Como proteger sua rede contra o vírus Nimda

Contents

Introduction

Este documento descreve maneiras de minimizar o impacto do worm Nimda na rede. Este documento aborda dois tópicos:

- A rede está infectada, o que pode ser feito? Como você pode minimizar os danos e as perdas?
- A rede ainda não está infectada ou está apenas parcialmente infectada. O que pode ser feito para minimizar a disseminação desse worm?

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

Para obter informações de fundo sobre o worm Nimda, consulte os seguintes 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 suportadas

A solução NBAR (Network-Based Application Recognition, reconhecimento de aplicativos baseados em rede) descrita neste documento requer o recurso de marcação baseado em classe no software Cisco IOS®. Especificamente, a capacidade de corresponder em uma parte de um URL de HTTP usa o recurso de classificação de subporta HTTP dentro do NBAR. As plataformas suportadas e os requisitos mínimos do Cisco IOS Software estão resumidos a seguir:

Platform	Versão mínima do Cisco IOS Software
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

Observação: você precisa habilitar o Cisco Express Forwarding (CEF) para usar o NBAR (Reconhecimento de Aplicativos Baseado em Rede).

O NBAR também é suportado em algumas plataformas do software Cisco IOS a partir da versão 12.1E. Consulte "Protocolos suportados" na documentação de reconhecimento de aplicativos baseados em rede.

A marcação baseada em classe e o Distributed NBAR (DNBAR) também estão disponíveis nas seguintes plataformas:

Platform	Versão mínima do Cisco IOS Software
7500	12.1(6)E
FlexWAN	12.1(6)E

Se você estiver implantando o NBAR, esteja ciente da ID de bug da Cisco CSCdv06207 (somente clientes registrados) . A solução alternativa descrita em CSCdv06207 talvez seja necessária se você encontrar este defeito.

A solução Access Control List (ACL) é suportada em todas as versões atuais do software Cisco IOS.

Para soluções em que você precisa usar a interface de linha de comando (CLI) de Qualidade de Serviço Modular (QoS - Modular Quality of Service) (como para tráfego ARP de limitação de taxa ou para implementar limitação de taxa com vigilante em vez de CAR), você precisa da Interface de Linha de Comando de Qualidade de Serviço Modular disponível nas versões 12.0XE, 12.1E do software Cisco IOS e todas as versões de 12.2.

Para o uso da Taxa de Acesso Comprometida (CAR - Committed Access Rate), você precisa do software Cisco IOS versão 11.1CC e de todas as versões do software 12.0 e posteriores.

Como minimizar os danos e limitar a falha

Esta seção descreve os vetores de infecção que podem espalhar o vírus Nimda e fornece dicas para reduzir a propagação do vírus:

- O worm pode se espalhar por anexos de e-mail do tipo MIME audio/x-wav.**Dicas:**Adicione regras no servidor SMTP (Simple Mail Transfer Protocol) para bloquear qualquer e-mail que tenha estes anexos:readme.exeAdmin.dll
- O worm pode se espalhar quando você navega por um servidor Web infectado com a execução do Javascript ativada e usa uma versão do Internet Explorer (IE) vulnerável às explorações discutidas no MS01-020 (por exemplo, IE 5.0 ou IE 5.01 sem SP2).**Dicas:**Use o Netscape como seu navegador, ou desative o Javascript no IE, ou obtenha o IE corrigido no SP II.Utilize o NBAR (Reconhecimento de aplicativo baseado em rede) da Cisco para filtrar os arquivos readme.eml a serem baixados. Aqui está um exemplo para configurar o NBAR:
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Após comparar o tráfego, você pode optar por descartar ou roteá-lo com base em política, para monitorar os hosts infectados. Exemplos da implementação completa estão em Using Network-Based Application Recognition and Access Control Lists for Blocking the "Code Red" Worm (Uso do reconhecimento de aplicativos baseado em rede e listas de controle de acesso para bloquear o worm "Code Red").
- O worm pode se espalhar de máquina para máquina na forma de ataques do IIS (ele tenta principalmente explorar vulnerabilidades criadas pelos efeitos do Code Red II, mas também vulnerabilidades previamente corrigidas pelo MS00-078).**Dicas:**Use os esquemas de código vermelho descritos em:Lidando com mallocfail e utilização elevada de CPU, resultante do worm "código vermelho”Usando o reconhecimento de aplicativos baseado em rede e listas de controle de acesso para bloquear o worm "Código vermelho"
  ```
  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*"
  ```
  Após comparar o tráfego, você pode optar por descartar ou roteá-lo com base em política, para monitorar os hosts infectados. Exemplos da implementação completa estão em Using Network-Based Application Recognition and Access Control Lists for Blocking the "Code Red" Worm (Uso do reconhecimento de aplicativos baseado em rede e listas de controle de acesso para bloquear o worm "Code Red").Pacotes SYN (sincronizar/iniciar) de TCP de limite de taxa. Isso não protege um host, mas permite que sua rede funcione de maneira degradada e ainda permaneça ativa. Ao limitar a taxa de SYNs, você está jogando fora pacotes que excedem uma determinada taxa, de modo que algumas conexões TCP passarão, mas não todas. Para obter exemplos de configuração, consulte a seção "Limite de taxa para pacotes

