentarios de BP:

La implementación de la notificación por parte del operador de red necesita equilibrar la certeza de una infección detectada con la incertidumbre de una detección transitoria de tráfico malicioso para minimizar la posibilidad de notificaciones falsas-positivas que podrían convertirse en una molestia para los clientes y llegar a ser inmanejables por el operador de red.

Puede encontrar más información en el Código de Conducta Anti-Bot de los Estados Unidos (ABC) para el servicio de Internet
Proveedores (ISP):
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

Fase: Identificación (supervisión y visibilidad, operador de red, proveedor de alojamiento)
Orientación para la aplicación: Eficacia (H/M/L): L (sólo notificación)

Dificultad de aplicación: (H/M/L): M

Tenga en cuenta que las mejores prácticas de esta agrupación se dirigen principalmente a los ISP que prestan servicio a los consumidores finales en redes de banda ancha residenciales, pero también pueden ser aplicables a otros usuarios y redes.

Número de BP: Nuevo BP6 (repetido de la sección de operadores de red)

Utilice el análisis de datos de Netflow para analizar los ataques DDoS:

Cuando sea posible, los operadores de red y los proveedores de alojamiento deberían permitir, recopilar y analizar los datos de Netflow para ayudar a la identificación y clasificación de los ataques DDoS. Los datos deben estar disponibles después del ataque para permitir un análisis posterior. Los datos de Netflow deben conservarse de acuerdo con la política de conservación de datos del operador de red.

Referencia/Comentarios de BP:

Los datos de Netflow pueden ser útiles para identificar ataques de spoofing.
Fase: Identificación (supervisión y visibilidad, operador de red, proveedores de alojamiento)

Orientación para la aplicación: Eficacia (H/M/L): H

Dificultad de aplicación: (H/M/L): M

Clasificación

Número de BP: Nuevo BP18 (repetido de la sección de operadores de red)
Clasificar los ataques DoS/DDoS:

Los operadores de red, los proveedores de alojamiento y los objetivos de DDoS, cuando sea posible, deben tener procesos y/o capacidades para analizar y clasificar un ataque DoS/DDoS. La clasificación de los ataques puede ayudar a determinar las mejores mitigaciones para el ataque y ayudar a identificar las mejoras necesarias para proporcionar una protección futura.

Referencia/Comentarios de BP:

Ejemplo de clasificación:
¿Ataque volumétrico?
Inundación directa de paquetes
Reflexión/Amplificación
¿Ataque a la capa de aplicación?
¿Ataque de estado o de agotamiento de recursos?
¿Ataque de avión de control?
¿Ataque específico Ipv6?
¿Fecha?

Fase: Clasificación (tipo de ataque, operador de red, proveedor de alojamiento, objetivo), post mortem y recuperación (operador de red, proveedor de alojamiento, objetivo)

Orientación para la aplicación:Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

Rastreo

Reacción

Número de BP: Nuevo BP12
Notificar a los clientes de hosting sobre el tráfico malicioso o DDoS

Los proveedores de alojamiento, siempre que sea posible, deben notificar a los clientes afectados si se detecta tráfico de red malicioso o DDoS procedente de sus servidores y, si procede, ayudar a los clientes a remediarlo.

Referencia/Comentarios de BP:

TBD

Fase: Reacción (Proveedor de alojamiento)

Orientación para la aplicación: Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-9-8065 (repetido desde la sección de operadores de red)

Los operadores de red y los proveedores de alojamiento deben establecer un proceso para la entrega de información a los miembros de las fuerzas del orden e identificar un punto de contacto (POC) para las actividades de coordinación.

Referencia/Comentarios de BP:
Ninguna.
Fase: Reacción (operador de red, proveedores de alojamiento)
Orientación para la aplicación: Eficacia (H/M/L): L
Dificultad de aplicación: (H/M/L): L

Post mortem y recuperación

Número de BP: 9-9-8762 (repetido desde la sección de operadores de red)
Recuperación de un ataque DoS:
Actualizado a:
Los operadores de red y los proveedores de alojamiento deberían, siempre que sea posible, cooperar con otros
organizaciones durante y después de incidentes cibernéticos significativos para compartir información sobre los pasos
de caracterizar el ataque, sobre las técnicas para identificar, filtrar y aislar el origen
puntos del ataque, y sobre las medidas adoptadas para desviar el tráfico legítimo y disuadir o
defenderse de ataques DoS similares.
Referencia/Comentarios de BP:
IETF RFC2350, CMU/SEI-98-HB-001. Nota: Esta mejor práctica podría afectar al 9-1-1 operaciones.
Actualizado para añadir:
Esta buena práctica está orientada a la recuperación de la infraestructura del operador ante un ataque DoS. Fase: Reacción (operador de red, proveedores de alojamiento); Post Mortem (operador de red, proveedores de alojamiento)
Orientación para la aplicación: Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): M

Número de BP: 9-8-8515 (repetido desde la sección de operadores de red)
Actualizado a:
Recuperación por uso indebido o consumo indebido de recursos del sistema:
Si se detecta un uso indebido o no autorizado de un sistema bajo su control (por ejemplo, la detección de la participación en un ataque DDoS), los operadores de red, los proveedores de alojamiento o los objetivos deben, cuando sea práctico, realizar un análisis forense del sistema, llevar a cabo un análisis post-mortem, aplicar controles para evitar futuros ataques y/o aplicar cuotas de recursos del sistema.
Referencia/Comentarios de BP:
IETF RFC2350, CMU/SEI-98-HB-001.

