Utilice NBAR y ACL para bloquear el gusano "Código rojo"

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Cómo bloquear el gusano de código rojo
Plataformas Soportadas
Detecte el intento de infección en los registros Web IIS
La marca de entrada “Código rojo” irrumpe utilizando la característica de marcación basada en la clase del IOS
Método A: Use un ACL
Método B: Utilice Policy-Based Routing (PBR)
Método C: Utilice la regulación de tráfico basada en la clase
Restricciones NBAR
Problemas conocidos
Información Relacionada

Introducción

Este documento proporciona un método para bloquear el gusano "Código rojo" en los puntos de ingreso a la red a través del Reconocimiento de aplicaciones basadas en red (NBAR) y Listas de control de acceso (ACL) dentro del software Cisco IOS® en los routers Cisco. Esta solución debería usarse junto con los parches recomendados para los servidores IIS de Microsoft.

Nota: Este método no funciona en los Cisco 1600 Series Routers.

Nota: Parte del tráfico P2P no se puede bloquear completamente debido a la naturaleza de su protocolo P2P. Estos protocolos P2P cambian dinámicamente sus firmas para evitar cualquier motor DPI que intente bloquear completamente su tráfico. Por lo tanto, se recomienda limitar el ancho de banda en lugar de bloquearlos completamente. Acelere el ancho de banda para este tráfico. Proporcione mucho menos ancho de banda; sin embargo, deje pasar la conexión.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Políticas de servicio de calidad de servicio (QoS) mediante los comandos de la interfaz de línea de comandos de QoS modular (CLI).
- NBAR
- Listas de control de acceso (ACL)
- Ruteo basado en políticas

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. La configuración en este documento se probó en el Cisco 3640 que ejecuta la versión 12.2(24a) del IOS de Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Cómo bloquear el gusano de código rojo

Lo primero que debe hacer para combatir "Código rojo" es aplicar el parche disponible de Microsoft (ver los enlaces en la sección Método A: Utilice una ACL a continuación). Esto protege los sistemas vulnerables y elimina el gusano de un sistema infectado. Sin embargo, la aplicación del parche a sus servidores sólo evita que el gusano infecte los servidores, no detiene las solicitudes GET HTTP de los servidores. Todavía existe la posibilidad de que el servidor sea bombardeado con una avalancha de intentos de infección.

La solución detallada en esta advertencia está diseñada para funcionar junto con el parche de Microsoft para bloquear las solicitudes GET HTTP "Código rojo" en un punto de ingreso a la red.

Esta solución intenta bloquear la infección, sin embargo no solucionará los problemas causados por la acumulación de un gran número de entradas de caché, adyacencias y entradas NAT/PAT, ya que la única manera de analizar el contenido de la solicitud GET HTTP es después del establecimiento de una conexión TCP. El siguiente procedimiento no ayudará a proteger contra un escaneo de la red. Sin embargo, protegerá un sitio de la infestación de una red externa o reducirá el número de intentos de infección que debe realizar una máquina. En combinación con el filtrado entrante, el filtrado saliente evita que los clientes infectados propaguen el gusano "Código rojo" a la Internet global.

Plataformas Soportadas

La solución descrita en este documento requiere la función de marcado basada en clase dentro del software Cisco IOS. Específicamente, la capacidad para coincidir en cualquier parte de una URL HTTP utiliza la característica de clasificación de subpuerto HTTP en NBAR. A continuación, se resumen las plataformas admitidas y los requisitos mínimos de software de Cisco IOS:

Platform	Mínimo de Cisco IOS Software
7200	12.1(5)T
7100	12.1(5)T
3745	12.2(8)T
3725	12.2(8)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

Nota: Debe activar Cisco Express Forwarding (CEF) para utilizar NBAR.

La marcación basada en clases y la NBAR distribuida (DNBAR) también están disponibles en las siguientes plataformas:

Platform	Mínimo de Cisco IOS Software
7500	12.1(6)E
FlexWAN	12.1(6)E

Detecte el intento de infección en los registros Web IIS

El intento de infección inicial envía una solicitud GET HTTP grande al servidor IIS de destino. A continuación se muestra la huella original de "Código rojo":

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

A continuación se muestra la huella "Código rojo" II:

