Cómo proteger su red del virus Nimda

Contenido

Introducción

Este documento describe las maneras de minimizar el impacto del gusano NIMDA en su red. Este documento dirige dos temas:

- ¿Se infecta la red, qué puede ser hecha? ¿Cómo puede usted minimizar el daño y el polvillo radiactivo?
- La red todavía no se infecta, ni se infecta solamente parcialmente. ¿Qué se puede hacer para minimizar la extensión de este gusano?

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes usados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

Para más información sobre los convenios del documento, refiera a los convenios de los consejos

técnicos de Cisco.

Antecedentes

Para la información previa en el gusano NIMDA, refiera a estos links:

- http://www.cert.org/body/advisories/CA200126_FA200126.html
- http://vil.nai.com/vil/content/v_99209.htm
- http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

Plataformas admitidas

La solución del Network-Based Application Recognition (NBAR) descrita en este documento requiere la característica del Marcado basado en clases dentro del software de 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:

Plataforma	Versión mínima del Software del IOS de Cisco
7200	12.1(5)T
7100	12.1(5)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(5)T

Note: Usted necesita permitir al Cisco Express Forwarding (CEF) para utilizar el Network-Based Application Recognition (NBAR).

NBAR también se utiliza en algunas plataformas del software del Cisco IOS que comienzan con la versión 12.1E. Vea los “protocolos admitidos” en la documentación del reconocimiento de la aplicación basada en la red.

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

Plataforma	Versión mínima del Software del IOS de Cisco
7500	12.1(6)E
FlexWAN	12.1(6)E

Si usted está desplegando NBAR, sea consciente del ID de bug CSCdv06207 (clientes registrados de Cisco solamente). La solución alternativa descrita en CSCdv06207 puede ser necesaria si usted encuentra este defecto.

La solución de la lista de control de acceso (ACL) se utiliza en todas las versiones actuales del

software del Cisco IOS.

Para las soluciones donde usted necesita utilizar el comando line interface(cli) de la calidad de servicio modular (QoS) (por ejemplo para el tráfico tarifa-limitador ARP o ejecutar la tarifa que limita con el policer en vez del COCHE), usted necesita la interfaz de línea de comando de calidad de servicio modular que está disponible en los Cisco IOS Software Release 12.0XE, 12.1E, 12.1T, y todas las versiones de 12.2.

Para el uso de la Velocidad de acceso pautada (COCHE), usted necesita el software release11.1CC del Cisco IOS y todo el software del versión de 12.0 y posterior.

Cómo minimizar el daño y limitar el polvillo radiactivo

Esta sección resume los vectores de la infección que pueden separar el virus NIMDA, y proporciona a las extremidades para reducir la extensión del virus:

- El gusano puede separarse a través de las conexiones del correo electrónico del tipo del IMITAR audio/x-wav.**Consejos:**Agregue las reglas en su servidor del Simple Mail Transfer Protocol (SMTP) para bloquear cualquier correo electrónico que tenga estas conexiones:readme.exeAdmin.dll
- El gusano puede separarse cuando usted hojea a un servidor Web infectado con la ejecución de Javascript activada y que usa una versión de Internet Explorer (IE) que sea vulnerable a los exploits discutidos en el MS01-020 (por ejemplo, IE 5.0 o IE 5.01 sin el SP2).**Consejos:**Utilice Netscape como su navegador, o inhabilite el Javascript en el IE, o consiga el IE parcheado a SP II.Utilice el Network-Based Application Recognition (NBAR) de Cisco para filtrar los ficheros readme.eml de ser descargado. Aquí está un ejemplo para configurar NBAR:
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Una vez que haya coincidido el tráfico, podrá optar por descartar o rutear basado en la política el tráfico para supervisar los hosts infectados. Los ejemplos de la instrumentación total se encuentran al usar el reconocimiento de la aplicación basada en la red y las listas de control de acceso para bloquear el gusano del “Código rojo”.
- El gusano puede separarse de la máquina para trabajar a máquina bajo la forma de ataques IIS (intenta sobre todo explotar las vulnerabilidades creadas por los efectos del rojo II del código, pero también las vulnerabilidades parcheadas previamente por el MS00-078).**Consejos:**Utilice los esquemas rojos del código descritos en:Qué hacer con mallocfail y la alta utilización de la CPU que surgen del gusano “Código rojo”Usando el reconocimiento de la aplicación basada en la red y las listas de control de acceso para bloquear el gusano del “Código rojo”
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*.ida*"
  Router(config-cmap)#match protocol http url "*cmd.exe*"
  Router(config-cmap)#match protocol http url "*root.exe*"
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Una vez que haya coincidido el tráfico, podrá optar por descartar o rutear basado en la política el tráfico para supervisar los hosts infectados. Los ejemplos de la instrumentación total se encuentran al usar el reconocimiento de la aplicación basada en la red y las listas de control de acceso para bloquear el gusano del “Código rojo”.el Tarifa-límite TCP sincroniza/los paquetes del comienzo (SYN). Esto no protege un host, pero permite que su

