Comment protéger votre réseau contre le virus Nimda

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Conventions](#)
[Informations générales](#)
[Plates-formes prises en charge](#)
[Comment minimiser les dommages et limiter les retombées](#)
[Informations connexes](#)

Introduction

Ce document décrit les moyens de minimiser l'impact du ver Nimda sur votre réseau. Ce document traite de deux sujets :

- Le réseau est infecté. Que peut-on faire ? Comment pouvez-vous minimiser les dommages et les retombées ?
- Le réseau n'est pas encore infecté ou n'est que partiellement infecté. Que peut-on faire pour réduire la propagation de ce ver ?

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Pour obtenir des informations de base sur le ver Nimda, reportez-vous aux liens suivants :

- 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

Plates-formes prises en charge

La solution de reconnaissance d'application basée sur le réseau (NBAR) décrite dans ce document nécessite la fonctionnalité de marquage basée sur les classes dans le logiciel Cisco IOS®. Et plus particulièrement, la capacité de faire correspondre sur n'importe quelle partie d'une adresse URL HTTP, la fonction de classification de port secondaire HTTP à l'intérieur d'une NBAR. Les plates-formes compatibles et les spécifications minimum requises pour le logiciel Cisco IOS sont récapitulées ci-dessous :

Plateforme	Version logicielle Cisco IOS minimale
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

Remarque : vous devez activer Cisco Express Forwarding (CEF) afin d'utiliser la reconnaissance d'application basée sur le réseau (NBAR).

NBAR est également pris en charge sur certaines plates-formes logicielles Cisco IOS à partir de la version 12.1E. Reportez-vous à la section « Protocoles pris en charge » dans la documentation de Network-Based Application Recognition.

Le marquage basée sur les classes et les NBAR distribués (DNBAR) sont également disponibles sur les plates-formes suivantes :

Plateforme	Version logicielle Cisco IOS minimale
7500	12.1(6)E

FlexWAN	12.1(6)E

Si vous déployez NBAR, tenez compte de l'ID de bogue Cisco CSCdv06207 (clients enregistrés uniquement) . La solution de contournement décrite dans CSCdv06207 peut être nécessaire si vous rencontrez ce défaut.

La solution ACL (Access Control List) est prise en charge dans toutes les versions actuelles du logiciel Cisco IOS.

Pour les solutions nécessitant l'utilisation de l'interface de ligne de commande (CLI) de la qualité de service modulaire (QoS) (par exemple pour le trafic ARP à limitation de débit ou pour mettre en oeuvre la limitation de débit avec le régulateur au lieu de CAR), vous avez besoin de l'interface de ligne de commande de la qualité de service modulaire qui est disponible dans le logiciel Cisco IOS versions 12.0XE, 12.1E, 12.1T et toutes les versions de 12.2.

Pour utiliser le débit CAR (Committed Access Rate), vous avez besoin de la version 11.1CC de la plate-forme logicielle Cisco IOS et de toutes les versions 12.0 et ultérieures.

Comment minimiser les dommages et limiter les retombées

Cette section décrit les vecteurs d'infection qui peuvent propager le virus Nimda et fournit des conseils pour réduire la propagation du virus :

- Le ver peut se propager via des pièces jointes de type MIME audio/x-wav.

  Conseils:

  - Ajoutez des règles sur votre serveur SMTP (Simple Mail Transfer Protocol) pour bloquer tout e-mail contenant les pièces jointes suivantes :

    - readme.exe

    - Admin.dll

- Le ver peut se propager lorsque vous naviguez sur un serveur Web infecté avec l'exécution Javascript activée et en utilisant une version d'Internet Explorer (IE) qui est vulnérable aux exploits décrits dans MS01-020 (par exemple, IE 5.0 ou IE 5.01 sans SP2).

  Conseils:

  - Utilisez Netscape comme navigateur, désactivez Javascript sur IE ou installez un correctif IE sur SP II.

  - Utilisez Cisco Network-based application Recognition (NBAR) pour empêcher le téléchargement des fichiers readme.eml. Voici un exemple de configuration de NBAR :

    <#root>

    ```
    Router(config)#
    ```

```
class-map match-any http-hacks
Router(config-cmap)#
match protocol http url "*readme.eml*"
```

Une fois que vous avez fait correspondre le trafic, vous pouvez choisir d'abandonner le trafic ou de le router en fonction d'une stratégie pour surveiller les hôtes infectés. Vous trouverez des exemples de mise en oeuvre complète dans Utilisation de la reconnaissance des applications réseau et des listes de contrôle d'accès pour bloquer le ver « Code Red ».

- Le ver peut se propager d'une machine à l'autre sous la forme d'attaques IIS (il tente principalement d'exploiter les vulnérabilités créées par les effets de Code Red II, mais aussi les vulnérabilités précédemment corrigées par MS00-078).

  Conseils:

  - Utilisez les schémas Code Red décrits dans :

    Réponse à un cas d'erreur mallocfail ou d'utilisation élevée du processeur résultant du ver « Code Red »

    Utilisation de la reconnaissance des applications réseau et des listes de contrôle d'accès pour bloquer le ver « Code Red »

    <#root>

    ```
    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*"
    ```

Une fois que vous avez fait correspondre le trafic, vous pouvez choisir d'abandonner le trafic ou de le router en fonction d'une stratégie pour surveiller les hôtes infectés. Vous trouverez des exemples de mise en oeuvre complète dans Utilisation de la reconnaissance des applications réseau et des listes de contrôle d'accès pour bloquer le ver « Code Red ».

