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

Tiago Heinrich[1], **Rafael R. Obelheiro**[1]

[1]Programa de Pós-Graduação em Computação Aplicada (PPGCA)
Universidade do Estado de Santa Catarina (UDESC)
Centro de Ciências Tecnológicas – 89.219-710 – Joinville – SC – Brasil

heinrichtx@gmail.com, rafael.obelheiro@udesc.br

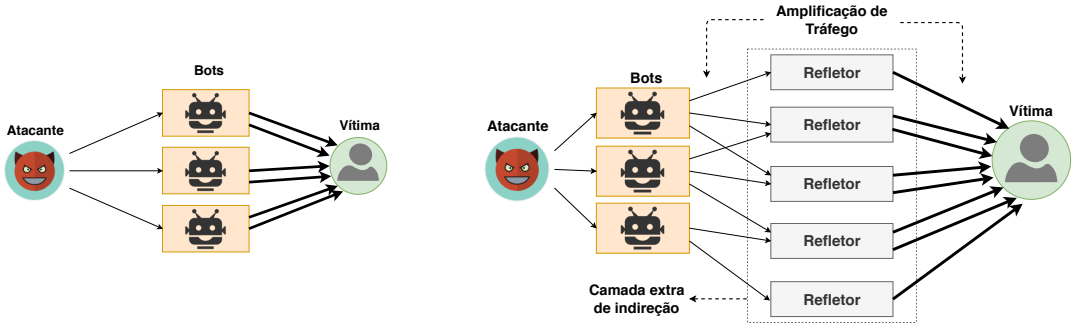
Abstract. *Distributed reflection denial of services (DRDoS) attacks are widespread on the Internet. These attacks offer several advantages to attackers, being very effective in crippling down individual hosts or even entire subnets. To detect, mitigate, and prevent DRDoS attacks, it is important to understand how they work, and what are their traffic characteristics. This paper presents a comparative analysis of DRDoS attacks against victims in Brazil and in the rest of the world. We analyze 190 days of traffic collected using a honeypot, with over 204 k DRDoS attacks. We describe and contrast several characteristics of DRDoS traffic, including an in-depth analysis of carpet bombing attacks. We conclude that attacks against Brazilian victims are less intense and sophisticated than attacks against other victims, which may indicate that the local scene may worsen if attackers improve their tactics and tools.*

Resumo. *Ataques distribuídos de negação de serviço por reflexão (distributed reflection denial of service, DRDoS) estão disseminados na Internet. Esses ataques oferecem diversas vantagens para os atacantes, sendo bastante eficazes em provocar a indisponibilidade de hosts individuais ou mesmo sub-redes inteiras. Para detectar, mitigar e prevenir ataques DRDoS, é importante entender como eles funcionam, e quais são suas características de tráfego. Este artigo apresenta uma análise comparativa de ataques DRDoS contra vítimas no Brasil e no resto do mundo. São analisados 190 dias de tráfego coletado usando um honeypot, contando com mais de 204 k ataques DRDoS. Várias características de tráfego DRDoS são descritas e comparadas, incluindo uma análise aprofundada de ataques de carpet bombing. É possível concluir que os ataques contra vítimas brasileiras são menos intensos e sofisticados que os ataques contra o restante do mundo, o que pode indicar que o cenário local pode piorar se os atacantes aperfeiçoarem suas táticas e ferramentas.*

1. Introdução

Ataques distribuídos de negação de serviço (*distributed denial of service*, DDoS) têm sido vistos na Internet há quase 25 anos [Mansfield-Devine 2015]. Nesses ataques, um conjunto de máquinas, tipicamente *bots*, envia tráfego para a vítima de maneira coordenada (Fig. 1(a)). O volume de dados leva ao esgotamento dos recursos do sistema e/ou da rede na vítima, causando sua indisponibilidade e prejudicando por tabela seus clientes legítimos [Nazario 2008].

