Stratégies de protection contre les attaques par déni de service distribuées

Contenu

Introduction

Ce livre blanc contient les informations afin de vous aider à comprendre comment des attaques de Distributed Denial of Service (DDoS) sont orchestrées, identifient des programmes utilisés pour faciliter des attaques DDoS, appliquent des mesures d'empêcher les attaques, les informations légales de rassemblement si vous suspectez une attaque, et se renseignent plus sur le degré de sécurité d'hôte.

Compréhension des fondements des attaques DDoS

Référez-vous à cette illustration :

Derrière un **client** est une personne qui orchestrent une attaque. **Un gestionnaire** est un hôte compromis avec une émission spéciale s'exécutant là-dessus. Chaque gestionnaire est capable de contrôler de plusieurs agents. **Un agent** est un hôte compromis qui lance une émission spéciale. Chaque agent est responsable de générer un flot des paquets qui est orienté sur la victime destinée.

Des attaquants ont été connus pour employer ces quatre programmes pour lancer des attaques DDoS :

1. Trinoo
2. TFN
3. TFN2K
4. Stacheldraht

Afin de faciliter DDoS, les attaquants doivent avoir des plusieurs centaines à plusieurs milliers d'hôtes compromis. Les hôtes sont habituellement Linux et EXPOSENT AU SOLEIL des ordinateurs ; mais, les outils peuvent être aussi bien mis en communication à d'autres Plateformes. Le processus de compromettre un hôte et d'installer l'outil est automatisé. Le processus peut être divisé en ces étapes, dans lesquelles les attaquants :

1. Initiez une phase de balayage l'où un grand nombre d'hôtes (sur l'ordre de 100,000 ou de plus) sont sondés pour une vulnérabilité connue.
2. Compromettez les hôtes vulnérables pour accéder.
3. Installez l'outil sur chaque hôte.
4. Utilisez les hôtes compromis pour d'autres lecture et compromissions.

Puisqu'un traitement automatisé est utilisé, les attaquants peuvent compromettre et installer l'outil sur un seul hôte dedans au-dessous de cinq secondes. En d'autres termes, plusieurs milliers d'hôtes peuvent être compromis dedans sous une heure.

Caractéristiques des programmes communs utilisés pour faciliter des attaques

Ce sont des programmes communs que l'utilisation de pirates informatiques afin de faciliter a distribué le déni de service des attaques :

- TrinooLa transmission entre les clients, les gestionnaires et les agents utilisent ces ports :`1524 tcp`
  `27665 tcp`
  `27444 udp`
  `31335 udp`**Remarque:** Les ports répertoriés ci-dessus sont les ports *par défaut* pour cet outil. Utilisez ces ports pour l'orientation et l'exemple seulement, parce que les numéros de port peuvent facilement être changés.
- TFNLa transmission entre les clients, les gestionnaires et les agents utilisent des paquets de réponse d'écho d'ÉCHO d'ICMP et d'ICMP.
- StacheldrahtLa transmission entre les clients, les gestionnaires et les agents utilisent ces ports :`16660 tcp`
  `65000 tcp`
  `ICMP ECHO`
  `ICMP ECHO REPLY`**Remarque:** Les ports précédemment répertoriés sont les ports par défaut pour cet outil. Utilisez ces ports pour l'orientation et l'exemple seulement, parce que les numéros de port peuvent facilement être changés.
- TFN2KLa transmission entre les clients, les gestionnaires et les agents n'utilise aucun port spécifique, par exemple, elle peut être fournie le délai d'exécution ou elle est choisie aléatoirement par un programme, mais est une combinaison d'UDP, d'ICMP et de paquets TCP.Pour une analyse détaillée des programmes de DDoS, lisez ces articles.

Remarque: Theaw lie le point aux sites Web externes non mis à jour par Cisco Systems.