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%
u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403 -
```

Observe que la solicitud GET siempre busca un archivo con una extensión .ida. Esta es una cadena común en todos los intentos de infección y, por lo tanto, se puede utilizar como criterio de coincidencia con el marcado basado en clase en IOS. El resto de la solicitud GET no será necesariamente coherente, ya que simplemente intenta crear un desbordamiento de búfer. Esto se puede ver comparando las dos entradas anteriores.

Ahora se informa que la diferencia entre estas dos firmas se debe a una nueva cepa del gusano "Código rojo", apodado CodeRed.v3 o CodeRed.C. La cepa "Código rojo" original contiene la cadena "NNNNNN" en la solicitud GET, mientras que la nueva cepa contiene "XXXXXXXX".

Consulte Symantec Advisory para obtener más detalles.

A las 6:24PM EDT, 6 de agosto de 2001, registramos una nueva huella. Hemos aprendido desde entonces que esta es la huella que deja el escáner de vulnerabilidad eEye .

```
2001-08-06 22:24:02 10.30.203.202 - 10.1.1.9 80 GET /x.ida AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1 -
```

La técnica para bloquear "Código rojo" proporcionada en esta advertencia también puede bloquear estos intentos de escaneo simplemente ajustando la definición de mapa de clase como se muestra en la siguiente sección.

La marca de entrada “Código rojo” irrumpe utilizando la característica de marcación basada en la clase del IOS

Para bloquear el gusano "Código rojo", utilice uno de los tres métodos descritos a continuación. Los tres métodos clasifican el tráfico malintencionado mediante la función Cisco IOS MQC. Este tráfico se descarta como se describe a continuación.

Método A: Use un ACL

Este método utiliza una ACL en la interfaz de salida para descartar los paquetes marcados con "Código rojo". Utilice el siguiente diagrama de red para ilustrar los pasos de este método:

Estos son los pasos para configurar este método:

1. Clasifique los piratas informáticos "Código rojo" entrantes con la función de marcación basada en clases del software Cisco IOS, como se muestra a continuación:
   ```
   Router(config)#class-map match-any http-hacks
   Router(config-cmap)#match protocol http url "*default.ida*"
   Router(config-cmap)#match protocol http url "*cmd.exe*"
   Router(config-cmap)#match protocol http url "*root.exe*"
   ```

   El mapa de clase anterior busca dentro de las URL HTTP y coincide con cualquiera de las cadenas especificadas. Observe que hemos incluido otros nombres de archivo además del default.ida de "Código rojo". Puede utilizar esta técnica para bloquear intentos de hackeo similares, como el virus Sadhead, que se explica en los siguientes documentos:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html
2. Cree una política y utilice el comando **set** para marcar los hacks "Código rojo" entrantes con un policy map. Este documento utiliza un valor DSCP de 1 (en decimal), ya que es poco probable que otro tráfico de red lleve este valor.Aquí se marcan los hacks "Código rojo"

entrantes con un mapa de políticas denominado "mark-inbound-http-hacks".

```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```

3. Aplique la política como política de entrada en la interfaz de entrada para marcar los paquetes "Código rojo" que llegan.

```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```

4. Configure una ACL que coincida con el valor DSCP de 1, según lo establecido por la política de servicio.

```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

Nota: Cisco IOS Software Releases 12.2(11) y 12.2(11)T introducen soporte para la palabra clave **log** en la ACL al definir en mapas de clase para su uso con NBAR (CSCdv48172). Si está utilizando una versión anterior, no utilice la palabra clave **log** en la ACL. Esto obliga a que todos los paquetes sean conmutados por proceso en lugar de conmutados por CEF, y NBAR no funcionará ya que requiere CEF.

5. Aplique la ACL saliente en la interfaz de salida que se conecta a los servidores Web de destino.

```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. Compruebe que la solución funciona como se espera. Ejecute el comando **show access-list** y asegúrese de que el valor "coincide" de la sentencia deny aumente.

