Brasil vs Mundo: Uma Análise Comparativa de Ataques DDoS por Reflexão

Tiago Heinrich e *Rafael R. Obelheiro*

Programa de Pós-Graduação em Computação Aplicada
Universidade do Estado de Santa Catarina – Joinville

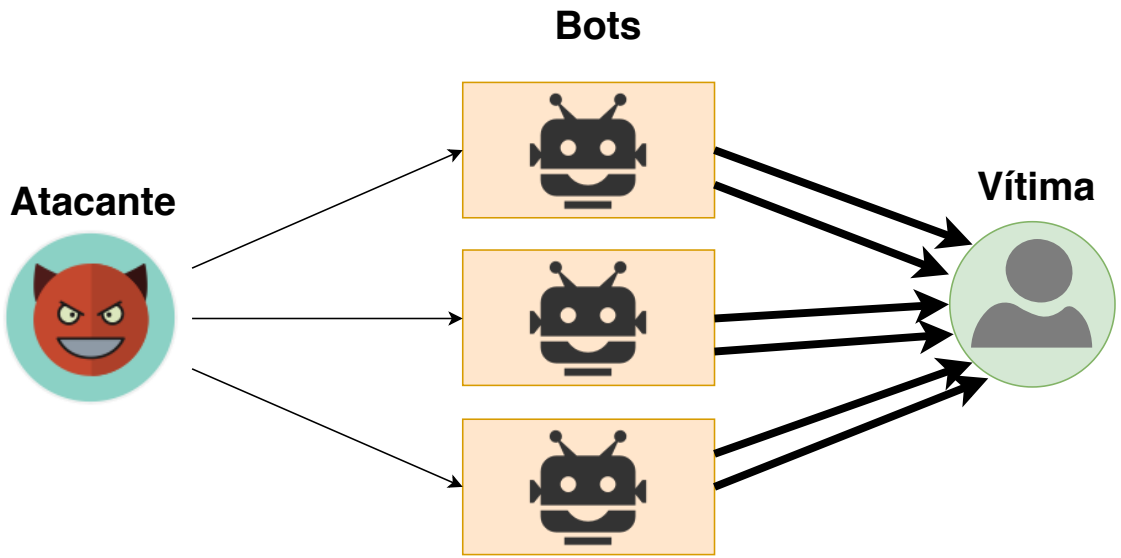
SBSeg 2019

São Paulo, 4 de setembro de 2019

Roteiro

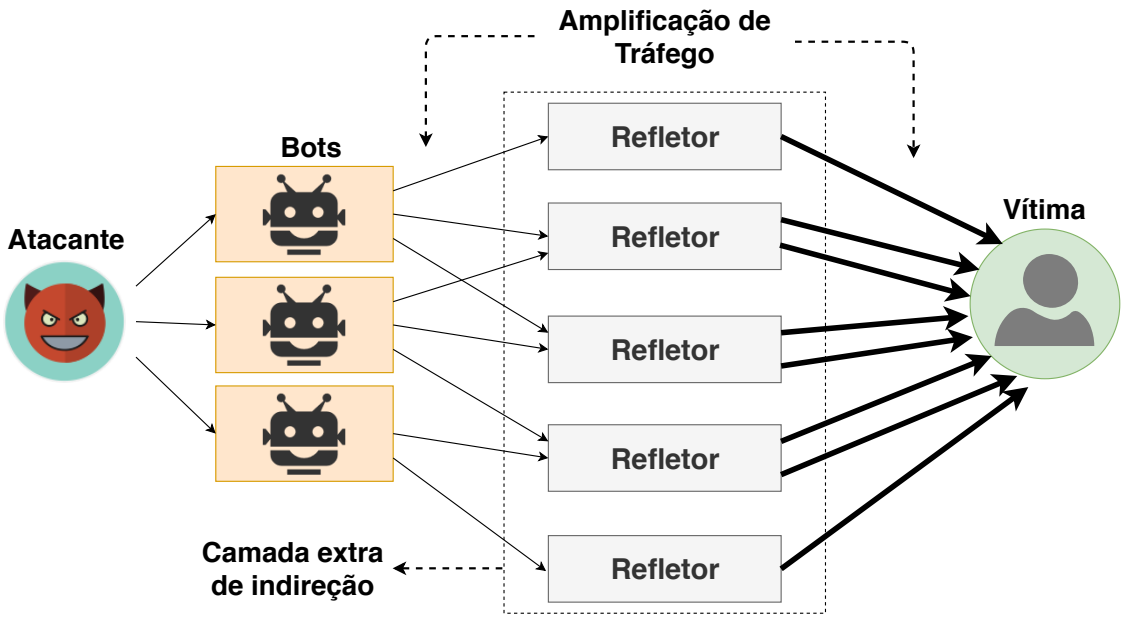
Introdução

- Ataques DDoS têm sido vistos na Internet há quase 25 anos
- O ataque consiste no envio coordenado de tráfego com o objetivo de deixar sistemas e redes indisponíveis para seus usuários legítimos
  - provocam disrupção de serviços e prejuízos financeiros



Ataques DDoS por reflexão (DRDoS)

- Um tipo popular de DDoS são os ataques por reflexão (DRDoS)
  - tráfego de ataque usa IP spoofing para que as respostas sejam refletidas para a vítima
- Vários protocolos pode ser usados, especialmente UDP
