Uso del reconocimiento de la aplicación basada en la red y ACL para bloqueo del gusano "Código rojo

Contenido

Introducción

Este documento proporciona un método para bloquear el gusano del “Código rojo” en los puntos de ingreso a la red con el Network-Based Application Recognition (NBAR) y el Listas de control de acceso (ACL) dentro del software de Cisco IOS® en los routeres Cisco. Esta solución debería usarse junto con los parches recomendados para los servidores IIS de Microsoft.

Nota: Este método no trabaja en los Cisco 1600 Series Router.

Nota: Un cierto tráfico P2P no puede ser totalmente bloqueado debido a la naturaleza de su protocolo P2P. Estos protocolos P2P cambian dinámicamente sus firmas para desviar cualquier motor DPI que intenta bloquear totalmente su tráfico. Por lo tanto, se recomienda para limitar el ancho de banda en vez totalmente de bloquearlos. Estrangule el ancho de banda para este tráfico. Dé mucho menos ancho de banda; sin embargo, deje la conexión ir a través.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Políticas de servicio del Calidad de Servicio (QoS) usando los comandos de la interfaz de línea del comando modular qos (CLI).
- NBAR
- 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 fue probada en el Cisco 3640 que funciona con la versión deL Cisco IOS 12.2(24a)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Cómo bloquear el gusano de código rojo

La primera cosa que usted debe hacer para combatir el “Código rojo” es aplica la corrección disponible desde Microsoft (véase los links en el método A de la sección: Utilice un ACL abajo). Esto protege los sistemas vulnerables y quita el gusano de un sistema infectado. Sin embargo, la aplicación de la corrección a sus servidores evita solamente que el gusano infecte los servidores, él no para las peticiones get HTTP de golpear los servidores. Todavía hay el potencial para que el servidor consiga bombardeado con una inundación de los intentos de infección.

La solución detallada en este advisory se diseña para trabajar conjuntamente con la parche de Microsoft para bloquear las peticiones get del “Código rojo” HTTP en un punto de ingreso a la red.

Esta solución intenta bloquear la infección, no obstante no curará los problemas causados por la acumulación de un gran número de entradas del caché, de adyacencias, y de entradas NAT/PAT, puesto que la única forma de analizar el contenido de la petición get HTTP está siguiendo el establecimiento de una conexión TCP. El siguiente procedimiento no ayudará a proteger contra una exploración de la red. Sin embargo, protegerá un sitio contra la infestación de una red externa o reducirá el número de intentos de infección que una máquina deba mantener. Conjuntamente con el filtrado de entrada, el filtrado de salida evita que los clientes infectados separen el gusano del “Código rojo” al Internet global.

Plataformas Soportadas

La solución descrita en este documento requiere la característica de marcación basada en la clase dentro del Cisco IOS Software. 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:

Plataforma	Software del Cisco IOS mínimo
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: Para utilizar NBAR debe activar Cisco Express Forwarding (CEF).

El Marcado basado en clases y el NBAR distribuido (DNBAR) están también disponibles en las Plataformas siguientes:

Plataforma	Software del Cisco IOS mínimo
7500	12.1(6)E
FlexWAN	12.1(6)E

Detecte el intento de infección en los registros Web IIS

La tentativa de la infección inicial envía una petición get grande HTTP al servidor IIS de la blanco. La huella original del “Código rojo” se muestra abajo:

```
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
```

La huella del “Código rojo” II se muestra abajo:

