Estratégias de proteção contra ataques de DDoS (Distributed Denial of Service)

Índice

Introdução

Este White Paper contém a informação a fim ajudá-lo a compreender como a recusa distribuída de ataques do serviço (DDoS) é orquestrada, reconhece os programas usados para facilitar ataques de ddis, aplica medidas impedir os ataques, informação jurídica do recolhimento se você suspeita um ataque, e aprende mais sobre a Segurança do host.

Entendendo os princípios básicos dos ataques de DDoS

Refira esta ilustração:

Por trás de um cliente há uma pessoa que organiza um ataque. Um alimentador é um host comprometido com um programa especial que está sendo executado nele. Cada alimentador é capaz de controlar agentes múltiplos. **Um agente** é um host comprometido que execute um programa especial. Cada agente é responsável para gerar um córrego dos pacotes que seja dirigido para a vítima pretendida.

Os atacantes foram sabidos para usar estes quatro programas para lançar ataques de ddis:

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

Para facilitar o DDoS, os atacantes precisam ter de várias centenas a vários milhares de hosts comprometidos. Os anfitriões são geralmente Linux e computadores do SOL; mas, as ferramentas podem ser movidas a outras Plataformas também. O processo de aceitação de um host e instalação da ferramenta é automatizado. O processo pode ser dividido nestas etapas, em que os atacantes:

1. Iniciam uma fase de varredura em que um grande número de hosts (cerca 100.000 ou mais) é verificado para detectar uma vulnerabilidade conhecida.

2. Comprometa os hosts vulneráveis para obter acesso.
3. Instale a ferramenta em cada host.
4. Use os host comprometido para uma exploração e uns acordos mais adicionais.

Porque um processo automático é usado, os atacantes podem comprometer e instalar a ferramenta em um host único dentro sob cinco segundos. Ou seja diverso mil anfitriões podem ser comprometidos dentro sob uma hora.

Características de programas comuns usados para facilitar ataques

Estes são os programas comuns que o uso dos hacker a fim facilitar distribuiu a recusa de ataques dos serviços:

- TrinooUma comunicação entre clientes, alimentadores e agentes usa estas portas:`1524 tcp`
  `27665 tcp`
  `27444 udp`
  `31335 udp`**Nota:** As portas relacionadas acima são as portas padrão desta ferramenta. Use essas portas apenas como orientação e exemplo, pois os números de porta podem ser facilmente alterados.
- TFNA comunicação entre clientes, gerenciadores e agentes utiliza pacotes ICMP ECHO e ICMP ECHO REPLY.
- StacheldrahtUma comunicação entre clientes, alimentadores e agentes usa estas portas:`16660 tcp`
  `65000 tcp`
  `ICMP ECHO`
  `ICMP ECHO REPLY`**Nota:** As portas alistadas previamente são as portas padrão para esta ferramenta. Use essas portas apenas como orientação e exemplo, pois os números de porta podem ser facilmente alterados.
- TFN2KUma comunicação entre clientes, alimentadores e agentes não usa nenhuma porta específica, por exemplo, pode ser fornecida no tempo de execução ou é escolhida aleatoriamente por um programa, mas é uma combinação de UDP, de ICMP e de pacotes de TCP.Para uma análise detalhada de programas DDoS, leia estes artigos.

Nota: Theaw liga o ponto às sites da web externo não mantidas pelo Cisco Systems.

O "trinoo" do DoS Project distribuiu uma ferramenta de ataque de recusa de serviço

O “Tribe Flood Network” distribuiu a ferramenta de ataque de recusa de serviço

A ferramenta de ataque de recusa de serviço distribuída de “stacheldraht”

A informação adicional em relação às ferramentas DDoS e às suas variações pode ser encontrada no deslocamento predeterminado do site da tempestade de pacote de informação de ferramentas de ataque distribuídas .

Prevenção

Estes são métodos sugeridos para impedir ataques de recusa de serviço distribuído.

1. Use o comando ip verify unicast reverse-path interface na interface de entrada no roteador

na extremidade ascendente da conexão.Este recurso examina cada pacote recebido como entrada daquela interface. Se o endereço IP de origem não tem uma rota nas tabelas de CEF que aponte de volta à mesma relação em que o pacote chegou, o roteador deixa cair o pacote.O efeito do unicast RPF é que para os ataques de smurf (e os outros ataques que dependem da falsificação do endereço IP de origem) no POP do ISP (aluguer e tratamento por imagens). Isso protege a rede e os clientes, além do restante da Internet. Para utilizar RPF de unicast, habilite switching de CEF ou switching distribuída de CEF no roteador. Não há necessidade de configurar a interface de entrada para switching de CEF. Desde que o CEF esteja em execução no roteador, poderão ser configuradas interfaces individuais com outros modos de switching. RPF é uma função da entrada que é ativada em uma interface ou sub-interface e opera em pacotes recebidos pelo roteador.Émuito importante para o CEF ser girado sobre no roteador. O RPF não trabalha sem CEF. O unicast RPF não é apoiado em nenhuma 11.2 ou 11.3 imagens. O unicast RPF é incluído em 12.0 nas Plataformas que apoiam o CEF, que inclui o AS5800. Dessa forma, o RFP de unicast pode ser configurado nas interfaces de discagem PSTN/ISDN no AS5800.