- Ataques DRDoS oferecem uma camada extra de indireção e amplificação de tráfego



Incidência de ataques DRDoS

- Cerca de 70% dos ataques DDoS usam refletores[1]
- Sobre o Brasil há poucos dados
  - 2018: 70+% das 158,4 k notificações de DoS envolviam DRDoS[2]
  - 2018.1: ataques usando UDP e amplificação DNS responderam por 50% da banda DDoS[3]
  - 2019: CERT.br notifica uma média de 343 k refletores abertos por mês (diferentes protocolos)

[1] `https://ddosmon.net/insight/`

[2] `https://www.cert.br/stats/incidentes/2018-jan-dec/analise.html`

[3] Arbor, `https://bit.ly/2EKEElw`

Tendências recentes em ataques DRDoS

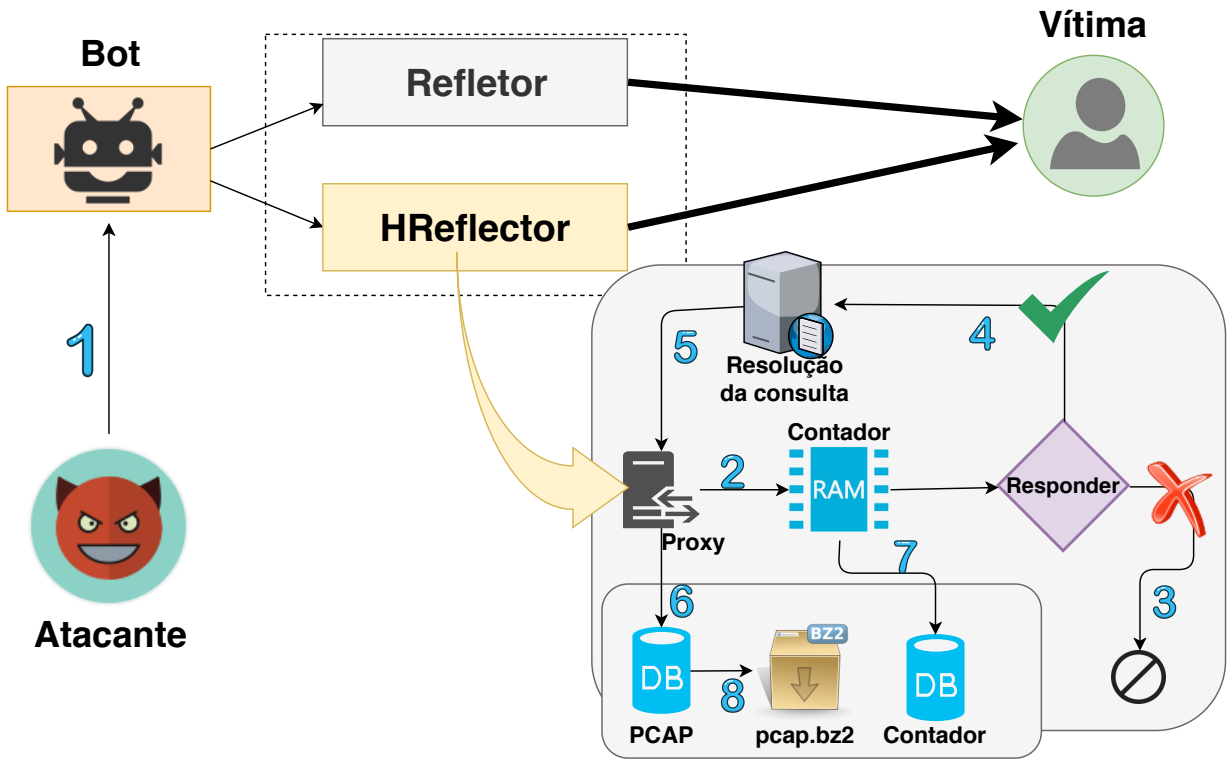
- **Ataques multiprotocolo**: vários protocolos usados simultaneamente contra uma mesma vítima
- **Ataques de carpet bombing**: visam múltiplos endereços de um sub-rede em vez de um endereço único
  - objetivo é saturar a rede, dificultando detecção/mitigação