Uma variante de ataques DDoS são os ataques distribuídos de negação de serviço por reflexão (*distributed reflection denial of service*, DRDoS), em que o tráfego é repassado a sistemas intermediários conhecidos como refletores [Paxson 2001]. Ataques DRDoS dificultam a descoberta dos atacantes devido a uma camada extra de indireção, além de fornecer amplificação de tráfego (Fig. 1(b)). Além disso, ataques DRDoS podem explorar vários protocolos, especialmente os baseados em UDP, com um grande número de servidores de Internet vulneráveis e/ou mal configurados que podem ser usados como refletores [Rossow 2014]. Em abril de 2019, o CERT.br enviou notificações sobre mais de 320 k refletores abertos apenas no Brasil [CERT.br 2019a].



(a) DDoS (b) DRDoS

Figura 1. Ataques DDoS e DRDoS

Os benefícios proporcionados aos atacantes ajudam a explicar a incidência significativa de tráfego DRDoS na Internet. Um relatório recente [NETSCOUT 2019] mostra um crescimento de 9% nos ataques DRDoS entre o segundo semestre de 2017 e o mesmo período de 2018, e estatísticas de abril de 2019 indicam que aproximadamente 70% dos ataques DDoS usam refletores [DDoSMon 2019]. Dados sobre o Brasil são mais escassos: o CERT.br relata ter recebido em 2018 158,4 k notificações de ataques de negação de serviço, sendo mais de 70% dos casos envolvendo protocolos usados em DRDoS [CERT.br 2019b], e a Arbor Networks aponta que, no primeiro semestre de 2018, ataques usando UDP e amplificação DNS respondem por cerca de 50% da banda consumida com ataques DDoS contra alvos brasileiros [Arbor 2018].

Os ataques DRDoS têm passado por evoluções, como ataques multiprotocolo e de *carpet bombing* [NETSCOUT 2019]. No primeiro caso, os ataques usam simultaneamente vários protocolos contra uma mesma vítima. No segundo caso, em vez do ataque visar um endereço IP específico, ele visa todos os endereços da sub-rede à qual pertence o alvo. Com isso, a rede e/ou os roteadores de borda da vítima ficam saturados com tráfego, e o ataque torna-se mais difícil de detectar e mitigar.

Embora a literatura registre diversos trabalhos que realizam a caracterização de tráfego DRDoS e das vítimas desses ataques [Krämer et al. 2015, Noroozian et al. 2016, Heinrich et al. 2017, Jonker et al. 2017, Thomas et al. 2017], é possível apontar duas lacunas. Uma delas é a falta de análises específicas sobre ataques e vítimas no Brasil, e como o cenário local se compara ao restante do mundo. A segunda lacuna reside na limitada discussão sobre as características mais recentes de ataques DRDoS, como *carpet bombing* e uso de múltiplos protocolos.

Este trabalho visa a suprir estas lacunas, analisando ataques DRDoS contra vítimas brasileiras e comparando-os com ataques a outros países. A análise é baseada em dados coletados usando o HReflector, um *honeypot* que emula refletores para vários protocolos que são explorados em ataques DRDoS (Chargen, DNS, NTP, Memcached, QOTD, SSDP e Steam), o qual foi desenvolvido no contexto deste trabalho. As principais contribuições do artigo são as seguintes:

1. Uma análise de 190 dias de tráfego DRDoS coletado pelo HReflector, com um total de 4,1 B de requisições e 25 k vítimas (sendo 865 vítimas brasileiras, com 47 M de requisições), e comparamos o tráfego referente a vítimas no Brasil com vítimas no resto do mundo;
2. Caracterizamos ataques *carpet bombing* observados em nosso *honeypot*, incluindo um novo tipo de ataque, chamado de ataque com antecedentes.

O restante do artigo está organizado da seguinte forma. A Seção 2 discute os trabalhos relacionados. A Seção 3 descreve o *honeypot* usado para observação e coleta de tráfego. A Seção 4 apresenta a análise dos dados. A Seção 5 faz uma análise mais aprofundada sobre ataques de *carpet bombing*. A Seção 6 conclui o artigo.

2. Trabalhos Relacionados

Esta seção apresenta a revisão de trabalhos relacionados, com foco na caracterização de tráfego de ataques DRDoS e DDoS, e de suas vítimas.

