Estrategias de protección contra ataques de la negación de servicio distribuida (DDoS)

Contenido

Introducción

Este White Paper contiene la información para ayudarle a entender cómo se orquestran los ataques distribuidos de la negación de servicio (DDoS), reconoce los programas usados para facilitar los ataques DDoS, aplica las medidas para prevenir los ataques, información forense del frunce si usted sospecha un ataque, y aprende más sobre la Seguridad del host.

Información sobre los fundamentos de los ataques DDoS

Refiera a este ejemplo:

Detrás de un Cliente hay una persona que organiza un ataque. Un Manipulador es un host comprometido en el que se ejecuta un programa especial. Cada programa piloto es capaz de controlar los agentes múltiples. **Un agente** es un host comprometido que funciona con un programa especial. Cada agente es responsable de generar una secuencia de los paquetes que se dirija hacia la víctima prevista.

Los atacantes se han sabido para utilizar estos cuatro programas para poner en marcha los ataques DDoS:

1. Trinoo
2. TFN
3. TFN2K
4. Stacheldraht

Para facilitar el DDoS, los atacantes necesitan tener de varios cientos a varios miles de hosts comprometidos. Los host son generalmente Linux y ordenadores del SOL; pero, las herramientas se pueden virar hacia el lado de babor a otras Plataformas también. El proceso mediante el que se compromete a un host y se instala la herramienta está automatizado. El proceso se puede dividir en estos pasos, en los cuales los atacantes:

1. Inicie una fase de escaneo en la que un gran número de hosts (alrededor de 100 000 o más)

sean sondeados para detectar alguna vulnerabilidad conocida.
2. Comprometa los hosts vulnerables para ganar acceso.
3. Instale la herramienta en cada host.
4. Utilice los host comprometidos para una exploración y compromisos más futuros.

Porque se utiliza un proceso automatizado, los atacantes pueden comprometer y instalar la herramienta en un solo host adentro bajo cinco segundos. Es decir varios miles de host se pueden comprometer adentro bajo hora.

Características de los programas comunes utilizados para facilitar ataques

Éstos son los programas comunes que los hackers utilizan para facilitar los ataques distribuidos de la negación de servicio:

- TrinooLa comunicación entre los clientes, los programas pilotos y los agentes utiliza estos puertos:`1524 tcp`
  `27665 tcp`
  `27444 udp`
  `31335 udp`**Nota:** Los puertos listados anteriormente son los puertos predeterminados para esta herramienta. Use estos puertos como orientación y ejemplo solamente, debido a que los números del puerto pueden cambiarse fácilmente.
- TFNLa comunicación entre los clientes, los manipuladores y los agentes utilizan los paquetes ECO ICMP y RESPUESTA DE ECO.ICMP.
- StacheldrahtLa comunicación entre los clientes, los programas pilotos y los agentes utiliza estos puertos:`16660 tcp`
  `65000 tcp`
  `ICMP ECHO`
  `ICMP ECHO REPLY`**Nota:** Los puertos enumerados previamente son los puertos predeterminados para esta herramienta. Use estos puertos como orientación y ejemplo solamente, debido a que los números del puerto pueden cambiarse fácilmente.
- TFN2KLa comunicación entre los clientes, los programas pilotos y los agentes no utiliza ningún puerto específico, por ejemplo, puede ser suministrada el tiempo de ejecución o es elegida aleatoriamente por un programa, pero es una combinación de UDP, de ICMP y de paquetes TCP.Para una análisis detallado de los programas del DDoS, lea estos artículos.

Nota: Theaw conecta la punta a los sitios Web externos no mantenidos por Cisco Systems.

La herramienta "trinoo" de DoS Project para ataques de negación de servicio distribuidos

La herramienta Tribe Flood Network de ataque de negación de servicio distribuida

Herramienta de establecimiento de rechazo del servicio distribuido "stacheldraht

La información adicional con respecto las herramientas del DDoS y a sus variantes se puede encontrar en el índice del sitio web de la tormenta de paquetes de las herramientas de ataque distribuidas .

Prevención

Éstos son métodos sugeridos para prevenir las negaciones distribuidas de ataque de servicio.

1. Utilice el comando ip verify unicast reverse-path interface en la interfaz de entrada en el router en el extremo por aguas arriba de la conexión.Esta función examina cada paquete recibido como entrada en esa interfaz. Si la dirección IP de origen no tiene una ruta en las tablas CEF que señale de nuevo a la misma interfaz en la cual el paquete llegó, el router cae el paquete.El efecto del unicast RPF es que para los ataques smurf (y los otros ataques que dependen del spoofing de la dirección IP de origen) en el POP ISP (arriendo y terminal de marcado manual). Esto protege su red y sus clientes, así como al resto de Internet. Para usar RPF unidifusión, habilite "CEF switching" o "CEF distributed switching" en el router. No es necesario configurar la interfaz de entrada para la conmutación CEF. Mientras que CEF se esté ejecutando en el router, las interfaces individuales se pueden configurar con otros modos de conmutación. RPF es una función del lado de entrada que se habilita en una interfaz o subinterfaz y funciona en paquetes recibidos por el router.Es muy importante que el CEF sea girado en el router. El RPF no trabaja sin el CEF. El unicast RPF no se soporta en ninguna 11.2 o 11.3 imágenes. El unicast RPF se incluye en 12.0 en las Plataformas que soportan el CEF, que incluye el AS5800. Por lo tanto, la RFP de unidifusión puede ser configurada en las interfaces de acceso telefónico PSTN/ISDN en el AS5800.
2. Filtre todo el espacio de la dirección del RFC-1918 usando el Listas de control de acceso (ACL).Refiera a este ejemplo:`access-list 101 deny ip 10.0.0.0 0.255.255.255 any`
`access-list 101 deny ip 192.168.0.0 0.0.255.255 any`
`access-list 101 deny ip 172.16.0.0 0.15.255.255 any`
`access-list 101 permit ip any any`