2. Filtre todo o espaço de endereços do RFC-1918 usando o Access Control Lists (ACLs).Refira este exemplo:
```
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
```
Um outro origem de informação sobre o espaço de endereços especial do IPv4 do uso que pode ser filtrado é o esboço de IETF (agora expirado) “que documenta os blocos de endereço especiais do IPv4 do uso que foram registrados com IANA .”
3. Aplicam o ingresso e a saída que filtram (veem o RFC-2267) usando ACL.Refira este exemplo: `{ ISP Core } -- ISP Edge Router -- Customer Edge Router -- { Customer network }`O roteador de extremidade ISP apenas deve aceitar tráfego com endereços de origem pertencentes à rede do cliente. A rede do cliente deve apenas aceitar tráfego com endereços fontes diferentes dos blocos de sua rede. Esta é uma amostra ACL para um roteador de ponta 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
```
Esta é uma amostra ACL para um roteador de ponta do cliente:
```
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
```
Se você conseguir ativar o Cisco Express Forwarding (CEF), a duração nas ACLs poderá ser substancialmente reduzida; portanto, aumente o desempenho habilitando o encaminhamento de caminho inverso unicast. A fim apoiar o Unicast Reverse Path Forwarding, você precisa somente de poder permitir o CEF no roteador no conjunto; a relação em que a característica é permitida não precisa de ser uma interface comutada CEF.
4. Use o CAR aos pacotes ICMP do limite de taxa.Refira este exemplo:
```
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. Configure a taxa limite para pacotes de SYN.Refira este exemplo:`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` No exemplo anterior, substitua:45000000 com a largura de banda máxima do enlace1000000 com um valor entre 50% e 30% da taxa de inundação do SYNtaxa de burst normal e taxa máxima de burst com valores precisosNote que se você ajusta a taxa de intermitência maior de 30%, muitos SYN legítimos podem ser deixados cair. A fim obter uma ideia de onde ajustar a taxa de intermitência, use o comando show interfaces rate-limit a fim indicar as taxas conformadas e excedidas para a relação. Seu objetivo é limitar a taxa de SYNs para o menos necessário para que as coisas funcionem novamente.**aviso:** Recomenda-se que você primeiramente mede uma quantidade de pacotes SYN durante o estado normal (antes que os ataques ocorram) e usa aqueles valores para limitar. Reveja os números com cuidado antes que você distribua esta medida.Se um ataque SYN é apontado contra um host particular, considere instalar um pacote de filtração IP nesse host. Um desses pacotes é o filtro de IP. Refira exemplos do filtro IP para detalhes de implementação.

Capturando a evidência e o contato da execução de lei

Se possível, obtenha uma amostra do tráfego do ataque para a análise traseiro (conhecida geralmente como uma “captura de pacote de informação "). Use Solaris ou uma estação de trabalho Linux com bastante potência de processamento prosseguir com o fluxo dos pacotes. Para obter tal captura de pacote de informação, use o programa do tcpdump (disponível para sistemas operacionais de Windows, de Solaris e de Linux) ou o programa da espião (disponível para o SO Solaris somente). Este é um exemplo básico de como usar aqueles programas:

```
tcpdump -i interface -s 1500 -w capture_file
  snoop -d interface -o capture_file -s 1500
```

O tamanho do MTU neste exemplo é 1500; mude este parâmetro se o MTU é maior de 1500.

Se você quer envolver a execução de lei e você está dentro do Estados Unidos, contacte seu escritório de campo local FBI. Mais informação está disponível no site do centro da proteção da infraestrutura nacional. Se você é ficado situado em Europa, nenhum ponto do contato existe. Contacte sua agência de execução de lei local e peça-ao auxílio.

CISCO NÃO PODE CONTACTAR AGÊNCIAS DE EXECUÇÃO DE LEI EM SEU NOME. A equipe Cisco PSIRT pode trabalhar com execução de lei uma vez que os contatos iniciais tenham sido feitos.

Para o material geral de segurança de host, visite o página da web CERT/CC.

Informações Relacionadas

- Caracterizando e Rastreando Inundações de Pacote com Uso de Cisco Routers
- Detalhes técnico da mitigação do worm

- Melhorando a Segurança em Cisco Routers
- Resposta de incidente de segurança de produto Cisco
- Segurança @ Cisco
- Suporte Técnico e Documentação - Cisco Systems