[Krämer et al. 2015] introduz AmpPots, que são *honeypots* específicos para observação e coleta de tráfego de ataques DRDoS. O artigo discute algumas características de ataques observados usando AmpPots, como duração, tipos de *payloads* usados, e geolocalização das vítimas.

[Noroozian et al. 2016] analisa tráfego DRDoS coletado por oito AmpPots durante 2014–2015, com um total de seis protocols (NTP, DNS, Chargen, SSDP, QOTD, e SNMP). O trabalho caracteriza as vítimas de DRDoS, incluindo tipo de rede, geolocalização e duração dos ataques. Foi identificada uma predominância de ataques contra vítimas em redes de banda larga, com o maior grupo sendo associado a jogos *online*.

[Thomas et al. 2017] também usam dados coletados por *honeypots* para caracterizar ataques DRDoS. O trabalho considera oito protocolos (QOTD, Chargen, DNS, NTP, SSDP, SQLMon, Portmap, e mDNS), e caracteriza vários aspectos de ataques, como duração, intensidade e protocolos mais usados, mas não discute as vítimas dos ataques.

Uma caracterização de ataques de negação de serviço (não apenas DRDoS) com base em dados coletados entre 2015 e 2017 é apresentada por [Jonker et al. 2017]. Foi observado um total de 2,2 M de redes /24 que foram vítimas de ataques DoS. A caracterização abrange aspectos como geolocalização das vítimas, protocolos usados nos ataques, duração e intensidade de ataques.

[Heinrich et al. 2017] efetua uma análise de dados coletados por um *honeypot* DNS. Embora limitada a um único protocolo, são discutidas características de ataques DRDoS (intensidade, duração, fator de amplificação, *payloads* usados) e a geolocalização das vítimas.

Uma avaliação do impacto de ataques DDoS gerados por *botnets* nas vítimas é apresentada em [Welzel et al. 2014]. Foram monitorados os canais de comunicação e controle (C&C) de 14 *botnets* para descobrir os alvos de ataques, e na sequência avaliou-se a disponibilidade desses alvos, constatando-se que cerca de 2/3 deles foram severamente afetados pelos ataques.

[Wang et al. 2018] também realiza uma análise de tráfego DDoS gerado por *botnets*. Foram observados ataques realizados por 674 *botnets* contra mais de 9 k vítimas, e verificou-se que muitos alvos sofriam ataques recorrentes com periodicidade previsível, e que ataques usando múltiplas *botnets* simultaneamente estão se tornando mais frequentes.

Existem alguns trabalhos que analisam serviços que efetuam ataques DDoS mediante pagamento (*booters*) [Santanna et al. 2015, Krupp et al. 2017, Zand et al. 2017]. Estes trabalhos concentram-se nas características do tráfego gerado por esses *booters*, desconsiderando as vítimas.

Este trabalho tem dois principais diferenciais em relação à literatura. Um deles é o foco nos ataques contra alvos no Brasil, e como eles se comparam aos ataques contra alvos em outros países. Outro diferencial é a análise de características mais recentes de ataques, como o uso simultâneo de múltiplos protocolos e o emprego de *carpet bombing*.

3. HReflector, um *Honeypot* Multiprotocolo

O HReflector é um *honeypot* multiprotocolo, que atualmente suporta sete protocolos distintos: Chargen, QOTD, DNS, NTP, SSDP, Memcache, e Steam. Esse *honeypot* responde a requisições desses protocolos de modo a passar-se por um refletor aberto, e registra todas as interações realizadas.

Como os serviços disponibilizados pelo *honeypot* não são anunciados publicamente, toda interação realizada com o sistema é considerada maliciosa. Dois tipos de tráfego são esperados: (1) varreduras (*scans*) que buscam sistemas vulneráveis e refletores abertos que possam ser explorados em ataques de reflexão, e (2) ataques DRDoS propriamente ditos. Para permitir que o *honeypot* seja identificado como um refletor aberto durante uma varredura mas cause um impacto limitado ao ser usado em um ataque DRDoS, o HReflector responde a apenas cinco requisições para um único endereço IP por dia.

