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

Contenu

Introduction

Ce document fournit une méthode de blocage du ver « Code Red » aux points d'entrée du réseau par une Network-Based Application Recognition (NBAR) et des Listes de contrôle d'accès (ACL) au sein du logiciel Cisco IOS® sur les routeurs Cisco. Cette solution devrait être utilisée conjointement avec les correctifs recommandés pour serveurs IIS de Microsoft.

Note: Cette méthode n'est pas applicable aux routeurs de la gamme Cisco 1600.

Note: Du trafic P2P ne peut pas être dû complètement bloqué à la nature de son protocole de P2P. Ces protocoles de P2P changent dynamiquement leurs signatures pour sauter toutes les engines DPI essayant de bloquer complètement leur trafic. Par conséquent, il est recommandé pour limiter la bande passante au lieu de les bloquer complètement. Étranglez la bande passante pour ce trafic. Donnez beaucoup moins de bande passante ; cependant, permettez la connexion d'intervenir.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Les stratégies de service de la Qualité de service (QoS) utilisant les commandes de l'interface modular QoS command line interface (CLI).
- NBAR
- ACLs
- Policy-based routing

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. La configuration dans ce document a été testée sur un Cisco 3640 utilisant la version 12.2(24a) du Cisco IOS

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 utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Comment bloquer le ver « Code Red »

La première chose que vous devriez faire pour combattre un « Code Red » c'est d'appliquer le correctif fourni par Microsoft (voir les liens dans la section Méthode A: Utilisez un ACL ci-dessous). Ceci va protéger les systèmes vulnérables et supprimer le ver d'un système infecté. Cependant, le fait d'appliquer le correctif à vos serveurs ne fait qu'empêcher le ver de les infecter mais cela ne bloque pas les requêtes HTTP GET d'affecter les serveurs. Il reste l'éventualité que le serveur se fasse bombarder par une marée de tentatives d'infection.

La solution qui est détaillée dans cette information-conseil est conçue pour fonctionner conjointement avec le correctif de Microsoft pour bloquer les « Code Red » et les requêtes HTTP GET au point d'entrée du réseau.

Cette solution s'efforce de bloquer l'infection, toutefois elle ne traitera pas les problèmes causés par le cumul d'un trop grand nombre d'entrées sur le cache, d'adjacences, et d'entrées NAT/PAT, étant donné que la seule façon d'analyser le contenu d'une requête HTTP GET c'est en établissant une connexion TCP. La procédure qui suit ne vous protégera pas contre un balayage du réseau. Mais elle protégera un site d'une infection provenant d'un réseau externe ou réduira le nombre de tentatives d'infections qu'une machine doit traiter. En plus du filtrage des entrées, le filtrage des sorties empêche les clients infectés de propager leurs vers « Code Red » sur Internet.

Plates-formes prises en charge

La solution décrite dans ce document requière une fonction de marquage basée sur les classes

contenue 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 :

Plate-forme	**Logiciel Cisco IOS minimum**
7200	12.1(5)T
7100	12.1(5)T
3745	12.2(8)T
3725	12.2(8)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

Note: Vous devez activer le Cisco Express Forwarding (CEF) pour pouvoir utiliser la NBAR.

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

Plate-forme	**Logiciel Cisco IOS minimum**
7500	12.1(6)E
FlexWAN	12.1(6)E

Détectez la tentative d'infection dans les journaux Web IIS

La tentative d'infection initiale envoie une immense requête HTTP GET sur le serveur IIS cible. L'encombrement initial du « Code Red » est montré ci-dessous :

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

L'encombrement initial sur II du « Code Red » est montré ci-dessous :

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%
u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403 -
```

Remarquez comme la requête GET est constamment à la recherche d'un fichier d'extension .ida. Il s'agit là d'une chaîne commune à toutes les tentatives d'infection et peut donc être utilisée en

tant que critère de correspondance par le marquage basé sur les classes dans l'IOS. Le reste de la requête GET ne sera pas nécessairement consistant car il va simplement essayer de créer un débordement de mémoire tampon. Ceci peut être observé en comparant les deux entrées ci-dessus.

On sait à présent que la différence entre ces deux signatures est due à une nouvelle souche du ver « Code Red », appelée CodeRed.v3 ou CodeRed.C. La souche initiale du « Code Red » contient la chaîne « NNNNNNNN » dans la requête GET, alors que la nouvelle souche contient « XXXXXXXX ». Veuillez consultez l' Information conseil de Symantec pour plus de détails.

À6:24PM EDT, le 6 août 2001, nous avons enregistré un nouvel encombrement. À présent nous savons qu'il s'agit là de l'encombrement laissé derrière par le balayage eEye vulnérabilité scanner .