Objetivo e contribuições

- **Objetivo**: analisar ataques DRDoS com base em dados coletados por um honeypot
  - focar em vítimas brasileiras, comparando-as com ataques a outros países
  - investigar ataques multiprotocolo e carpet bombing
- **Contribuições**
  - arquitetura de honeypot que emula refletores para 7 protocolos
  - análise de 190 dias de tráfego DRDoS coletado pelo honeypot, com 4,1 B de requisições e 25 k vítimas
  - caracterização de ataques carpet bombing observados em nosso honeypot

Arquitetura do HReflector

- Honeypot projetado especificamente para ser usado como refletor em ataques DRDoS
- Suporte a múltiplos protocolos
  - emulação: Chargen, NTP, QOTD, SSDP, Steam
  - proxy: DNS e Memcached



Mecanismos de contenção

- Limite diário de requisições por IP de origem: reduz o tráfego enviado pelo HReflector quando usado como refletor
  - requisições excedentes são registradas, mas não respondidas
  - limite fixado em 5 requisições/dia por IP
- Blacklist de endereços IP: suprime respostas a varreduras por refletores abertos
  - compilada de diversas fontes na Internet + notificações recebidas

Implementação e coleta de dados

- HReflector foi implementado em Python/Linux, usando SQLite para o BD, Unbound e Memcached para os servidores locais
  - AMD Phenom II (4 núcleos), 4 GB RAM, Ethernet 100 Mbps
- Implantado na rede da UDESC, com IP globalmente roteável exposto diretamente à Internet (sem FW/NAT)
- Coleta de dados iniciada no final de setembro/2018, com breves interrupções por problemas de infraestrutura (elétrica/rede)

Definições usadas na análise

- É preciso identificar **ataques** e **vítimas**, mas. . .
  - não há consenso na literatura sobre definição de ataque DRDoS (do ponto de observação de um refletor)
    - ★ adaptou-se definição usada em trabalhos anteriores do grupo (estabelecida empiricamente)
  - ataques de carpet bombing complicam a noção de vítima
    - ★ endereço IP único ou sub-rede?
    - ★ difícil precisar a sub-rede a que pertence um endereço IP

Ataque DRDoS

Um ataque DRDoS é formado por um conjunto com no mínimo 5 requisições com endereço IP de origem referente a uma mesma vítima e com espaçamento máximo de 60 segundos entre requisições consecutivas

Vítima

Uma vítima é definida pelos três primeiros octetos do endereço IP de origem (i.e., bloco CIDR /24)