Existem ainda organizações, como [Cymru 2019, OpenNTP 2019], que realizam *scans* na Internet para localizar refletores abertos e notificar os seus responsáveis. Para evitar que o *honeypot* seja identificado nesses *scans*, o HReflector não responde a requisições originadas pelos endereços IP usados nessas varreduras.

O HReflector é similar em projeto ao AmpPot [Krämer et al. 2015], com as principais diferenças sendo em especificidades de implementação e no conjunto de protocolos suportados. O HReflector faz *proxy* de requisições DNS e Memcached para servidores reais que operam na interface de *loopback* (isto é, só podem ser acessados localmente), de modo a respeitar a semântica complexa desses protocolos. Os demais protocolos são emulados pelo próprio *honeypot*, que sintetiza respostas válidas, porém com conteúdo forjado. O HReflector é escrito em Python e executa em Linux, e foi implantado em uma máquina com processador AMD Phenom II X4 B93 (quatro núcleos), 4 GB de memória RAM e e rede Ethernet de 100 Mbps.

4. Análise de dados

A coleta de dados teve foi de um período de 190 dias, entre setembro de 2018 a abril de 2019. A coleta pelo HReflector é realizada 24/7, o sistema possui um endereço IP globalmente roteável e está exposto diretamente à Internet (isto é, não está atrás de um *firewall* ou NAT). Nesta seção, analisamos os dados coletados, descrevendo as características do tráfego observado e contrastando o tráfego referente a vítimas brasileiras com o tráfego do restante do mundo.

4.1. Visão Geral

Durante o período de coleta o HReflector recebeu 65,2 GB de tráfego, contendo um total de 4,1 B de requisições, uma média de 21,7 M de requisições por dia. Ao todo foram respondidas apenas 0,035% das requisições recebidas, em decorrência do limite de requisições aplicado no HReflector.

Para que seja possível identificar e contabilizar ataques DRDoS, é necessário ter uma definição que permita classificar um conjunto de pacotes recebidos como sendo um ataque. Infelizmente, não há consenso na literatura sobre esse ponto: [Krämer et al. 2015], [Fachkha et al. 2015], [Thomas et al. 2017] e [Heinrich et al. 2017] usam definições ligeiramente divergentes. Neste trabalho será adotada a definição de [Heinrich et al. 2017] para ataques DoS explorando o DNS, com uma adaptação mínima (o uso de "vítima" no lugar de "endereço IP de origem") para contemplar ataques de *carpet bombing*:

> *Um ataque DRDoS consiste em 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.*

Como um ataque DRDoS pode explorar múltiplos protocolos para realizar a amplificação de tráfego, requisições de diferentes protocolos serão agregadas em um único ataque se forem destinadas à mesma vítima e respeitarem o lapso temporal.

Devido à ocorrência de ataques de *carpet bombing*, uma vítima foi definida como sendo os três primeiros octetos do endereço IP de origem, ou seja, endereços IP pertencentes ao mesmo bloco CIDR /24 foram considerados como uma única vítima. Essa heurística é inevitavelmente imprecisa, podendo juntar ataques separados em um único ataque caso os alvos estejam dentro do mesmo bloco /24. O efeito dessa imprecisão é uma eventual subestimativa de ataques e vítimas, e uma superestimativa do número de requisições por ataque e do número de ataques de *carpet bombing*. Ainda assim, os dados coletados no *honeypot* sugerem uma baixa probabilidade de ocorrência de ataques independentes simultâneos contra alvos no mesmo bloco /24.

Para identificar quais vítimas de ataques são brasileiras, usou-se dados disponíveis no WHOIS: uma consulta ao WHOIS por um endereço IP retorna diversos atributos referentes ao bloco de endereços no qual esse IP se insere, dentre os quais o país. Uma limitação inerente a essa abordagem é que organizações brasileiras que utilizam provedores de nuvem ou redes de distribuição de conteúdo podem usar endereços IP atribuídos a esses provedores e que são identificados no WHOIS como pertencentes a outros países (como o país sede do provedor, por exemplo). Isso significa que pode haver ataques contra alvos brasileiros que foram classificados como pertencentes ao resto do mundo, e vice-versa. A despeito dessa limitação, os dados do WHOIS são os mais fidedignos dis-

poníveis publicamente, não sendo factível, com base apenas nos endereços IP, identificar os que porventura tenham sido classificados de forma errônea.