red se ejecute en una forma disminuida y todavía permanece para arriba. Por SYNs tarifa-limitador, usted está lanzando lejos los paquetes que exceden una cierta velocidad, así que algunas conexiones TCP conseguirán a través, pero no todos. Por los ejemplos de la configuración, refiera “tarifa que limita para a la sección de los paquetes SYN TCP” de usar el COCHE durante los ataques DOS.Considere tarifa-limitar el tráfico del Address Resolution Protocol (ARP) si la cantidad de exploraciones ARP está causando los problemas en la red. Para el tráfico del tarifa-límite ARP, configura el siguiente:

```
class-map match-any arp
   match protocol arp
!
!
policy-map ratelimitarp
   class arp
      police 8000 1500 1500 conform-action transmit exceed-action drop violate-action drop
```

Esta directiva entonces necesita ser aplicada al interfaz relevante LAN como política de resultado. Modifique las figuras como apropiadas abastecer el número de ARP por segundo que usted quiera permitir en la red.

- El gusano puede separarse destacando un .eml o .nws en el explorador con Active Directory (escritorio activo) activado (W2K/ME/W98 por abandono). Esto hace el THUMBVW.DLL ejecutar el fichero e intentar descargar el README.EML referido a él (dependiendo de su versión y de las Configuraciones de la zona IE).**Tip**: Según lo recomendado arriba, uso NBAR de filtrar readme.eml de ser descargado.
- El gusano puede separarse a través de las unidades correlacionadas. Cualquier equipo infectado que haya asociado los controladores de red infectará probablemente todos los ficheros en la unidad correlacionada y sus sub-directórios**Consejos:**Bloquee el Trivial File Transfer Protocol (TFTP) (puerto 69) de modo que los equipos infectados no puedan utilizar el TFTP para transferir los ficheros a los host no infectados. Asegúrese de que el acceso TFTP para el Routers esté todavía disponible (pues usted puede necesitar la trayectoria al código de actualización). Si el router está ejecutando la versión de software 12.0 del Cisco IOS o más adelante, usted tiene siempre la opción de usar el File Transfer Protocol (FTP) para transferir las imágenes al Routers que funciona con el software del Cisco IOS.Bloque NetBIOS. NetBIOS no debe tener que dejar un red de área local (LAN). Los proveedores de servicio deben filtrar NetBIOS hacia fuera por los puertos de bloqueo 137, 138, 139, y 445.
- El gusano hace uso de su propio motor SMTP para mandar los email para infectar otros sistemas.**Tip**: Bloquee el puerto 25 (SMTP) en las porciones internas de su red. Los usuarios que están extrayendo su email usando el protocolo Post Office Protocol (POP) 3 (puerto 110) o el protocolo de acceso del correo de Internet (IMAP) (puerto 143) no necesitan el acceso al puerto 25. Permita solamente que el puerto 25 sea revestimiento abierto el servidor SMTP para la red. Esto puede no ser posible para los usuarios que usan Eudora, Netscape, y Outlook Express, entre otros, pues tienen su propio motor SMTP y generarán las conexiones salientes usando el puerto 25. Una cierta investigación pudo necesitar ser aplicado a las aplicaciones posibles de los servidores proxy o de un cierto otro mecanismo.
- Limpie Cisco CallManager/Servidores de aplicaciones**Tip**: Los usuarios con los encargados de llamada y los servidores de aplicación de administrador de la llamada en sus redes tienen que hacer el siguiente para parar la extensión del virus. No deben hojear al equipo infectado del encargado de llamada y también no deben compartir ninguna unidades en el servidor de administración de la llamada. Siga las instrucciones proporcionadas en el virus NIMDA de la limpieza de Cisco CallManager 3.x y servidores de aplicaciones del CallManager para limpiar

el virus NIMDA.

- Filtre el virus NIMDA en el CSS11000**Tip**: Los usuarios con el CSS11000 deben seguir las instrucciones proporcionadas en la filtración del virus NIMDA en el CSS11000 para limpiar el virus NIMDA.
- Respuesta del sistema seguro detector de intrusión de Cisco (identificación del CS) al virus NIMDA**Tip**: La identificación del CS tiene dos diversos componentes disponibles. Uno es el IDS mediante host (HIDS) que tiene un sensor y la identificación Basada en red (NIDS) del host que tiene un sensor de la red, que responde de una diversa manera al virus NIMDA. Por una explicación más detallada y las medidas recomendadas, refiérase a cómo el Cisco Secure IDS responde al virus NIMDA.

Información Relacionada

- Usando el reconocimiento de la aplicación basada en la red y las listas de control de acceso para bloquear el gusano del “Código rojo”
- Qué hacer con mallocfail y la alta utilización de la CPU que surgen del gusano “Código rojo”
- Uso de CAR durante ataques de DOS
- Advisories y avisos del Cisco Security
- Soporte técnico y documentación - Cisco Systems