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%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 -
```

Note que la petición get está buscando siempre un archivo con una extensión .ida. Esto es una cadena común en todos los intentos de infección y se puede por lo tanto utilizar como los criterios de concordancia con el Marcado basado en clases en el IOS. El resto de la petición get no será necesariamente constante como apenas está intentando crear un desbordamiento de búfer. Esto puede ser vista comparando las dos entradas arriba.

Ahora está siendo señalado que la diferencia entre estas dos firmas es debido a una nueva cepa del gusano del “Código rojo”, del CodeRed.v3 doblado o del CodeRed.C. La tensión original del “Código rojo” contiene la cadena “NNNNNNNN” en la petición get, mientras que la nueva cepa contiene el “”. Refiera al Consejo sobre Symantec para más detalles.

En 6:24PM EDT, el 6 de agosto 2001, registramos una nueva huella. Hemos aprendido desde entonces que ésta es la huella que es dejada detrás por el escáner de vulnerabilidad de 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 el “Código rojo” proporcionó en este advisory puede también bloquear éstos las tentativas de la exploración simplemente apretando la definición del mapa de clase tal y como se muestra en de 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 del “Código rojo”, utilice uno de los tres métodos descritos más abajo. Los tres métodos clasifican el tráfico malévolo usando la característica del Cisco IOS MQC. Este tráfico entonces se cae como se describe a continuación.

Método A: Use un ACL

Este método utiliza un ACL en la interfaz de salida para caer los paquetes marcados del “Código rojo”. Utilicemos el siguiente diagram de red para ilustrar los pasos en este método:

Aquí están los pasos a configurar este método:

1. Clasifique los cortes entrantes del “Código rojo” con la característica de marcación basada en la clase en Cisco IOS Software, como se muestra abajo:`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*"`**
   La correspondencia antedicha de la clase mira dentro de HTTP URL y hace juego las cadenas especificadas unas de los. Note que hemos incluido otros nombres del archivo además del default.ida del “Código rojo”. Usted puede utilizar esta técnica para bloquear los intentos de irrupción similares, tales como el virus Sadmind, que se explica en los documentos siguientes:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html
2. Construya una directiva y utilice el **comando set** de marcar los cortes entrantes del “Código

rojo” con una correspondencia de políticas. Este documento utiliza un valor DSCP de 1 (en el decimal) puesto que es inverosímil que algún otro tráfico de la red está llevando este valor.Aquí marcamos los cortes entrantes del “Código rojo” con una correspondencia de políticas nombrada los “marca-entrante-HTTP-cortes”.`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 directiva como política de entrada en la interfaz de entrada para marcar los paquetes de llegada del “Código rojo”.`Router(config)#`**`interface serial 0/0`**
   `Router(config-if)#`**`service-policy input mark-inbound-http-hacks`**
4. Configure un ACL que haga juego en el valor DSCP de 1, como fija 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: Los Cisco IOS Software Releases 12.2(11) y 12.2(11)T introducen el soporte para la palabra clave del **registro** en el ACL en la definición en las correspondencias de la clase para el uso con NBAR (CSCdv48172). Si usted está utilizando una versión anterior, no utilice la palabra clave del **registro** en el ACL. El hacer fuerza tan todos los paquetes para ser process-switched en vez de CEF-Switched, y el NBAR no trabajará puesto que requiere el CEF.
5. Aplique el ACL de salida en la interfaz de salida que conecta con los servidores Web de Target text.`Router(config)#`**`interface ethernet 0/1`**
   `Router(config-if)#`**`ip access-group 105 out`**
6. Verifique que su solución trabaje como se esperaba. Ejecute el **comando show access-list** y asegúrese de que “hace juego” el valor para el enunciado de negación está incrementando.`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 para la configuración, usted puede también inhabilitar el envío de los mensajes del inalcanzable IP con el **comando no ip unreachable interface-level** de evitar hacer al router gastar a los recursos excesivos.Este método no se recomienda si usted puede directiva-ruta el tráfico DSCP=1 al null0, según lo descrito en la sección del método B.

Método B: Utilice Policy-Based Routing (PBR)

Este método utiliza el Policy-Based Routing a los paquetes marcados del “Código rojo” de bloque. Usted no necesita aplicar los comandos en este método si los métodos A o el C se configuran ya.

Aquí están los pasos a implementar este método:

1. Clasifique el tráfico y marqúelo. Utilice los **comandos class-map and policy-map** mostrados en el método A.
2. Utilice el **comando service-policy** de aplicar la directiva como política de entrada en la interfaz de entrada para marcar los paquetes de llegada del “Código rojo”. Vea el método A.

3. Cree un IP ampliado ACL que haga juego en los paquetes marcados del “Código rojo”.`Router(config)#`**`access-list 106 permit ip any any dscp 1`**
4. Utilice el **comando route-map** de construir un 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 sus trabajos de la solución como se esperaba con el **comando show access-list**. Si usted está utilizando los ACL de salidas y ha habilitado el registro de ACL, usted también puede utilizar los **comandos show log**, como se muestra abajo:`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 descarte en la interfaz de ingreso del router, bastante que necesitando un ACL de salida en cada interfaz de egreso. Una vez más recomendamos el inhabilitar de los mensajes de envío del inalcanzable IP con el comando no ip unreachables.

C del método: Utilice la regulación de tráfico basada en la clase

Este método es generalmente el más scalable pues no depende del PBR o de los ACL de salidas.

1. Clasifique el tráfico usando los **comandos class-map** mostrados en el método A.
2. Construya una directiva usando el **comando policy-map** y utilice el **comando police** de 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** de aplicar la directiva como política de entrada en la interfaz de entrada para caer los paquetes del “Código rojo”.`Router(config)#`**`interface serial 0/0`**
   `Router(config-if)#`**`service-policy input drop-inbound-http-hacks`**
4. Verifique que su solución trabaje como se esperaba con el **comando show policy-map interface**. Asegúrese de que usted vea incrementar los valores para la clase y los criterios de concordancia 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 usar el NBAR con los métodos en este documento, observe que las características siguientes no son soportadas por el NBAR:

- Más de 24 coincidencias simultáneas URL, de los host o del tipo MIME
- El corresponder con más allá de los primeros 400 bytes en un URL
- Tráfico no IP
- Multicast y otros modos de la transferencia NON-CEF
- Paquetes fragmentados
- Pedidos de HTTP persistentes canalizados
- Clasificación URL/HOST/MIME/con el HTTP seguro
- Flujos asimétricos con los protocolos con estado
- Paquetes que originan de o destinado al router que ejecuta el NBAR

Usted no puede configurar el NBAR en las interfaces lógicas siguientes:

- Fast EtherChannel
- Interfaces que utilizan el Tunelización o el cifrado
- VLAN
- Interfaces del dialer
- PPP de links múltiples

Nota: El NBAR es configurable en los VLA N a partir del Cisco IOS Release 12.1(13)E, pero soportado en el trayecto de Switching del software solamente.

Puesto que el NBAR no se puede utilizar para clasificar el tráfico de la salida en un link PÁLIDO donde se utiliza el hacer un túnel o el cifrado, apliqúelo en lugar de otro a otras interfaces en el router, tal como la interfaz LAN, para realizar la clasificación de entrada antes de que el tráfico se conmute al link PÁLIDO para la salida.

Para más información acerca de NBAR, vea los links en la información relacionada