A Tabela 1 apresenta as estatísticas gerais para o tráfego processado pelo *honeypot*. Observou-se um total de 204 k ataques DRDoS. As frações de requisições e ataques dirigidos a alvos brasileiros são equivalentes (1,1%), com uma fração comparativamente maior de vítimas (3,4%). Isso indica que o Brasil teve menos vítimas que sofreram múltiplos ataques do que o resto do mundo.

Tabela 1. Estatisticas 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

A Tabela 2 apresenta a distribuição de protocolos de acordo com o número de requisições. O ranqueamento dos protocolos é idêntico nos dois casos, mudando apenas a porcentagem. Os dois protocolos com maior número de requisições, Chargen e Memcached, concentram 95,7% das requisições disparadas contra vítimas brasileiras e 96,8% do restante do mundo. Considerando o número de ataques, a Tabela 3 mostra novamente uma concentração: três protocolos (Chargen, DNS e SSDP) respondem por 94,7% dos ataques contra vítimas brasileiras, enquanto que 93,6% dos ataques contra o resto do mundo usam Memcached e Chargen.

Três pontos devem ser destacados aqui. O primeiro é que, considerando vítimas no Brasil, DNS e SSDP somam 49,2% dos ataques mas apenas 4,1% do volume de requisições, o que indica muitos ataques mas de pouca intensidade; algo semelhante é observado para as vítimas no resto do mundo, onde Memcached responde por 47,1% dos ataques mas apenas 13,7% das requisições. O segundo destaque está justamente nos ataques usando Memcached, que possuem menor incidência no Brasil do que no resto do mundo, possivelmente por terem sido difundidos mais recentemente [Majkowski 2018, Kottler 2018]. Por fim, chama a atenção a baixa incidência de NTP, que é um protocolo com alto potencial de amplificação [Rossow 2014, Czyz et al. 2014] e que costuma ser citado entre os mais utilizados (por exemplo, [NETSCOUT 2019] apontou que o NTP foi usado em 28,8% dos ataques DRDoS no segundo semestre de 2018, enquanto [Thomas et al. 2017] relatou seu uso em 51,7% de ataques observados entre 2014 e 2017).

O fator médio de amplificação obtido com cada protocolo é retratado na Figura 2. Memcached, que foi o protocolo mais usado contra vítimas no resto do mundo, apresentou a maior amplificação média, de 262. Chargen e SSDP, que também foram bastante usados (especialmente no Brasil), têm amplificação média de 60 ou mais. Por outro lado, o DNS, que foi o terceiro protocolo em número de ataques, teve um fator médio de amplificação de apenas 18. Referências na literatura apontam fatores maiores de amplificação para esse protocolo: [Rossow 2014] observou amplificação média de 28,7, e [Heinrich et al. 2017] reportou amplificações médias de 96,3 e 74,1 (o trabalho aborda dois conjuntos de dados).

4.2. Avaliação das vítimas

Os ataques observados pelo *honeypot* tiveram como alvo 181 k endereços IP distintos, que foram agrupados em 25.180 vítimas de acordo com seus blocos /24. Ao todo o HReflector