- Paquets SYN (Synchronize/Start) TCP Rate-Limit. Cela ne protège pas un hôte, mais permet à votre réseau de fonctionner de manière dégradée et de rester opérationnel. En limitant le débit des SYN, vous jetez les paquets qui dépassent un certain débit, de sorte que certaines connexions TCP passent, mais pas toutes. Pour des exemples de configuration, référez-vous à la section « Limitation de débit pour les paquets SYN TCP » de Utilisation de CAR pendant des attaques DOS.
- Envisagez le trafic ARP (Address Resolution Protocol) à débit limité si la quantité d'analyses ARP entraîne des problèmes sur le réseau. Pour limiter le débit du trafic ARP, configurez les éléments suivants :

<#root>

```
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
```

Cette stratégie doit ensuite être appliquée à l'interface LAN concernée en tant que stratégie de sortie. Modifiez les figures comme il convient pour tenir compte du nombre de protocoles ARP par seconde que vous souhaitez autoriser sur le réseau.

- Le ver peut se propager en mettant en surbrillance un .eml ou un .nws dans Explorer avec Active Desktop activé (W2K/ME/W98 par défaut). Cela entraîne l'exécution du fichier THUMBVW.DLL et la tentative de téléchargement du fichier README.EML référencé dans celui-ci (en fonction de la version d'IE et des paramètres de zone).

  Conseil : comme recommandé ci-dessus, utilisez NBAR pour empêcher le téléchargement de readme.eml.

- Le ver peut se propager à travers les lecteurs mappés. Toute machine infectée ayant des lecteurs réseau mappés infectera probablement tous les fichiers sur le lecteur mappé et ses sous-répertoires

  Conseils:

  - Bloquez le protocole TFTP (Trivial File Transfer Protocol) (port 69) afin que les ordinateurs infectés ne puissent pas utiliser TFTP pour transférer des fichiers vers des hôtes non infectés. Assurez-vous que l'accès TFTP pour les routeurs est toujours

disponible (car vous aurez peut-être besoin du chemin pour mettre à niveau le code). Si le routeur exécute le logiciel Cisco IOS version 12.0 ou ultérieure, vous avez toujours la possibilité d'utiliser le protocole FTP (File Transfer Protocol) pour transférer des images aux routeurs exécutant le logiciel Cisco IOS.

    - Bloquez NetBIOS. NetBIOS ne doit pas avoir à quitter un réseau local (LAN). Les fournisseurs de services doivent filtrer NetBIOS en bloquant les ports 137, 138, 139 et 445.

- Le ver utilise son propre moteur SMTP pour envoyer des e-mails afin d'infecter d'autres systèmes.

  Conseil : bloquez le port 25 (SMTP) sur les parties internes de votre réseau. Les utilisateurs qui récupèrent leur courrier électronique à l'aide du protocole POP (Post Office Protocol) 3 (port 110) ou IMAP (Internet Mail Access Protocol) (port 143) n'ont pas besoin d'accéder au port 25. Autorisez uniquement l'ouverture du port 25 face au serveur SMTP pour le réseau. Cela peut ne pas être faisable pour les utilisateurs d'Eudora, Netscape et Outlook Express, entre autres, car ils disposent de leur propre moteur SMTP et génèrent des connexions sortantes à l'aide du port 25. Il peut s'avérer nécessaire d'étudier les utilisations possibles des serveurs proxy ou d'un autre mécanisme.

- Nettoyer les serveurs Cisco CallManager/Applications

  Conseil : les utilisateurs disposant de serveurs d'applications Call Manager et Call Manager sur leurs réseaux doivent effectuer les actions suivantes pour arrêter la propagation du virus. Ils ne doivent pas rechercher la machine infectée à partir du Gestionnaire d'appels et ne doivent pas non plus partager de lecteurs sur le serveur du Gestionnaire d'appels. Suivez les instructions fournies dans Nettoyage du virus Nimda à partir de Cisco CallManager 3.x et des serveurs d'applications CallManager pour nettoyer le virus Nimda.

- Filtrer le virus Nimda sur le CSS 11000

  Conseil : les utilisateurs de CSS 11000 doivent suivre les instructions fournies dans Filtrage du virus Nimda sur CSS 11000 pour le nettoyage du virus NIMDA.

- Réponse de Cisco Secure Intrusion Detection System (CS IDS) au virus Nimda

  Conseil : deux composants différents sont disponibles pour le système CS IDS. L'un d'eux est le système IDS basé sur l'hôte (HIDS), qui possède un capteur hôte, et le système IDS basé sur le réseau (NIDS), qui possède un capteur réseau, qui répondent tous deux d'une manière différente au virus Nimda. Pour une explication plus détaillée et la ligne de conduite recommandée, consultez Comment Cisco Secure IDS répond au virus Nimda.

Informations connexes

- Utilisation de la reconnaissance des applications réseau et des listes de contrôle d'accès pour bloquer le ver « Code Red »
- Réponse à un cas d'erreur mallocfail ou d'utilisation élevée du processeur résultant du ver «

Code Red »
- Utilisation de CAR lors d'attaques par déni de service (DoS)
- Notifications et avis de sécurité Cisco
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.