`interface xy`
`ip access-group 101 in`Otra fuente de información sobre el espacio de la dirección especial del IPv4 del uso que puede ser filtrado es el borrador IETF (ahora expirado) “que documenta los bloqueos de dirección especiales del IPv4 del uso que se han registrado con el IANA .”
3. Aplican el ingreso y el filtrado de salida (véase RFC-2267) usando los ACL.Refiera a este ejemplo: `{ ISP Core } -- ISP Edge Router -- Customer Edge Router -- { Customer network }`El router de borde de ISP debería aceptar sólo el tráfico con direcciones de origen que pertenezcan a la red del cliente. La red cliente sólo debe aceptar el tráfico con direcciones de origen que no sean las del bloque de red cliente. Esto es una muestra ACL para un router de borde ISP:`access-list 190 permit ip {customer network} {customer network mask} any`
`access-list 190 deny ip any any [log]`

`interface {ingress interface} {interface #}`
`ip access-group 190 in` Esto es una muestra ACL para a Router borde del cliente:`access-list 187 deny ip {customer network} {customer network mask} any`
`access-list 187 permit ip any any`

`access-list 188 permit ip {customer network} {customer network mask} any`
`access-list 188 deny ip any any`

`interface {egress interface} {interface #}`
`ip access-group 187 in`
`ip access-group 188 out` Si puede activar Cisco Express Fowarding (CEF), la extensión de las ACL puede reducirse substancialmente y, de esta forma, aumentar el desempeño ya que permite el envío por trayecto inverso de unidifusión. Para soportar el Unicast Reverse Path Forwarding, usted necesita solamente poder habilitar el CEF en el router en su conjunto; la interfaz en la cual se habilita la característica no necesita ser un Switched Interface CEF.
4. Utilice el CAR a los paquetes icmp del límite de velocidad.Refiera a este ejemplo:`interface xy`

```
 rate-limit output access-group 2020 3000000 512000 786000 conform-action transmit exceed-
action drop access-list 2020 permit icmp any any echo-reply
```

5. Configure la limitación de velocidad para los paquetes SYN.Refiera a este ejemplo:
```
access-list 152 permit tcp any host eq www
access-list 153 permit tcp any host eq www established

interface {int}
rate-limit output access-group 153 45000000 100000 100000
conform-action transmit exceed-action drop
 rate-limit output access-group 152 1000000 100000 100000
conform-action transmit exceed-action drop
```
En el ejemplo anterior, substituya:45000000 con el ancho de banda de link máximo1000000 con un valor de entre 50% y 30% de la tasa de inundaciones SYNvelocidades de ráfaga normal y máxima con valores precisosObserve que si usted fija la velocidad de ráfaga mayor el de 30%, muchos SYN legítimos pueden ser caídos. Para conseguir una idea de donde fijar la velocidad de ráfaga, utilizar el comando show interfaces rate-limit para visualizar las tarifas conformadas y excedidas para la interfaz. Su objetivo es limitar la velocidad de SYN lo menos posible como para que todo funcione nuevamente.**Advertencia:** Se recomienda que usted primera cantidad de la medida de paquetes SYN durante el estado normal (antes de que ocurren los ataques) y utiliza esos valores para limitar. Revise los números cuidadosamente antes de que usted despliegue esta medida.Si un Ataque SYN está dirigido contra un host determinado, considere instalar un paquete de filtración IP en ese host. Uno de esos paquetes es el filtro de IP. Refiera a los ejemplos del filtro IP para los detalles de instrumentación.

Capturando las pruebas y entrar en contacto el cumplimiento de la ley

Si es posible, obtenga una muestra del tráfico del ataque para el análisis posterior (conocido comúnmente como “captura de paquetes "). Utilice Solaris o una estación de trabajo Linux con bastante potencia de procesamiento de continuar con el flujo de paquetes. Para obtener a tal captura de paquetes, utilice el programa del tcpdump (disponible para los sistemas operativos de Windows, de Solaris y de Linux) o el programa del fisgón (disponible para el sistema operativo Solaris solamente). Éste es un ejemplo básico de cómo utilizar esos programas:

```
tcpdump -i interface -s 1500 -w capture file
  snoop -d interface -o capture file -s 1500
```

La talla del MTU en este ejemplo es 1500; cambie este parámetro si el MTU es mayor de 1500.

Si usted quiere implicar el cumplimiento de la ley y usted está dentro de los Estados Unidos, entre en contacto su oficina de campo local FBI. Más información está disponible en el sitio web del centro de la protección de la infraestructura nacional. Si usted está situado en Europa, ninguna punta del contacto existe. Entre en contacto a su autoridad competente local y pida la ayuda.

CISCO NO PUEDE ENTRAR EN CONTACTO A LAS AUTORIDADES COMPETENTES EN NOMBRE SU. Una vez que haya establecido los contactos iniciales, el equipo de PSIRT de Cisco puede trabajar con el cumplimiento de la ley.

Para material sobre la seguridad general del host, visite la página web CERT/CC.

Información Relacionada

- Caracterización y seguimiento de la inundación de paquetes usando routers de Cisco
- Detalles técnicos de la mitigación del gusano
- Mejora de seguridad de los routers de Cisco
- Respuesta ante problemas de seguridad de productos Cisco
- Seguridad @ Cisco
- Soporte Técnico y Documentación - Cisco Systems