Como proteger sua rede contra o vírus Nimda

Índice

Introdução

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

- A rede é contaminada, o que pode ser feita? Como pode você minimizar o dano e a precipitação?
- A rede não é contaminada ainda, nem é contaminada somente parcialmente. O que pode ser feito para minimizar a disseminação desse worm?

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

Para a informações de fundo no worm de Nimda, refira estes 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 do Network-Based Application Recognition (NBAR) descrita neste documento exige os recursos de marcação baseado em classe dentro do software de 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:

Plataforma	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

Nota: É necessário habilitar o CEF (Cisco Express Forwarding) para usar o NBAR (Reconhecimento de Aplicativo Baseado em Rede).

O NBAR é apoiado igualmente em algumas Plataformas de Cisco IOS Software que começam com liberação 12.1E. Veja “protocolos suportados” na documentação do reconhecimento de aplicativo baseado em rede.

O Class-based Marking e o nbar distribuído (DNBAR) estão igualmente disponíveis nas seguintes Plataformas:

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

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

A solução do Access Control List (ACL) é apoiada em todas as versões atual do Cisco IOS Software.

Para as soluções onde você precisa de usar o comando line interface(cli) da Qualidade de Serviço modular (QoS) (como para o tráfego ARP da taxa limite ou para executar a taxa que limita com o vigilante em vez do CAR), você precisa a interface de Command-Line Qualidade de Serviço Modular que está disponível nos Cisco IOS Software Release 12.0XE, no 12.1E, no 12.1T, e em todas as liberações de 12.2.

Para o uso de taxa de acesso comprometida (CAR), você precisa o Cisco IOS Software release11.1CC e todo o software do liberação de 12.0 e o mais atrasado.

Como minimizar o dano e limitar a precipitação

Esta seção esboça os vetores da infecção que podem espalhar o vírus de NIMDA, e fornece pontas para reduzir a propagação do vírus:

- O worm pode espalhar com os anexos de Email do tipo MIMICAR audio/x-wav.**Dicas:**Adicionar regras em seu server do Simple Mail Transfer Protocol (SMTP) para obstruir todo o email que tiver estes acessórios:readme.exeAdmin.dll
- O worm pode espalhar quando você consulta um servidor de Web contaminado com a execução em javascript permitida e que usa uma versão de Internet Explorer (IE) que seja vulnerável às façanhas discutidas no MS01-020 (por exemplo, IE 5.0 ou IE 5.01 sem SP2).**Dicas:**Use Netscape como seu navegador, ou desabilite o Javascript no IE, ou obtenha o IE remendado a SP II.Utilize o NBAR (Reconhecimento de aplicativo baseado em rede) da Cisco para filtrar os arquivos readme.eml a serem baixados. Está aqui 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. Os exemplos da implementação direta são encontrados em usar o reconhecimento de aplicativo baseado em rede e as listas de controle de acesso para obstruir o worm do “código vermelho”.
- O worm pode espalhar da máquina para fazer à máquina sob a forma dos ataques IIS (tenta primeiramente explorar as vulnerabilidades criadas pelos efeitos do código vermelho II, mas igualmente as vulnerabilidades remendadas previamente 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 aplicativo baseado em rede e as listas de controle de acesso para obstruir o worm do “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. Os exemplos da implementação direta são encontrados em usar o reconhecimento de aplicativo baseado em rede e as listas de controle de acesso para obstruir o worm do “código vermelho”.Pacotes SYN (sincronizar/iniciar) de TCP de limite de taxa. Isto não protege um host, mas permite que sua rede seja executado em um modo degradado e ainda permanece acima. Pela taxa limite SYN, você está jogando afastado os pacotes que excedem uma determinada taxa, assim que algumas conexões de TCP obterão completamente, mas não tudo. Para exemplos de configuração, refira “taxa que limita para a seção dos pacotes SYN de TCP” de usar o CAR durante ataques DOS.Considere o tráfego

do Protocolo de Resolução de Endereço de taxa limitante (ARP) se a quantidade de varreduras ARP está 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. Altere as figuras como apropriadas para cobrir por segundo o número de ARP que você quer permitir na rede.

- O worm pode espalhar destacando um .eml ou .nws no explorador com a área de trabalho ativa permitida (W2K/ME/W98 à revelia). 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:** Como recomendado acima, uso NBAR filtrar readme.eml da transferência.
- O worm pode se difundir em unidades mapeadas. Toda a máquina infectada que traçar driveres de rede contaminará provavelmente todos os arquivos na movimentação traçada e em seus sub-diretórios**Dicas:**Obstrua o Trivial File Transfer Protocol (TFTP) (porta 69) de modo que as máquinas infectadas não possam usar o TFTP para transferir arquivos aos anfitriões NON-contaminados. Assegure-se de que o acesso TFTP para roteadores esteja ainda disponível (porque você pode precisar o trajeto ao código de upgrade). Se o roteador é versão 12.0 ou mais recente running do Cisco IOS Software, você tem sempre a opção de USO do protocolo de transferência de arquivo (FTP) transferir imagens ao Roteadores que executa o Cisco IOS Software.Bloco NetBIOS. NetBIOS não deve ter que sair de uma rede de área 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:** Obstrua a porta 25 (S TP) nas porções internas de sua rede. Os usuários que estão recuperando seu email usando o protocolo Post Office Protocol (POP) 3 (porta 110) ou o protocolo de acesso do correio de Internet (IMAP) (porta 143) não precisam o acesso à porta 25. Só permita que a porta 25 seja aberta direcionando o servidor de SMTP para a rede. Isto não pode ser praticável para os usuários que usam Eudora, Netscape, e Outlook Express, entre outros, porque têm seu próprio Engine de SMTP e gerarão conexões externas usando a porta 25. Pode ser necessário realizar uma investigação dos possíveis usos dos servidores proxy ou de algum outro mecanismo.
- Limpe o CallManager da Cisco/servidores de aplicativos**Dica:** Os usuários com os serveres de aplicativo dos gerenciadores de chamada e do gerenciador de chamada em suas redes têm que fazer o seguinte para parar o espalhamento do vírus. Não devem consultar à máquina infectada do gerenciador de chamada e igualmente não devem compartilhar de nenhuma movimentações no server do gerenciador de chamada. Siga as instruções fornecidas no vírus de NIMDA da limpeza do CallManager da Cisco 3.x e nos servidores de Aplicativos CallManager limpando o vírus de NIMDA.
- Filtre o vírus de NIMDA no CSS11000**Dica:** Os usuários com CSS11000 devem seguir as instruções fornecidas em filtrar o vírus de NIMDA no CSS11000 limpando o vírus de NIMDA.
- Resposta do Cisco Secure Intrusion Detection System (CS IDS) ao vírus de NIMDA**Dica:** O CS IDS tem dois componentes diferentes disponíveis. Um é o IPS baseados em host (HIDS)

que tem um sensor do host e o IDS Com base na rede (NID) que tem um sensor de rede, ambo responde em uma maneira diferente ao vírus de NIMDA. Para mais explicação detalhada e o curso de ação recomendado, refira como o Cisco Secure IDS responde ao vírus de NIMDA.

Informações Relacionadas

- Usando o reconhecimento de aplicativo baseado em rede e as listas de controle de acesso para obstruir o worm do “código vermelho”
- Lidando com mallocfail e utilização elevada de CPU, resultante do worm "código vermelho”
- Usando CAR durante ataques de DOS
- Recomendações de Segurança da Cisco e observações
- Suporte Técnico e Documentação - Cisco Systems