Comment protéger votre réseau contre le virus Nimda

Contenu

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

Introduction

Ce document décrit des manières de réduire l'incidence du ver Nimda sur votre réseau. Ce document aborde deux thèmes :

- Le réseau est infecté, ce qui peut être fait ? Comment pouvez-vous réduire les dommages et les retombées radioactives ?
- Le réseau n'est pas encore infecté, ou seulement est partiellement infecté. Que peut être fait pour réduire se propager de ce ver ?

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Pour l'information générale sur le ver Nimda, référez-vous à ces liens :

- 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 fondée sur le réseau (NBAR) décrite dans ce document exige le fonctionnalité de marquage basée sur les classes dans le logiciel de 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 :

Plate-forme	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

Note: Vous devez permettre au Technologie Cisco Express Forwarding (CEF) afin d'utiliser le Reconnaissance d'application fondée sur le réseau (NBAR).

NBAR est également pris en charge sur quelques plates-formes logicielles de Cisco IOS commençant par la version 12.1E. Voir « les protocoles pris en charge » dans la documentation Fondé(e) sur le réseau de reconnaissance d'application.

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

Plate-forme	Version logicielle Cisco IOS minimale
7500	12.1(6)E
FlexWAN	12.1(6)E

Si vous déployez NBAR, rendez-vous compte de l'ID de bogue Cisco CSCdv06207 (clients enregistrés seulement). Le contournement décrit dans CSCdv06207 peut être nécessaire si vous rencontrez ce défaut.

La solution de liste de contrôle d'accès (ACL) est prise en charge dans des toutes les versions en cours de logiciel de Cisco IOS.

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

Pour l'usage du Fonction Committed Access Rate (CAR), vous avez besoin du logiciel release11.1CC de Cisco IOS et de tout le logiciel de release de 12.0 et postérieur.

Comment réduire les dommages et limiter les retombées radioactives

Cette section trace les grandes lignes des vecteurs d'infection qui peuvent se propager le virus Nimda, et fournit des conseils pour réduire l'étalement du virus :

- Le ver peut se propager par des pièces jointes à un courriel du type MIME audio/x-wav.**Conseils :**Ajoutez les règles sur votre serveur de Protocole SMTP (Simple Mail Transfer Protocol) de bloquer n'importe quel email qui a ces connexions :readme.exeAdmin.dll
- Le ver peut se propager quand vous parcourez un web server infecté avec l'exécution de Javascript activée et utilisante une version de l'Internet Explorer (IE) qui est vulnérable aux exploits discutées dans MS01-020 (par exemple, IE 5.0 ou IE 5.01 sans SP2).**Conseils :**Utilisez Netscape en tant que votre navigateur, ou désactivez le Javascript sur l'IE, ou obtenez l'IE corrigé au fournisseur de services II.Employez le Reconnaissance d'application fondée sur le réseau (NBAR) de Cisco pour filtrer des fichiers readme.eml d'être téléchargé. Voici un exemple pour configurer NBAR :
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Une fois que vous avez apparié le trafic, vous pouvez choisir de jeter ou artère basée par stratégie le trafic pour surveiller les hôtes infectés. Des exemples de l'implémentation complète sont trouvés en utilisant la reconnaissance Fondé(e) sur le réseau et les listes de contrôle d'accès d'application pour bloquer le ver de « Code Red ».
- Le ver peut se propager de la machine à machine sous forme d'attaques IIS (elle tente principalement d'exploiter des vulnérabilités créées par les effets du Code Red II, mais également des vulnérabilités précédemment corrigées par MS00-078).**Conseils :**Utilisez les schéma Code Red décrits dans :**Réponse à un cas d'erreur mallocfail ou d'utilisation élevée du processeur résultant du ver « Code Red »**Utilisant la reconnaissance Fondé(e) sur le réseau et les listes de contrôle d'accès d'application pour bloquer le ver de « Code Red »
  ```
  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 apparié le trafic, vous pouvez choisir de jeter ou artère basée par stratégie le trafic pour surveiller les hôtes infectés. Des exemples de l'implémentation complète sont trouvés en utilisant la reconnaissance Fondé(e) sur le réseau et les listes de contrôle d'accès d'application pour bloquer le ver de « Code Red ».Le TCP de rate-limit synchronisent/paquets de début (synchronisation). Ceci ne protège pas un hôte, mais il

permet à votre réseau de fonctionner d'une manière dégradée et reste toujours. Par des synchronisations de limitation de débit, vous jetez les paquets qui dépassent un certain débit, ainsi quelques connexions TCP obtiendront, mais pas tous. Pour des exemples de configuration, référez-vous « limitation de débit à la section pour de TCP de synchronisation paquets » d'utiliser le CAR pendant les attaques DoS.Considérez le trafic de protocole de résolution d'adresses à limitation de débit (ARP) si la quantité de balayages d'ARP pose des problèmes dans le réseau. Au trafic ARP de rate-limit, configurez ce qui suit :

```
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 alors être appliquée à l'interface appropriée de RÉSEAU LOCAL comme stratégie de sortie. Modifiez les figures comme appropriées pour couvrir le nombre d'ARPs par seconde que vous voulez accorder sur le réseau.