```
Router#show access-list 105
Extended IP access list 105
 deny ip any any dscp 1 log (2406 matches)
 permit ip any any (731764 matches)
```

En el paso de configuración, también puede inhabilitar el envío de mensajes IP inalcanzables con el comando **no ip unreachable** interface-level para evitar que el router gaste recursos excesivos.Este método no se recomienda si puede rutear el tráfico DSCP=1 a Null 0, como se describe en la sección Método B.

Método B: Utilice Policy-Based Routing (PBR)

Este método utiliza el ruteo basado en políticas para bloquear los paquetes marcados con "Código rojo". No es necesario aplicar los comandos de este método si los métodos A o C ya están configurados.

Estos son los pasos para implementar este método:

1. Clasifique el tráfico y márquelo. Utilice los comandos **class-map** y **policy-map** que se

muestran en el método A.
2. Utilice el comando **service-policy** para aplicar la política como política de entrada en la interfaz de entrada para marcar los paquetes "Code Red" que llegan. Véase el método A.
3. Cree una ACL IP extendida que coincida con los paquetes marcados como "Código rojo".
```
Router(config)#access-list 106 permit ip any any dscp 1
```

4. Utilice el comando **route-map** para generar una política de ruteo.
```
Router(config)#route-map null_policy_route 10
Router(config-route-map)#match ip address 106
Router(config-route-map)#set interface Null0
```
5. Aplique el route-map a la interfaz de entrada.
```
Router(config)#interface serial 0/0
Router(config-if)#ip policy route-map null_policy_route
```

6. Verifique que su solución funcione según lo esperado con el comando **show access-list**. Si está utilizando ACL de salida y ha habilitado el registro de ACL, también puede utilizar los comandos **show log**, como se muestra a continuación:
```
Router#show access-list 106
Extended IP access list 106
 permit ip any any dscp 1 (1506 matches)

Router#show log
Aug 4 13:25:20: %SEC-6-IPACCESSLOGP:
 list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
Aug 4 13:26:32: %SEC-6-IPACCESSLOGP:
 list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
```
Podemos tomar la decisión de descartar en la interfaz de ingreso del router, en lugar de necesitar una ACL de salida en cada interfaz de salida. Una vez más, recomendamos inhabilitar el envío de mensajes IP inalcanzables con el comando **no ip unreachables**.

Método C: Utilice la regulación de tráfico basada en la clase

Este método es generalmente el más escalable ya que no depende de PBR ni de ACL de salida.

1. Clasifique el tráfico usando los comandos **class-map** mostrados en el método A.
2. Cree una política usando el comando **policy-map** y utilice el comando **police** para especificar una acción de descarte para este tráfico.
```
Router(config)#policy-map drop-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#police 1000000 31250 31250
 conform-action drop exceed-action drop violate-action drop
```

3. Utilice el comando **service-policy** para aplicar la política como política de entrada en la interfaz de entrada para descartar los paquetes "Code Red".
```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

4. Verifique que su solución funcione según lo esperado con el comando **show policy-map interface**. Asegúrese de ver los valores incrementados para la clase y los criterios de coincidencia individuales.
```
Router#show policy-map interface serial 0/0

Serial0/0
```

```
Service-policy input: drop-inbound-http-hacks

  Class-map: http-hacks (match-any)
    5 packets, 300 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: protocol http url "*default.ida*"
      5 packets, 300 bytes
      5 minute rate 0 bps
    Match: protocol http url "*cmd.exe*"
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: protocol http url "*root.exe*"
      0 packets, 0 bytes
      5 minute rate 0 bps
    police:
      1000000 bps, 31250 limit, 31250 extended limit
      conformed 5 packets, 300 bytes; action: drop
      exceeded 0 packets, 0 bytes; action: drop
      violated 0 packets, 0 bytes; action: drop
      conformed 0 bps, exceed 0 bps, violate 0 bps

  Class-map: class-default (match-any)
    5 packets, 300 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
```

Restricciones NBAR

Al utilizar NBAR con los métodos de este documento, tenga en cuenta que NBAR no admite las siguientes funciones:

- Más de 24 coincidencias simultáneas de URL, HOST o tipo MIME
- Coincidiendo más allá de los primeros 400 bytes en una URL
- Tráfico que no es de IP
- Modos de conmutación de multidifusión y otros modos de conmutación que no sean CEF
- Paquetes fragmentados
- Solicitudes HTTP persistentes canalizadas
- URL/HOST/MIME/ clasificación con HTTP seguro
- Flujos asimétricos con protocolos stateful
- Paquetes que se originan o se dirigen al router que ejecuta NBAR

No puede configurar NBAR en las siguientes interfaces lógicas:

- Fast EtherChannel
- Interfaces que utilizan tunelización o encripción
- VLAN
- Interfaces del marcador
- PPP de links múltiples

Nota: NBAR se puede configurar en las VLAN a partir de la versión 12.1(13)E del IOS de Cisco, pero sólo se admite en la trayectoria de conmutación del software.

Dado que NBAR no se puede utilizar para clasificar el tráfico de salida en un link WAN donde se utiliza tunelización o cifrado, aplíquelo en su lugar a otras interfaces del router, como la interfaz LAN, para realizar la clasificación de entrada antes de que el tráfico se conmute al link WAN para la salida.

Para obtener más información sobre NBAR, vea los enlaces de la información relacionada