- Geolocalização das vítimas estabelecida usando dados do WHOIS
  - possível imprecisão para clientes de nuvens e CDNs

Estatísticas gerais

Grupo de ataque	requisições	%	vítimas	%	ataques	%
Brasil	47.124.818	1,1	864	3,4	2.364	1,1
Mundo	4.077.014.253	98,8	24.316	96,5	201.943	98,8
Total	**4.124.139.071**	100,0	**25.180**	100,0	**204.307**	100,0

- Volume total de tráfego processado: 65,2 GB
- Total de 4,1 B requisições processadas (média de 21,7 M/dia)
  - apenas 0,035% foram respondidas pelo honeypot
- Mais de 204 k ataques DRDoS observados
- 181 k endereços distintos $\rightarrow$ 25,2 k vítimas (/24)
  - vítimas em 186 países
    - ★ concentradas nos EUA (46,4%) e China (6,6%)
- Brasil teve 1,1% de requisições e ataques mas 3,4% de vítimas
  - menos vítimas que sofreram múltiplos ataques

Requisições e ataques por protocolo

Requisições

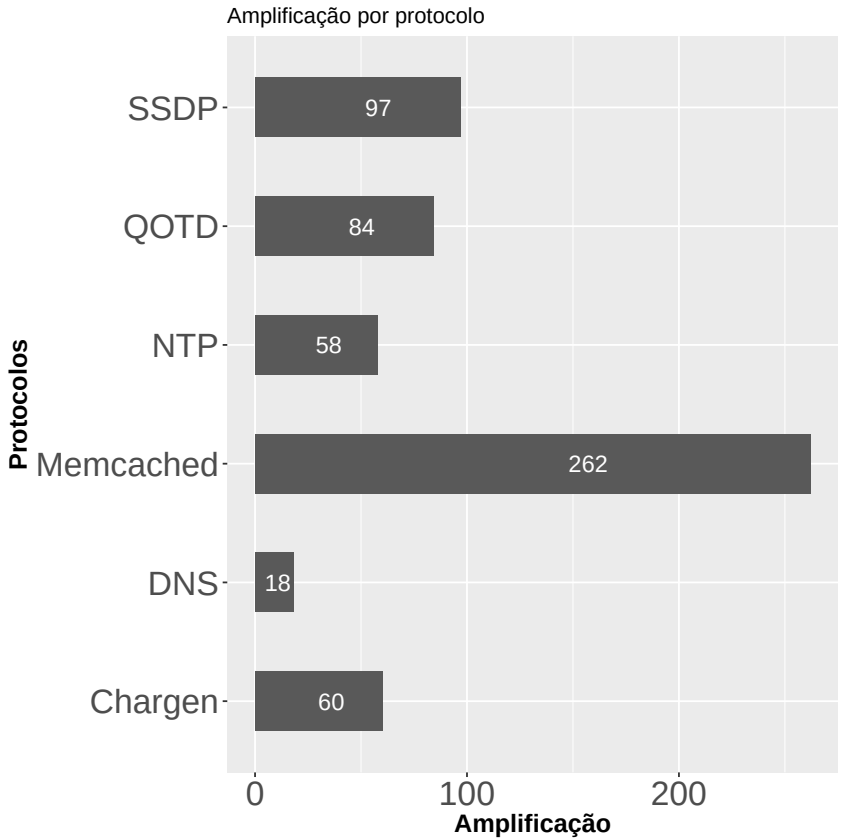
Protocolo	Brasil %	Mundo %
Chargen	90,6	83,1
Memcached	5,1	13,7
DNS	2,5	1,9
SSDP	1,6	0,9
NTP	0,08	0,08
QOTD	0,0	0,05
Steam	0,0	0,0

Ataques

Protocolo	Brasil %	Mundo %
Memcached	4,6	47,1
Chargen	45,5	46,5
DNS	17,8	3,4
SSDP	31,4	2,5
NTP	0,5	0,34
QOTD	0,0	0,091
Steam	0,0	0,006

