BGP no Bloqueio de DoS Flood

Eduardo Ascenço Reis
<eduardo@intron.com.br>
<eduardo.reis@comdominio.com.br>

<bgp@comdominio.com.br>

Agenda

- Definição da Abordagem do Trabalho
- Caracterização de Ataques DoS/DDoS
- Caracterização do Efeito de Flood
- Identificação do Evento de Ataque
- Definição do Modelo
- Bloqueio utilizando BGP Communities para Black Hole
- Bloqueio utilizando Black Hole Route-Server no ISP
- Ataque por Múltiplas Entradas
- Caso de Pontos de Troca de Tráfego (PTT/NAP)
- Abordagem Alternativa de Proteção (SinkHole)
- Estudo de Caso
- Demonstração de Bloqueio
- Pontos Extras
- Referências

Definição da Abordagem do Trabalho

Este trabalho abordará formas de tratamento do efeito de Flood ou inundação, que se caracteriza por alto tráfego de entrada em ataques de DoS (Deny of Service).

Esse efeito é um problema normalmente enfrentado por muitos provedores de serviço Internet (Provedores de Acesso, Backbone, Serviços, Operadoras, Data Centers, etc).

O foco do trabalho será na infra-estrutura lógica de rede (BackBone) das empresas afetadas por ataques desse tipo e não exatamente na parte de segurança relacionada ao DoS.

Caracterização de Ataques DoS/DDoS (1/3)

- Objetivo: indisponibilizar um serviço aberto na Internet (HTTPd, SMTPd, etc)

- Motivo: spam, concorrente (LAN house), ex-funcionário (implanta IRCd), etc

- Origem: Uma (DoS – Deny of Service) ou
  Muitas (DDoS –Distributed Deny of Service)

Caracterização de Ataques DoS/DDoS (2/3)

Endereços IP de Origem

Tipo	Característica	Observação
1	Público Real	Fácil Rastreamento
2	Privado / Loopback	Poderia ter sido bloqueado na origem (política anti-spoofing)
3	Público Forjado	Mais comum e de difícil rastreamento

Número de Endereços IP Envolvidos

Tipo	**Origem**	**Destino**
1	1	1
2	Muitos	1
3	Muitos	Muitos

Caracterização de Ataques DoS/DDoS (3/3)

Caracterização do Efeito de Flood (1/4)

Efeito Inundação (Flood) – Visão do provedor de acesso do alvo:

- Alto tráfego de entrada
- Saturação de link IP
- Comprometimento das conexões externas

Normalmente é um efeito indireto do ataque DoS (SYN Flood, UDP frag), salvo ataques contra a infraestrutura.

Tráfego do ataque ocupa o meio de transmissão prejudicando o tráfego válido de clientes (alvo e demais clientes afetados indiretamente) e do tráfego de controle (BGP).

Caracterização do Efeito de Flood (2/4)

Consequências Financeiras

- Eventual quebra de SLA com clientes
- Eventual desistência futura (descrédito no serviço)
- Consumo de banda no link IP com o UPStream ISP (franquia mínima com excedente variável baseado em 95% – o que corresponde a 36h mês).

Dependendo da frequência dos ataques, acordos de troca de tráfego podem também ser prejudicados, pois pode ocorrer uma inversão no sentido do tráfego – relação OUT/IN passando de fornecedor para consumidor de conteúdo.