L'outil d'attaque de déni de service distribué du « trinoo » du projet DOS

L'outil d'attaque de déni de service distribué « de réseau d'inondation de tribu »

L'outil d'attaque de déni de service distribué de « stacheldraht »

Les informations complémentaires concernant des outils de DDoS et leurs variantes peuvent être trouvées à l'index du site Web de tempête de paquets des outils distribués d'attaque .

Prévention

Ce sont des méthodes suggérées pour empêcher des attaques de déni de service distribué.

1. Utilisez la commande d'interface d'ip verify unicast reverse-path sur l'interface d'entrée sur le routeur à l'extrémité en amont de la connexion.Cette caractéristique examine chaque paquet reçu comme entrée sur cette interface. Si l'adresse IP source n'a pas une artère dans les tables CEF qui redésigne la même interface sur laquelle le paquet est arrivé, le routeur relâche le paquet.L'effet d'Unicast RPF est qu'il arrête les attaques smurf (et d'autres attaques qui dépendent de l'adresse IP source charriant) au BRUIT de l'ISP (bail et connexion à distance). Ceci protège votre réseau et clients, aussi bien que le reste de l'Internet. Pour utiliser l'unicast RPF, l'enable « commutation de CEF » ou « CEF a distribué la commutation » dans le routeur. Il n'y a aucun besoin de configurer l'interface d'entrée pour la commutation de CEF. Tant que le CEF s'exécute sur le routeur, des interfaces individuelles peuvent être configurées avec d'autres modes de commutation. Le RPF est une fonction de côté entrée qui a activé sur une interface ou une sous-interface et traite des paquets reçus par le routeur.Il est très important que le CEF soit activé dans le routeur. Le RPF ne fonctionne pas sans CEF. Unicast RPF n'est pas pris en charge dans 11.2 ou 11.3 images quelconques. Unicast RPF est inclus en 12.0 sur les Plateformes qui prennent en charge le CEF, qui inclut l'AS5800. Par conséquent, l'unicast RFP peut être configuré sur les interfaces commutées PSTN/ISDN sur l'AS5800.
2. Filtrez tout l'espace d'adressage RFC 1918 utilisant le Listes de contrôle d'accès (ACL).Référez-vous à cet exemple :
```
access-list 101 deny ip 10.0.0.0    0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0  0.15.255.255 any
access-list 101 permit ip any any

interface xy
   ip access-group 101 in
```
Une autre source d'informations sur l'espace spécial d'ipv4 addres d'utilisation qui peut être filtré est le projet soumis à l'IETF (maintenant expiré) « documentant les blocs spéciaux d'ipv4 addres d'utilisation qui ont été inscrits à l'IANA . »
3. Appliquez le d'entrée et le de sortie filtrant (voir le RFC-2267) utilisant ACLs.Référez-vous à cet exemple : `{ ISP Core } -- ISP Edge Router -- Customer Edge Router -- { Customer network }`Le routeur de périphérie ISP devrait seulement recevoir le trafic avec des adresses sources appartenant au réseau client. Le réseau client devrait seulement recevoir le trafic avec des adresses sources autres que le bloc de réseau client. C'est un ACL d'échantillon pour un routeur de périphérie ISP :
```
access-list 190 permit ip {customer network} {customer network mask} any
access-list 190 deny ip any any [log]

interface {ingress interface} {interface #}
ip access-group 190 in
```
C'est un ACL d'échantillon pour un routeur de Customer Edge :
```
access-list 187 deny ip {customer network} {customer network mask} any
access-list 187 permit ip any any

access-list 188 permit ip {customer network} {customer network mask} any
access-list 188 deny ip any any

interface {egress interface} {interface #}
ip access-group 187 in
ip access-group 188 out
```
Si vous pouvez activer le Technologie Cisco Express Forwarding (CEF), la longueur sur l'ACLs peut être sensiblement réduite et augmenter ainsi la représentation en activant le Reverse Path Forwarding d'unicast. Afin de prendre en charge le Reverse Path Forwarding d'unicast, vous devez seulement pouvoir activer le CEF sur le routeur dans son ensemble ; l'interface sur laquelle la caractéristique est activée n'a pas besoin d'être une interface commutée par CEF.