- Brasil
  - requisições: Chargen+Memcached (95,7%)
  - ataques: Chargen+DNS+SSDP (94,7%)
  - DNS+SSDP somam 49,2% dos ataques mas 4,1% de requisições
    - ★ muitos ataques, mas de pouca intensidade
- Resto do mundo
  - requisições: Chargen+Memcached (96,8%)
  - ataques: Memcached+Chargen (93,6%)
  - Memcached: 47,1% dos ataques mas 13,7% de requisições
- Ataques usando Memcached são menos comuns no Brasil
- Baixa incidência de NTP
  - estudos anteriores reportam 30–50% do tráfego DRDoS

Fatores de amplificação



- Chargen, Memcached, SSDP com boa amplificação (60–262)
- DNS menor que o reportado na literatura (29–96)

Duração e intensidade dos ataques

Duração

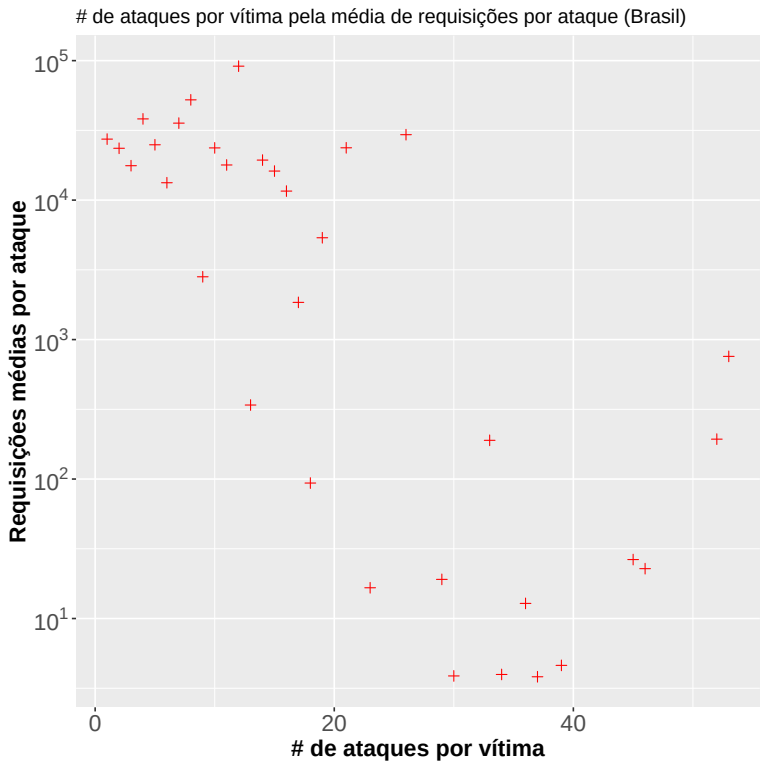
	Brasil	Mundo
média	1490 s	560 s
máxima	39,1 h	114,2 h
ataques $>$ 1 h	8,9%	3,5%

