Cómo proteger su red del virus Nimda

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Antecedentes](#)
[Plataformas Soportadas](#)
[Cómo minimizar el daño y limitar el polvillo radiactivo](#)
[Información Relacionada](#)

Introducción

Este documento describe los modos para minimizar el impacto del gusano NIMDA en su red. Este documento abarca 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 propagación de este gusano?

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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 obtener más información sobre las convenciones del documento, consulte las Convenciones

de 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 Soportadas

La solución del Network-Based Application Recognition (NBAR) descrita en este documento requiere la característica de marcación basada en la clase 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

Nota: Para utilizar el reconocimiento de la aplicación basada en la red (NBAR) debe activar Cisco Express Forwarding (CEF).

El NBAR también se soporta en algunas Plataformas del Cisco IOS Software que comienzan con la versión 12.1E. Consulte “Protocolos admitidos” en la documentación de Network-Based Application Recognition.

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 el NBAR, sea consciente del Id. de bug Cisco CSCdv06207 (clientes registrados solamente). El método alternativo que se describe en CSCdv06207 puede ser necesario si aparece este defecto.

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

Cisco IOS Software.

Para las soluciones donde usted necesita utilizar el comando line interface(cli) de la calidad de servicio modular (QoS) (por ejemplo para el tráfico ARP de la limitación de la tarifa o implementar la tarifa que limita con el policer en vez del CAR), 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 (CAR), usted necesita el Cisco IOS Software release11.1CC y todas las versiones y posterior del software 12.0.

Cómo minimizar el daño y limitar el polvillo radiactivo

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

- El gusano puede separarse a través de los elementos adjuntos de 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 habilitada 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 Reconocimiento de aplicación con base en la red de Cisco (NBAR) para evitar que se descarguen archivos leame.eml Aquí está un ejemplo para configurar el 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 código rojo II, pero también las vulnerabilidades parcheadas previamente por el MS00-078).**Consejos:**Use los esquemas del Código Rojo 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”.Limite la velocidad de los paquetes SYN (sincronizar/iniciar) TCP. Esto no protege un host, pero permite que su red se ejecute en una forma disminuida y todavía permanece para arriba. Por la limitación de la tarifa SYN, usted

está lanzando lejos los paquetes que exceden una cierta velocidad, así que algunas conexiones TCP conseguirán a través, pero no todos. Para los ejemplos de configuración, refiera “tarifa que limita para a la sección de los paquetes SYN TCP” de usar el CAR durante los ataques DOS.Considere el tráfico del Address Resolution Protocol (ARP) de la limitación de la tarifa si la cantidad de exploraciones ARP está causando los problemas en la red. Para limitar la velocidad del tráfico de ARP, configure lo 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
```

Entonces, esta política debe aplicarse a la interfaz LAN pertinente como una política de resultados. Modifique las figuras como apropiadas abastecer el número de ARP por segundo que usted quiera permitir en la red.

- El gusano puede separarse resaltando un .eml o .nws en el explorador con Active Directory (escritorio activo) habilitado (W2K/ME/W98 por abandono). Esto hace que THUMBVW.DLL ejecute el archivo e intente descargar el README.EML al cual aquél hace referencia (según la versión de IE y configuraciones de zona).**Consejo:** Según lo recomendado arriba, uso NBAR de filtrar readme.eml de ser descargado.
- El gusano puede propagarse por la unidad asignada. Cualquier equipo infectado que haya asociado los controladores de red infectará probablemente todos los archivos 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 archivos a los host no infectados. Asegúrese de que el acceso TFTP a los Routers esté todavía disponible (pues usted puede necesitar la trayectoria al código de actualización). Si el router es la versión del Cisco IOS Software corriente 12.0 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 Cisco IOS Software.NetBios del bloque. El NetBios no debe tener que dejar un red de área local (LAN). Los proveedores del servicio deberían filtrar NetBIOS mediante los puertos de bloqueo 137, 138, 139 y 445.
- El gusano usa su propio motor SMTP para enviar correos electrónicos fuera e infecta otros sistemas.**Consejo:** Bloquee el puerto 25 (S TP) 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 Internet Mail Access Protocol (IMAP) (puerto 143) no necesitan el acceso al puerto 25. Sólo permita que el puerto 25 se abra enfrentando al 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. Sería conveniente investigar los usos posibles de los servidores proxy o de algún otro mecanismo.
- Limpie el Cisco CallManager/a los Servidores de aplicaciones**Consejo:** Los usuarios con el Call Managers 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 administrador 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 del Cisco CallManager 3.x y de los servidores de aplicaciones del CallManager para limpiar el virus NIMDA.
- Filtre el virus NIMDA en el CSS11000**Consejo:** 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 Cisco Secure Intrusion Detection System (CS IDS) al virus NIMDA**Consejo:** El CS IDS tiene dos diversos componentes disponibles. Uno es el IDS mediante host (HIDS) que tiene un sensor y el network basado IDS (NID) del host que tiene un sensor de la red, que responde de una diversa manera al virus NIMDA. Por una más explicación 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
- Cisco Security Advisory y avisos
- Soporte Técnico y Documentación - Cisco Systems