Caracterização do Efeito de Flood (3/4)

Caracterização do Efeito de Flood (4/4)

OUT: Tráfego de Saída
IN: Tráfego de Entrada

Identificação do Evento de Ataque

Situação: Ataque DoS em andamento com efeito Flood

Sistema Interno de Defesa do Provedor de Acesso do Alvo

Alarmes de Segurança →

Padrão de Tráfego Suspeito
Intrusion Detection System (IDS)
(e.g. Snort)

Threshold no links de borda e Acesso do Cliente Alvo (e.g. MRTG)

Análise dos fluxos de tráfego de ataque (e.g. Cisco Netflow)

↓

Resultado: Identificado Endereço IP Alvo

Definição do Modelo (1/2)

- ISP Cliente: Fornece acesso IP ao alvo do ataque DoS
- ISP: Fornece conexão IP ao ISP cliente

Utilização em Exemplos:

Espaço de Endereçamento IP privado – RFC1918 [1]
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

ASN privados – RFC1930 [2]
64512 – 65535

Definição do Modelo (2/2)

Bloqueio com BGP Communities para Black Hole (1/6)

BGP-4 (Border Gateway Protocol 4) [3]

BGP Communities Attribute [4]
Type Code 8 - optional transitive with variable length

Cada Community tem 8 octetos e
podem ser expressos na forma **<ASN>:<VALUE>**

Well-known Communities (e.g. NO_EXPORT, NO_ADVERTISE, etc)

Communities => Identificação de Prefixo

Muito utilizado por ISP - ajuda na simplificação na administração/operação das políticas de roteamento (IPJ) [5].

BGP-4 => Sinalização Remota de Black Hole via Communities
REMOTE TRIGGERED BLACKHOLE (RTB)
MCI/UUNET [6] - (Sprint) [7].

Bloqueio com BGP Communities para Black Hole (2/6)

Bloqueio com BGP Communities para Black Hole (3/6)

Bloqueio com BGP Communities para Black Hole (4/6)

Bloqueio com BGP Communities para Black Hole (5/6)

```
!
! Exemplo de Configuração BGP para cliente
!
route-map static-to-bgp permit 10
 match tag 12345
 set community 65002:666
 set origin igp
!
! Redistribuição no BGP das rotas estáticas identificadas
! com TAG padrão
!
router bgp 65000
!
 redistribute static route-map static-to-bgp
!
! No route-map do neighbor do ISP, permitir anúncios com
! match na community 65002:666
!
! Exemplo de IP bloqueado com rota estática para Null0 e TAG
!
ip route 192.168.10.10 255.255.255.255 Null0 tag 12345
!
```

***

Adaptado dos trabalhos de Christopher Morrow e Brian (MCI/UUNET) [6] e Barry Greene (Cisco) [8]. Configuração Cisco em carácter ilustrativo. No site existe exemplo de configuração para Juniper também.

Bloqueio com BGP Communities para Black Hole (6/6)

```
!
! Exemplo de Configuração BGP para ISP
!
! Rota Estática next-hop de descerte - Test Net (192.0.2.0/24)
ip route 192.0.2.0 255.255.255.0 Null0
!
ip community-list standard black-hole-id permit 65002:666
!
ip prefix-list BGP-CIDR-cliente description CIDR ISP Cliente
ip prefix-list BGP-CIDR-cliente seq 10 permit 192.168.0.0/20 le 32
!
! Route-map de entrada com neighbor ISP cliente
! deve ter outras entradas para permitir os anúncios normais.
!
route-map BlackHole-IN permit 10
 match community black-hole-id
 match ip address prefix-list BGP-CIDR-cliente
 set ip next-hop 192.0.2.1
 set community no-export additive
!
!
router bgp 65002
!
neighbor < ISP-cliente-ip > route-map BlackHole-IN in
!
neighbor < ISP-cliente-ip > ebgp multi-hop 2
!
```

Bloqueio Utilizando Black Hole Route−Server no ISP (1/4)

Abordagem Alternativa

Sinalização de bloqueio também é trocada via BGP, porém utiliza uma segunda sessão dedicada entre o ISP cliente e o servidor de bloqueio no ISP.

O servidor de bloqueio do ISP utiliza o recurso de BGP communities para repassar a sinalização de bloqueio aos roteadores do ISP.