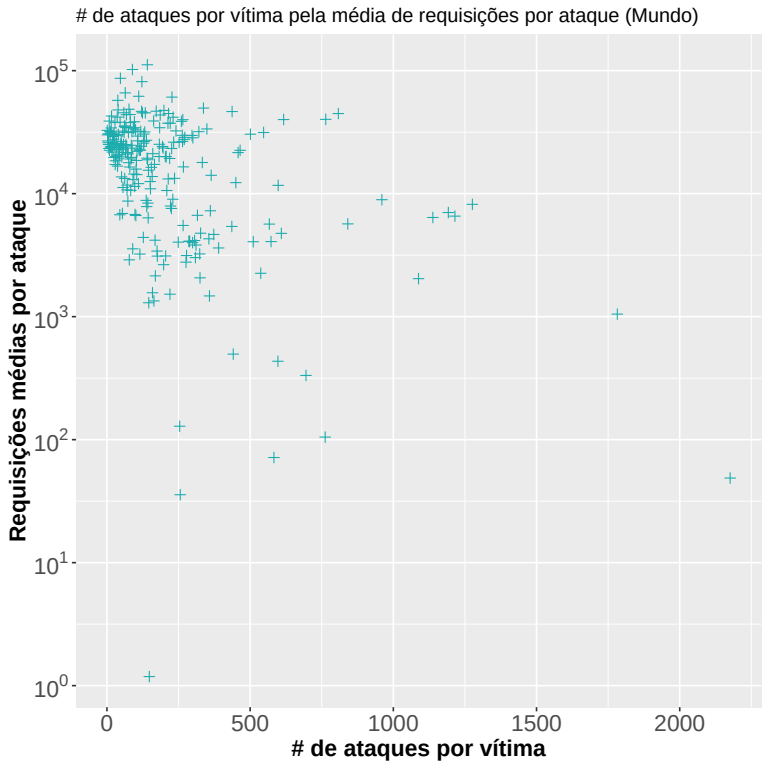
Requisições/ataque

	Brasil	Mundo
média	19,9 k	20,2 k
máximo	1,1 M	33,0 M
ataques $>$ 100 k req	0,05%	3,8%

- Ataques contra o Brasil foram em geral mais longos do que contra o resto do mundo
  - a partir do 17° percentil, ataques no Brasil têm maior duração
- Resto do mundo teve maior proporção de ataques com grande volume de requisições

Ataques/vítima vs requisições/ataque

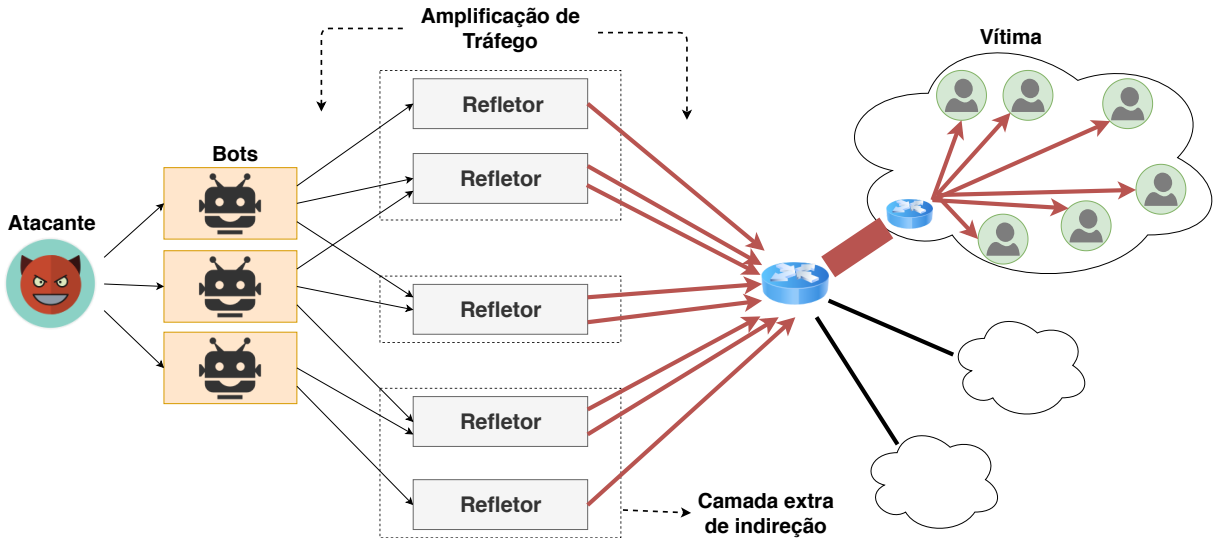




- Vítimas que sofreram menos ataques receberam ataques com mais requisições
- Vítimas com apenas 1 ataque: 68% no Brasil, 50% no resto do mundo
- Máx ataques por vítima: 53 no Brasil, 2,1 k no resto do mundo

Ataques de carpet bombing (CB)