- Le ver peut se propager en mettant en valeur un .eml ou .nws dans l'explorateur avec l'Active Desktop activé (W2K/ME/W98 par défaut). Ceci fait exécuter le THUMBVW.DLL le fichier et la tentative de télécharger le README.EML référencé dans lui (selon vos configurations de version et de zone IE).**Conseil** : Comme recommandé ci-dessus, utilisation NBAR de filtrer readme.eml d'être téléchargé.
- Le ver peut se propager par les lecteurs tracés. N'importe quel ordinateur infecté qui a les lecteurs réseau tracés infectera vraisemblablement tous les fichiers sur le lecteur tracé et ses sous-répertoires**Conseils :**Bloquez le Protocole TFTP (Trivial File Transfer Protocol) (port 69) de sorte que les ordinateurs infectés ne puissent pas employer le TFTP pour transférer des fichiers vers les hôtes non infectés. Assurez-vous que l'accès TFTP pour des Routeurs est encore disponible (car vous pouvez avoir besoin du chemin pour améliorer le code). Si le routeur exécute la version de logiciel 12.0 de Cisco IOS ou plus tard, vous avez toujours l'option d'utiliser le protocole FTP (FTP) de virer des images sur des Routeurs exécutant le logiciel de Cisco IOS.Bloc Netbios. Netbios ne devrait pas devoir laisser un réseau local (RÉSEAU LOCAL). Les fournisseurs de services devraient filtrer Netbios par les ports de blocage 137, 138, 139, et 445.
- Le ver se sert de sa propre engine de SMTP pour envoyer des courriers électroniques pour infecter d'autres systèmes.**Conseil** : Bloquez le port 25 (SMTP) sur les parties internes de votre réseau. Les utilisateurs qui récupèrent leur courrier électronique utilisant le Post Office Protocol (BRUIT) 3 (port 110) ou le protocole IMAP (IMAP) (port 143) n'ont pas besoin de l'accès au port 25. Permettez seulement au port 25 pour être revêtement ouvert le serveur SMTP pour le réseau. Ceci peut ne pas être faisable pour des utilisateurs utilisant Eudora, Netscape, et Outlook Express, notamment, car ils ont leur propre engine de SMTP et génèreront les connexions sortantes utilisant le port 25. Une certaine enquête pourrait devoir être appliquée aux utilisations possibles des serveurs proxys ou d'un autre mécanisme.
- Serveurs propres de Cisco CallManager/applications**Conseil** : Les utilisateurs avec des serveurs d'applications de gestionnaires d'appel et de gestionnaire d'appel dans leurs réseaux doivent faire le suivant pour arrêter se propager du virus. Ils ne doivent pas parcourir à l'ordinateur infecté du gestionnaire d'appel et également ils ne doivent partager aucun lecteurs sur le serveur de gestionnaire d'appel. Suivez les instructions données dans le virus Nimda de nettoyage du Cisco CallManager 3.x et des serveurs d'applications de CallManager pour

nettoyer le virus Nimda.

- Filtrez le virus Nimda sur le CSS 11000**Conseil** : Les utilisateurs avec CSS 11000 doivent suivre les instructions données en filtrant le virus Nimda sur CSS 11000 pour nettoyer le virus Nimda.
- Réponse Cisco Secure de système de détection d'intrusion (ID de CS) au virus Nimda**Conseil** : Les ID de CS a deux composants différents disponibles. Un est les ID gérés par le système central (HIDS) qui a un capteur d'hôte et les ID Fondé(e) sur le réseau (NIDS) qui a un capteur de réseau, qui répondent d'une manière différente au virus Nimda. Pour une explication plus détaillée et la ligne de conduite recommandée, référez-vous à comment le Cisco Secure IDS répond au virus Nimda.

Informations connexes

- Utilisant la reconnaissance Fondé(e) sur le réseau et les listes de contrôle d'accès d'application pour bloquer le ver de « 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
- Support et documentation techniques - Cisco Systems