```
2001-08-06 22:24:02 10.30.203.202 - 10.1.1.9 80 GET /x.ida AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1 -
```

La technique qui permet de bloquer un « Code Red » fourni dans ce conseil d'information peut également servir pour bloquer ces tentatives de balayage simplement en renforçant la définition de la table des caractères, comme indiqué dans la section suivante.

Marquez les tentatives de piratage « Code Red » en utilisant une fonction de marquage de classe IOS

Pour bloquer le ver « Code Red », utilisez l'une des trois méthodes décrites ci-dessous. Chacune des trois méthodes classifie le trafic malveillant en utilisant la fonction MQC du Cisco IOS. Ce trafic est alors abandonné de la manière décrite ci-dessous.

Méthode A : Utilisez un ACL

Cette méthode utilise un ACL sur l'interface de sortie pour abandonner les paquets de « Code Red » marqués. Nous allons utiliser le diagramme de réseau suivant pour illustrer les étapes contenues dans cette méthode :

Voici les étapes à suivre pour configurer cette méthode :

1. Classifiez les tentatives entrantes de piratage « Code Red » avec la fonction de marquage basée sur les classes du logiciel Cisco IOS, tel que montré ci-dessous :

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*default.ida*"
Router(config-cmap)#match protocol http url "*cmd.exe*"
Router(config-cmap)#match protocol http url "*root.exe*"
```

La table de classe indiquée ci-dessus va regarder à l'intérieur des URL HTTP et faire correspondre les chaînes spécifiées. Notez que nous avons inclus d'autres noms de fichier en plus du default.ida du « Code Red ». Vous pouvez utiliser cette technique pour bloquer des tentatives de piratage similaires, telles que le virus Sadmind, ce qui est expliqué dans les documents suivants :http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html

2. Définissez une stratégie et utilisez la commande **set** pour marquer les tentatives entrantes de piratage « Code Red » avec une table de stratégie. Ce document utilise une valeur DSCP de 1 (en décimale) car il est peu probable qu'un tout autre trafic de réseau porte cette valeur.Dans le cas présent, nous allons marquer les tentatives entrantes de piratage « Code Red » avec une carte de stratégie libellée « mark-inbound-http-hacks ».
```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```

3. Appliquez la stratégie comme une stratégie entrante sur l'interface d'entrée pour marquer les paquets de « Code Red » entrants.
```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```

4. Configurez un ACL qui corresponde à la valeur DSCP de 1, tel que définit par la stratégie de service.
```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

   Note: Les versions 12.2(11) and 12.2(11)T du logiciel Cisco IOS offrent une prise en charge du **log keyword** sur l'ACL en définissant les tables de classe à utiliser avec NBAR (CSCdv48172). Si vous utilisez une version antérieure, n'utilisez pas le **log keyword** sur l'ACL. Cette action force tous les paquets d'être gérés par commutateur au lieu d'une gestion commutateur par CEF et NBAR ne fonctionnera pas car il requière le CEF.
5. Appliquez l'ACL sortant sur l'interface de sortie connectée aux serveurs Web cibles.
```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. Vérifiez que votre solution fonctionne comme prévu. Exécutez la commande **show access-list** et assurez-vous que la valeur de « correspondance » pour l'instruction de refus va en augmentant.
```
Router#show access-list 105
Extended IP access list 105
 deny ip any any dscp 1 log (2406 matches)
 permit ip any any (731764 matches)
```
   Dans l'étape de configuration, vous pouvez également désactiver l'envoi de messages IP d'inaccessibilité avec la commande d'interface **no ip unreachable** pour éviter que le routeur ne dépense trop de ressources.Cette méthode n'est pas recommandée si vous pouvez effectuer une stratégie de routage du trafic DSCP=1 sur une valeur Null 0, comme décrit dans la section de la méthode B.

Méthode B : Utilisez le Policy-Based Routing (PBR)

Cette méthode utilise une méthode de routage basée sur la stratégie (PBR) pour bloquer les

paquets de « Code Red » marqués. Vous n'avez pas besoin d'appliquer les commandes dans cette méthode si les méthodes A ou C sont déjà configurées.