Objetivos

Preparación

Número de BP: 8-9-8074 (repetido desde la sección de operadores de red) Actualizado

Ataque de denegación de servicio (DoS) - Objetivo:

Siempre que sea posible, los operadores de red, los proveedores de alojamiento y las redes de destino, así como los equipos de los proveedores de equipos, deberían ser capaces de sobrevivir a aumentos significativos tanto en el número de paquetes como en la utilización del ancho de banda. Siempre que sea posible, los proveedores de equipos y software deben desarrollar características efectivas de supervivencia al DoS/DDoS para sus líneas de productos. La infraestructura que soporta los servicios de misión crítica debe estar diseñada para aumentos significativos en el volumen de tráfico y debe incluir dispositivos de red capaces de filtrar y/o limitar la tasa de tráfico. Los ingenieros de red deben conocer las capacidades de los dispositivos y cómo emplearlas con el máximo efecto. Siempre que resulte práctico, los sistemas de misión crítica deben desplegarse en una configuración de clústeres que permita el equilibrio de carga del exceso de tráfico y estar protegidos por un dispositivo de protección DoS/DDoS especialmente diseñado. Los operadores de infraestructuras críticas deben desplegar hardware y software de supervivencia al DoS siempre que sea posible.

Referencia/Comentarios de BP:

Nota: Esta Buena Práctica podría afectar a las operaciones del 9-1-1.

Por ejemplo, defensa contra ataques SYN Flood, CERT/CC ® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks - http://www.cert.org/advisories/CA-1996-21.html. Relacionado con NRIC BP 8753A.

Tenga en cuenta que, los operadores de red, los proveedores de alojamiento, los objetivos y los proveedores de equipos deben determinar qué servicios son de misión crítica en la aplicación de esta Buena Práctica.

Fase: Preparación (capacidad y recursos, operador de red, proveedor de alojamiento, objetivo)

Orientación para la aplicación:Eficacia (H/M/L): M

Dificultad de aplicación: (H/M/L): H

Número de BP: Nuevo BP7

Los servicios web deben limitar las cargas útiles que puedan provocar una congestión del ancho de banda de salida de los servidores web:

Los proveedores de aplicaciones web deben limitar los objetos grandes, como las descargas de documentos de gran tamaño, para evitar que las solicitudes repetidas consuman un ancho de banda de salida significativo del servidor (es decir, el ancho de banda del sitio del servidor al sitio del cliente), lo que puede causar una condición de DoS para los usuarios legítimos. Además, considere limitar el número de peticiones http get/post permitidas por dirección IP en un rango de tiempo específico.

Referencia/Comentarios de BP:

TBD

Fase: Preparación (minimizar la superficie de ataque, el objetivo)

Orientación para la aplicación: Eficacia (H/M/L): M

Dificultad de aplicación: (H/M/L): H

Número de BP: Nuevo BP13

Vigilancia del objetivo para el tráfico malicioso o DDoS:

Los objetivos deben supervisar los registros de seguridad y del servidor para determinar si se ha producido un tráfico anómalo o eventos de seguridad. Esto es útil para determinar si el Objetivo está siendo atacado o se ha producido un ataque recientemente; también puede indicar un precursor de un ataque.

Referencia/Comentarios de BP:

Hay que tener en cuenta que los objetivos de los ataques pueden ser tanto los usuarios finales como los operadores de red y los proveedores de alojamiento.

Fase: Preparación (seguimiento y visibilidad, objetivo)

Orientación para la aplicación:Eficacia (H/M/L): H

Dificultad de aplicación: (H/M/L): M

Número BP: Nuevo BP15

Utilizar las redes de entrega de contenidos para proporcionar solidez a las aplicaciones:

Los objetivos de los ataques deben utilizar redes de entrega de contenidos (CDN) para proporcionar solidez y minimizar la susceptibilidad a los ataques DoS/DDoS. Las CDNs pueden utilizarse para distribuir la capacidad de las aplicaciones a través de la red, haciéndola más robusta contra los ataques DoS/DDoS.