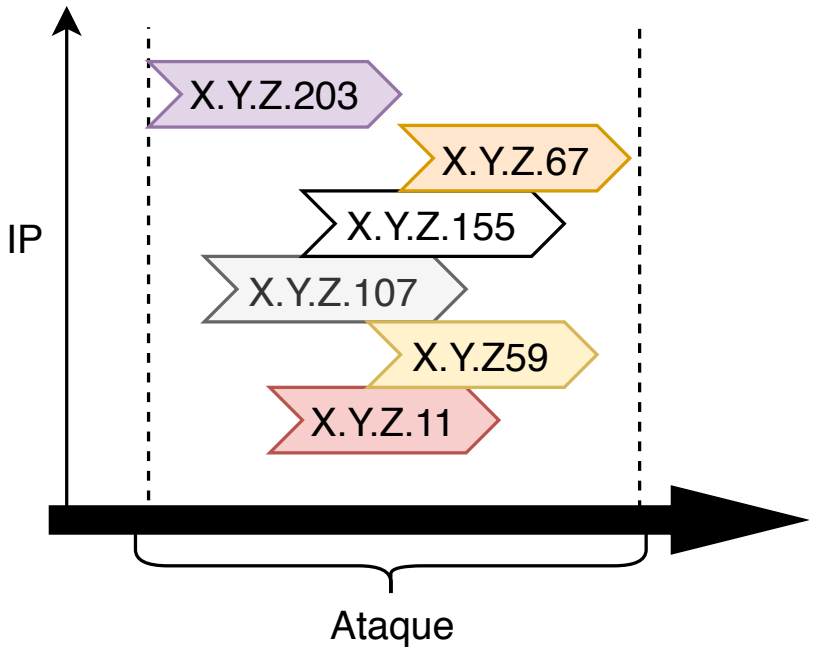
- Direcionam o tráfego para múltiplos endereços IP na mesma sub-rede, em vez de para um único endereço



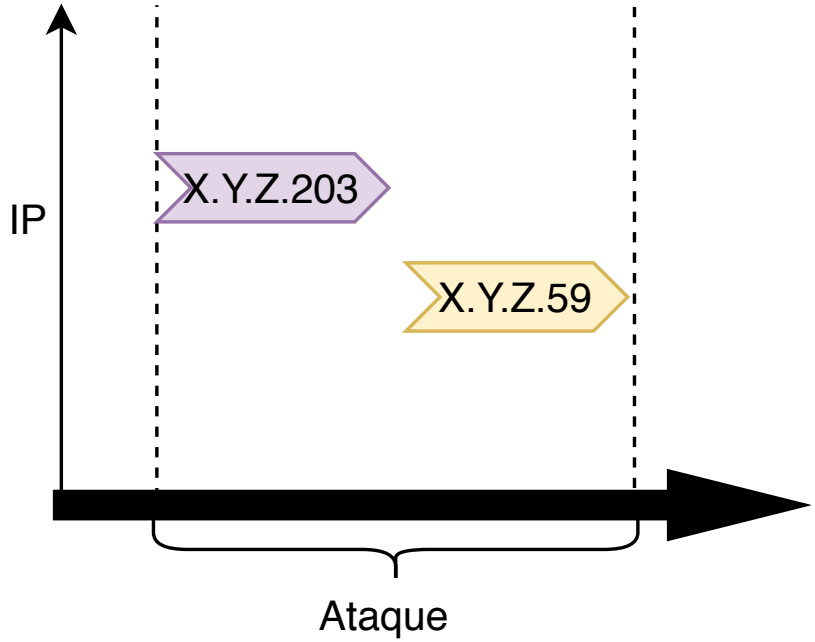
- Saturam os enlaces de acesso das vítimas desejadas
- Dificultam detecção e mitigação do ataque
  - detecção: identificar tráfego anômalo em sub-redes inteiras
  - mitigação: desviar o tráfego das sub-redes completas para um serviço anti-DDoS

Ataques CB observados no HReflector

- 4,8 k ataques CB
  - apenas 0,05% exploraram múltiplos protocolos
- Variantes típicas



endereços IP concomitantes



endereços IP consecutivos

Duração e intensidade dos ataques CB

Duração

	Brasil	Mundo
média	52 min	55 min
máxima	39,1 h	79,7 h
75° percentil	17 min	30 min