Voici les étapes à suivre pour la mise en œuvre de cette méthode :

1. Classifiez le trafic et marquez-le. Utilisez les commandes **class-map** et **policy-map** , tel que montrées dans la méthode A.
2. Utilisez la commande **service-policy** pour définir la stratégie en tant que stratégie d'entrée sur l'interface d'entrée pour marquer les paquets de « Code Red » entrants. Voir la méthode A.
3. Créez un ACL d'IP développée qui ont une correspondance sur les paquets de « Code Red » marqués.
   ```
   Router(config)#access-list 106 permit ip any any dscp 1
   ```
4. Utilisez la commande **route-map** pour établir une stratégie de routage.
   ```
   Router(config)#route-map null_policy_route 10
   Router(config-route-map)#match ip address 106
   Router(config-route-map)#set interface Null0
   ```
5. Appliquez la table route-map à l'interface d'entrée.
   ```
   Router(config)#interface serial 0/0
   Router(config-if)#ip policy route-map null_policy_route
   ```
6. Vérifiez que votre solution fonctionne comme prévu avec la commande **show access-list** . Si vous utilisez des ACL en sortie et avez activé la journalisation ACL, vous pouvez également utiliser les commandes **show log**, comme montré ci-dessous :
   ```
   Router#show access-list 106
   Extended IP access list 106
    permit ip any any dscp 1 (1506 matches)

   Router#show log
   Aug 4 13:25:20: %SEC-6-IPACCESSLOGP:
    list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
   Aug 4 13:26:32: %SEC-6-IPACCESSLOGP:
    list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
   ```
   Vous pouvez décider d'abandonner au niveau de l'interface d'entrée du routeur, plutôt que de devoir demander une ACL de sortie sur chaque interface de sortie. De nouveau, nous vous recommandons de désactiver l'envoi de messages IP d'inaccessibilité avec la commande **no ip unreachables** .

Méthode C : Utilisez une stratégie selon la classe

Cette méthode est généralement la plus extensible car elle ne dépend pas du PBR ou des ACL en sortie.

1. Classifiez le trafic en utilisant les commandes **class-map** montrées dans la méthode A.
2. Définissez une stratégie en utilisant la commande **policy-map** et utilisez la commande **police** pour spécifier une action d'abandon pour ce trafic.

```
Router(config)#policy-map drop-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#police 1000000 31250 31250
 conform-action drop exceed-action drop violate-action drop
```

3. Utilisez la commande **service-policy** pour définir la stratégie en tant que stratégie d'entrée sur l'interface d'entrée pour abandonner les paquets de « Code Red ».
```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

4. Vérifiez que votre solution fonctionne comme prévu avec la commande **show policy-map interface** . Assurez-vous que vous voyez augmenter les valeurs pour la classe et le critère de correspondance individuel.
```
Router#show policy-map interface serial 0/0

Serial0/0

  Service-policy input: drop-inbound-http-hacks

    Class-map: http-hacks (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol http url "*default.ida*"
        5 packets, 300 bytes
        5 minute rate 0 bps
      Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
        1000000 bps, 31250 limit, 31250 extended limit
        conformed 5 packets, 300 bytes; action: drop
        exceeded 0 packets, 0 bytes; action: drop
        violated 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

    Class-map: class-default (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Restrictions NBAR

Quand vous utilisez la NBAR avec les méthodes présentées dans ce document, veuillez noter que les fonctions suivantes ne sont pas prises en charge par la NBAR :

- Plus de 24 correspondances d'URL, d'Hôtes ou de type MIME, simultanément
- Mise en correspondance au delà des 400 premiers octets dans un URL
- Le trafic Non-IP
- Le multicast et autres modes de commutation non-CEF
- Des paquets fragmentés
- Requêtes HTTP persistantes canalisées
- Classification URL/HOST/MIME/ avec HTTP sécurisé
- Débits asymétriques avec état des protocoles

- Les paquets provenant de ou destinés à un routeur utilisant la NBAR

Vous ne pouvez pas configurer la NBAR sur les interfaces logiques suivantes :

- Fast EtherChannel
- Interfaces utilisant le tunneling ou le cryptage
- VLAN
- Interfaces de numéroteur
- Multilink PPP

Note: La NBAR est configurable sur des VLAN depuis la version 12.1(13)E du Cisco IOS, mais n'est prise en charge uniquement qu'au niveau du chemin de commutation du logiciel.

Puisque la NBAR ne peut être utilisée pour classifier le trafic de sortie sur une liaison WAN où l'on utilise le tunneling ou le cryptage, vous devrez plutôt l'appliquer sur les autres interfaces du routeur, tel que l'interface LAN, pour effectuer une classification des entrées avant que le trafic de sortie ne soit commuté vers la liaison WAN.

Pour plus d'informations NBAR, voyez les liens dans les informations relatives