Referencia/Comentarios de BP:

TBD

Fase: Preparación (despliegue de herramientas de mitigación, objetivo)

Orientación para la aplicación: Eficacia (H/M/L): H

Dificultad de aplicación: (H/M/L): L

Número de BP: Nuevo BP17

Implantar la depuración de datos de destino in situ:

Los objetivos DDoS pueden emplear, cuando sea factible, centros de depuración de datos de tráfico para filtrar el tráfico de ataque DDoS. Esto puede lograrse "desviando" el tráfico DDoS sospechoso de ataque a un centro de depuración in situ donde se pueda filtrar el tráfico de ataque y "desviando" el tráfico legítimo de vuelta al objetivo.

Referencia/Comentarios de BP:

Es importante dimensionar la capacidad de la red in situ y de los centros de depuración para acomodar el tráfico de los ataques, con el fin de minimizar los posibles daños colaterales causados por las grandes oleadas de tráfico.

Fase: Preparación (despliegue de herramientas de mitigación, filtrado de alojamiento)

Orientación para la aplicación:Eficacia (H/M/L): H

Dificultad de aplicación: (H/M/L): H

Identificación

Clasificación

Número de BP: Nuevo BP18 (repetido de la sección de operadores de red)
Clasificar los ataques DoS/DDoS:

Los operadores de red, los proveedores de alojamiento y los objetivos de DDoS, cuando sea posible, deben tener procesos y/o capacidades para analizar y clasificar un ataque DoS/DDoS. La clasificación de los ataques puede ayudar a determinar las mejores mitigaciones para el ataque y ayudar a identificar las mejoras necesarias para proporcionar una protección futura.

Referencia/Comentarios de BP:

Ejemplo de clasificación:
¿Ataque volumétrico?
Inundación directa de paquetes
Reflexión/Amplificación
¿Ataque a la capa de aplicación?
¿Ataque de estado o de agotamiento de recursos?
¿Ataque de avión de control?
¿Ataque específico Ipv6?
¿Fecha?

Fase: Clasificación (tipo de ataque, operador de red, proveedor de alojamiento, objetivo), post mortem y recuperación (operador de red, proveedor de alojamiento, objetivo)

Orientación para la aplicación: Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

Rastreo

Reacción

Post mortem y recuperación

Número de BP: 9-8-8561
Recuperación de un ataque de denegación de servicio - Objetivo:

Si un elemento de la red, un sistema o un servidor bajo el control del Objetivo experimentó un DoS o Ataque DDoS, el Objetivo debe considerar:

1) Añadir más capacidad local (ancho de banda o servidores) al servicio atacado;
2) Desplegar dispositivos de mitigación específicos para DoS/DDoS basados en la premisa y/o utilizar capacidades anti-DoS en el hardware local;
3) Adquirir protecciones DDoS basadas en la red para su operador de red, proveedor de alojamiento, o un proveedor de mitigación DDoS de terceros;
4) Para los sistemas apropiados, como los sitios web, preparar un plan para minimizar los servicios prestados por el sitio en caso de que se produzca un futuro ataque que disminuya los efectos del mismo sin dejar de prestar servicios esenciales o importantes a sus clientes;
5) Coordinar con los proveedores de software y hardware para orientar la configuración óptima de los dispositivos;
6) Diseñar su sistema para capturar el tráfico de ataque, las direcciones IP atacantes y las marcas de tiempo correspondientes;
7) Compartir la captura de código hostil/de ataque, tácticas, técnicas, fuentes de ataque y procedimientos a las organizaciones que puedan experimentar tipos

de ataques similares y a las organizaciones de coordinación central como US-CERT y NCS/NCC para su revisión, análisis y distribución a un público más amplio; y

8) Trabaje con el operador de la red, el proveedor de alojamiento, el ISAC o el CERT para identificar los ordenadores atacantes y limpiar las máquinas en el extremo distante para minimizar el posibilidad de futuros ataques.

Referencia/Comentarios de BP:

Fase: Post Mortem (Objetivo)
Orientación para la aplicación: Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H

Número de BP: 9-8-8515 (repetido desde la sección de operadores de red)

Actualizado a:

Recuperación por uso indebido o consumo indebido de recursos del sistema:

Si se detecta un uso indebido o no autorizado de un sistema bajo su control (por ejemplo, la detección de la participación en un ataque DDoS), los operadores de red, los proveedores de alojamiento o los objetivos deben, cuando sea práctico, realizar un análisis forense del sistema, llevar a cabo un análisis post-mortem, aplicar controles para evitar futuros ataques y/o aplicar cuotas de recursos del sistema.

Referencia/Comentarios de BP:

IETF RFC2350, CMU/SEI-98-HB-001.
Fase: Post Mortem (operador de red, proveedor de alojamiento, objetivo)
Orientación para la aplicación: Eficacia (H/M/L): M
Dificultad de aplicación: (H/M/L): H