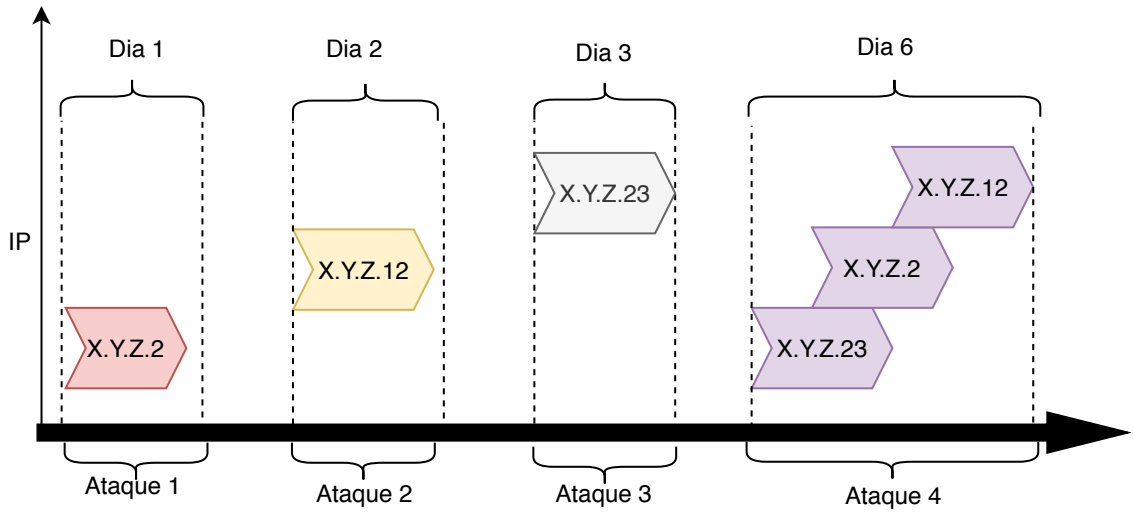
Requisições/ataque

	Brasil	Mundo
média	3,7 k	76,0 k
máximo	200,0 k	8,5 M

- Durações de ataques CB têm distribuições similares após o 10° percentil
- Ataques CB contra vítimas brasileiras tiveram volume bastante inferior de requisições
- Ataques exploraram frações pequenas dos blocos /24
  - $>$ 50% do bloco: 9,2% (BR), 1,5% (mundo)
  - $\leq$ 30% do bloco: 90,0% (BR), 98,3% (mundo)

Ataques CB com antecedentes

- Ataque contra múltiplos endereços IP ocorre depois de alguns dias em que são observados ataques a um único endereço IP da sub-rede em cada dia
  - considerados antecedentes do CB porque têm características semelhantes
    - ★ protocolo (Chargen), duração, número de requisições
- 18,9% dos ataques CB observados tiveram antecedentes
- Ataques antecedentes (média): 1 minuto, 13,5 k requisições
- Ataques finais (média): 4 minutos, 7,8 k requisições (por endereço IP)



Conclusão

- Entender o funcionamento de ataques DRDoS é importante para ajudar na busca de mecanismos para detectar, mitigar e prevenir esse tipo de ataque
- Análise comparativa de ataques DRDoS contra vítimas no Brasil e no resto do mundo
  - ataques no Brasil estão atrás, em termos de intensidade e de mix de protocolos, aos observados contra outras vítimas
    - ★ situação pode piorar se os ataques/atacantes evoluírem
- Perspectivas futuras
  - prosseguir com a coleta de dados para poder analisar a evolução dos ataques
  - buscar parceiros de pesquisa para aumentar o número de honeypots e ampliar o escopo de análise

Brasil vs Mundo: Uma Análise Comparativa de Ataques DDoS por Reflexão

Tiago Heinrich e *Rafael R. Obelheiro*

Programa de Pós-Graduação em Computação Aplicada
Universidade do Estado de Santa Catarina – Joinville

SBSeg 2019

São Paulo, 4 de setembro de 2019