*** Case Global Crossing

Bloqueio Utilizando Black Hole Route−Server no ISP (2/4)

Bloqueio Utilizando Black Hole Route−Server no ISP (3/4)

Bloqueio Utilizando Black Hole Route−Server no ISP (4/4)

Ataque por Múltiplas Entradas (1/3)

Ataque por Múltiplas Entradas – 1 ISP com RTB (2/3)

Ataque por Múltiplas Entradas – Ambos ISP com RTB (3/3)

Caso de Pontos de Troca de Tráfego (PTT/NAP) – (1/3)

Acordo de Troca de Tráfego Multilateral

[*] Matrix Comutação Switch Família Ethernet

Caso de Pontos de Troca de Tráfego (PTT/NAP) – (2/3)

Acordo de Troca de Tráfego Multilateral

Ataque

(4)

Como identificar do ISP Origem ?
Como bloquear sem desligar link ?

[*}: ISP não possuem filtros Anti-spoofing

Caso de Pontos de Troca de Tráfego (PTT/NAP) – (3/3)

Acordo de Troca de Tráfego Bilateral

Por Sub-Interface (ISP)

- ✔ **Análise de Tráfego**
- ✔ **Bloqueio**

[*] Matrix Comutação Switch Família Ethernet

Abordagem Alternativa de Proteção – Sink Hole (1/4)

Alternativa (RFC–3882) [9]

O tráfego total para IP alvo é redirecionado para servidor de segurança (Sink Hole Server), que filtra o tráfego do ataque e permite o encaminhamento do tráfego normal para o host alvo.

Abordagem Alternativa de Proteção – Sink Hole (2/4)

Abordagem Alternativa de Proteção – Sink Hole (3/4)

Bloqueio Geral

Abordagem Alternativa de Proteção – Sink Hole (4/4)

Bloqueio Seletivo

Estudo de Caso (1/4)

Estudo de Caso (2/4)

Estudo de Caso (3/4)

Estudo de Caso (4/4)

Demonstração de Bloqueio

- ✔ Testes de Conectividade (ping e traceroute)
  Registro.br
  Estação da Apresentação

- ✔ Verificação de Entrada BGP
  route-server.gblx.net
  route-views.routeviews.org

Alvo: IP 200.219.219.219

```
inetnum:      200.219.192/19
asn:          AS16397
entidade:     Comdominio Soluções de Tecnologia S/A.
```

Pontos Extras

- **Bloqueio Recursivo**
  O upstream ISP poderia repassar o bloqueio (BGP communities) para os seus upstream ISPs e peers, sob o controle do ISP cliente.

- **Anti-Spoofing**
  A utilização de Filtros nos elementos concentradores de acesso e borda poderiam ajudar a minimizar os problemas de ataques.

Referências

[1] RFC 1918 – Address Allocation for Private Internets

[2] RFC 1930 – Guidelines for creation, selection, and registration of an Autonomous System (AS)

[3] RFC 1771 – A Border Gateway Protocol 4 (BGP–4)

[4] RFC 1997 – BGP Communities Attribute

[5] Cisco – IPJ – Application of BGP Communities
http://www.cisco.com/warp/public/759/ipj_6–2/ipj_6–2_bgp_communities.html

[6] MCI/UUNET – Morrow, Christopher L.
http://www.secsup.org/CustomerBlackHole/

[7] Sprint – REMOTE TRIGGERED BLACKHOLE (RTB)
http://www.sprintlink.net/policy/bgp.html

[8] NANOG – ISP Security – Real World Techniques
http://www.nanog.org/mtg–0110/greene.html

[9] RFC3882 – Configuring BGP to Block Denial–of–Service Attacks

Agradecimentos

.comDominio

Equipes de Engenharia, Operações e HOC.

Equipe de Redes.

Global Crossing®

Marco Medugno <Marco.Medugno@globalcrossing.com>

http://www.intron.com.br/doc/gter18.bgp-bloqueio-dos-flood.ear.pdf