4. CAR d'utilisation aux paquets d'ICMP de raté limit.Référez-vous à cet exemple :`interface xy rate-limit output access-group 2020 3000000 512000 786000 conform-action transmit exceed-action drop access-list 2020 permit icmp any any echo-reply`
5. Configurez la limitation de débit pour des paquets de synchronisation.Référez-vous à cet exemple :
```
access-list 152 permit tcp any host eq www
access-list 153 permit tcp any host eq www established

interface {int}
rate-limit output access-group 153 45000000 100000 100000
conform-action transmit exceed-action drop
 rate-limit output access-group 152 1000000 100000 100000
conform-action transmit exceed-action drop
```
Dans l'exemple précédent, remplacez :**45000000** avec la bande passante de liaison maximale**1000000** avec une valeur qui est entre 50% et 30% du taux d'inondation de synchronisation*éclatez la normale* et *éclatez les* débits *maximum* avec des valeurs précisesNotez que si vous placez le débit de rafales plus grand que 30%, beaucoup de synchronisations légitimes peuvent être relâchées. Afin d'avoir une idée d'où placer le débit de rafales, employez la commande de **show interfaces rate-limit** afin d'afficher les débits conformés et dépassés pour l'interface. Votre objectif est au rate-limit les synchronisations en tant que peu selon les besoins pour obtenir des choses fonctionnant de nouveau.**Avertissement :** Il est recommandé que vous la première quantité de mesure de paquets de synchronisation pendant l'état normal (avant que les attaques se produisent) et employez ces valeurs pour limiter. Passez en revue les nombres soigneusement avant que vous déployiez cette mesure.Si une attaque de synchronisation est visée contre un hôte spécifique, envisagez d'installer un module de filtrage IP sur cet hôte. Un tel module est filtre IP . Référez-vous aux exemples de filtre IP pour des détails d'implémentation.

Capturant des preuves et contacter l'application de la loi

Si possible, obtenez un échantillon du trafic d'attaque pour l'analyse postérieure (généralement connue sous le nom de « capture de paquet "). Utilisez Solaris ou un poste Linux avec assez de capacité de traitement de suivre l'écoulement des paquets. Pour obtenir une telle capture de paquet, utilisez le programme de tcpdump (disponible pour Windows, Solaris et des systèmes d'exploitation Linux) ou le programme de fureteur (disponible pour le système d'exploitation solaris seulement). C'est un exemple de base de la façon utiliser ces programmes :

```
tcpdump -i interface -s 1500 -w capture_file
  snoop -d interface -o capture_file -s 1500
```
La taille de MTU dans cet exemple est 1500 ; changez ce paramètre si le MTU est plus grand que 1500.

Si vous voulez comporter l'application de la loi et vous êtes dans les Etats-Unis, entrez en contact avec votre bureau sur site des gens du pays FBI. Plus d'informations sont disponibles au site Web national de centre de protection d'infrastructure. Si vous vous trouvez en Europe, aucun point de contact n'existe. Contactez votre organisme d'application de la loi local et demandez l'assistance.

CISCO NE PEUT PAS CONTACTER DES ORGANISMES D'APPLICATION DE LA LOI EN VOTRE NOM. L'équipe de PSIRT peut travailler avec l'application de la loi une fois que vous avez établi les contacts initiaux.

Pour le contenu général de degré de sécurité d'hôte, visitez la page Web CERT/CC.

Informations connexes

- Caractérisation et suivi des inondations de paquets à l'aide de routeurs Cisco
- Détails techniques de réduction de ver
- Amélioration de la Sécurité sur des Routeurs de Cisco
- Résolution d'incidents de sécurité des produits Cisco
- Sécurité @ Cisco
- Support et documentation techniques - Cisco Systems