TCP SYN" de Uso de CAR durante ataques DOS.Considere o tráfego do Protocolo de Resolução de Endereços (ARP - Address Resolution Protocol) limitador de taxa se a quantidade de varreduras ARP estiver causando problemas na rede. Para limitar a taxa de tráfego ARP, configure o seguinte:

```
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
```

Em seguida, essa política precisa ser aplicada à interface LAN relevante como uma política de saída. Modifique as figuras conforme apropriado para atender ao número de ARPs por segundo que você deseja permitir na rede.

- O worm pode se espalhar realçando .eml ou .nws no Explorer com Ative Desktop habilitado (W2K/ME/W98 por padrão). Isso faz com que a THUMBVW.DLL execute o arquivo e tente carregar o README.EML relacionado nele (dependendo de sua versão do IE e configurações de zona).**Dica:** conforme recomendado acima, use NBAR para filtrar o arquivo readme.eml de download.
- O worm pode se difundir em unidades mapeadas. Qualquer máquina infectada que tenha mapeado unidades de rede provavelmente infectará todos os arquivos na unidade mapeada e seus subdiretórios**Dicas:**Bloquear Protocolo de Transferência Trivial de Arquivos (TFTP - Trivial File Transfer Protocol) (porta 69) para que as máquinas infectadas não possam usar o TFTP para transferir arquivos para hosts não infectados. Verifique se o acesso TFTP para roteadores ainda está disponível (pois você pode precisar do caminho para atualizar o código). Se o roteador estiver executando o software Cisco IOS versão 12.0 ou posterior, você sempre terá a opção de usar o FTP para transferir imagens para roteadores que executam o software Cisco IOS.Bloquear NetBIOS. O NetBIOS não deve ter que deixar uma rede local (LAN). Os provedores de serviços devem filtrar a saída de NetBIOS, bloqueando as portas 137, 138, 139 e 445.
- O worm utiliza seu próprio mecanismo de SMTP para enviar e-mails e infectar outros sistemas.**Dica:** bloqueie a porta 25 (SMTP) nas partes internas da rede. Os usuários que estão recuperando seus e-mails usando o Protocolo de Correio (POP - Post Office Protocol) 3 (porta 110) ou o Protocolo de Acesso ao Internet Mail (IMAP - Internet Mail Access Protocol) (porta 143) não precisam de acesso à porta 25. Só permita que a porta 25 seja aberta direcionando o servidor de SMTP para a rede. Isso pode não ser viável para usuários que usam Eudora, Netscape e Outlook Express, entre outros, pois eles têm seu próprio mecanismo SMTP e gerarão conexões de saída usando a porta 25. Pode ser necessário realizar uma investigação dos possíveis usos dos servidores proxy ou de algum outro mecanismo.
- Limpar servidores Cisco CallManager/Applications**Dica:** os usuários com servidores de aplicativos Call Managers e Call Manager em suas redes devem fazer o seguinte para interromper a propagação do vírus. Eles não devem navegar até a máquina infectada do Call Manager e também não devem compartilhar nenhuma unidade no servidor do Call Manager. Siga as instruções fornecidas em Clearing Nimda Virus from Cisco CallManager 3.x and CallManager Applications Servers para limpar o vírus Nimda.
- Filtre o vírus Nimda no CSS 11000**Dica:** os usuários com CSS 11000 devem seguir as instruções fornecidas em Filtragem do vírus Nimda no CSS 11000 para limpar o vírus NIMDA.

- Resposta do Cisco Secure Intrusion Detection System (CS IDS) ao vírus Nimda**Dica:** o CS IDS tem dois componentes diferentes disponíveis. Um é o IDS baseado em host (HIDS) que tem um sensor de host e o IDS baseado em rede (NIDS) que tem um sensor de rede, ambos respondendo de maneira diferente ao vírus Nimda. Para obter uma explicação mais detalhada e o curso de ação recomendado, consulte Como o Cisco Secure IDS responde ao vírus Nimda.

Informações Relacionadas

- Usando o reconhecimento de aplicativos baseado em rede e listas de controle de acesso para bloquear o worm "Código vermelho"
- Lidando com mallocfail e utilização elevada de CPU, resultante do worm "código vermelho"
- Usando CAR durante ataques de DOS
- Avisos e conselhos de segurança da Cisco
- Suporte Técnico e Documentação - Cisco Systems