Tabela 2. Distribuição de requisições por protocolo

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

Tabela 3. Distribuição de ataques por protocolo

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

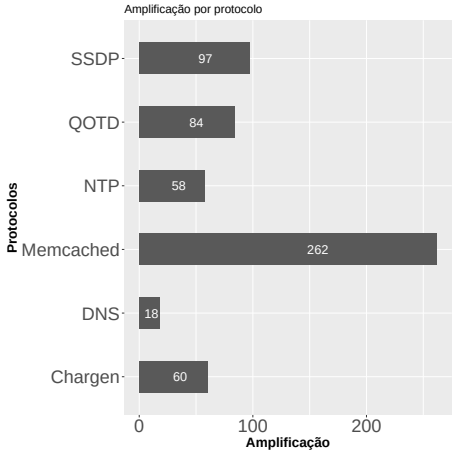


Figura 2. Amplificação por protocolo

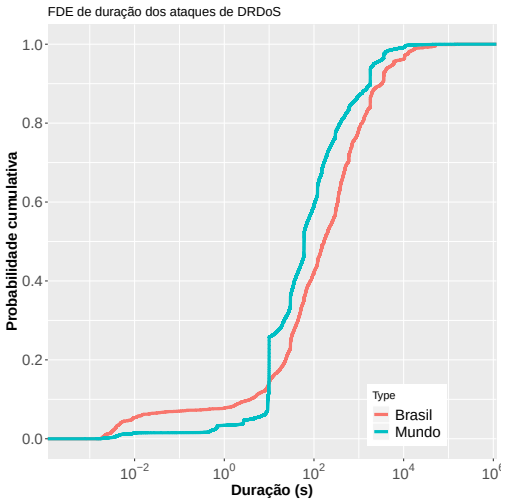


Figura 3. FDE da duração dos ataques

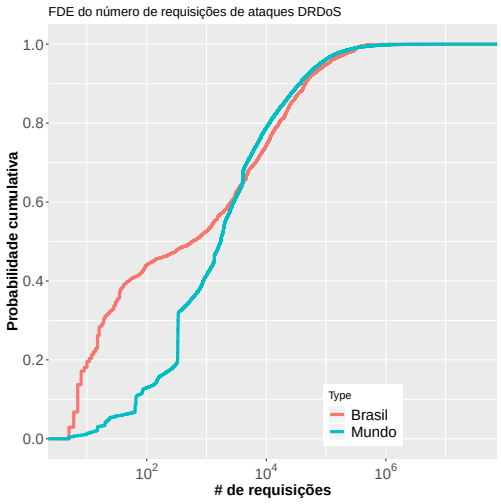


Figura 4. FDE das requisições por ataque

refletiu tráfego para 186 países, sendo EUA (46,4%) e China (6,6%) os países com maior concentração de vítimas.

A Figura 3 apresenta as funções de distribuição empírica (FDE) para a duração dos ataques. A duração é medida como a diferença de tempo entre a primeira e a última requisição em um ataque. Ambos as distribuições (Brasil e mundo) apresentam assimetria à direita. A partir do 17° percentil, os ataques a alvos brasileiros têm maior duração do que os ataques a outros países. A duração média observada foi de 1.490 s (Brasil) e 560 s (mundo). Ao todo 212 ataques no Brasil (8,9%) e 7093 no Mundo (3,5%) duraram mais do que uma hora. O maior ataque registrado no Brasil teve duração de 39,1-h (1,6 dias), enquanto que no Mundo o maior ataque teve duração de 114,2 h (4,8 dias).

A Figura 4 apresenta a FDE para o número de requisições por ataque. Até o 65º percentil, os ataques a alvos brasileiros possuem mais requisições do que os ataques a outros países; depois disso, a situação se inverte. O número médio de requisições por ataque foi similar, 19.934 (Brasil) e 20.188 (mundo). Foram observados 120 ataques para o Brasil (0,05%) com mais de 100 k requisições e 7.776 ataques no mundo (3,8%). O maior ataque para o Brasil teve 1,1 M de requisições, enquanto que o maior ataque para o resto do mundo teve 33 M de requisições. Analisando a Figura 3 em conjunto com a Figura 4, é possível apontar que os ataques contra o Brasil foram em geral mais longos do que os ataques contra o restante do mundo, mas estes tiveram a maior proporção de ataques com grande volume de requisições.

O período em que os ataques são realizados é apresentado na Figura 5, com o fuso horário de Brasília. Para o Brasil há mais ataques durante dias e horários de trabalho (entre 09h de segunda-feira e 20h de sexta-feira), com uma exceção notável nos sábados à tarde, entre 16h e 18h. Os ataques no mundo estão mais dispersos, havendo uma correlação com os ataques no Brasil em dois *slots* de tempo, segundas e terças-feiras às 05h).

A Figura 6 apresenta a FDE do número de ataques por vítima. O gráfico corrobora o observado na Seção 4.1, que o Brasil teve menos vítimas que sofreram múltiplos ataques. 68% das vítimas brasileiras e 50% das vítimas no restante do mundo sofreram

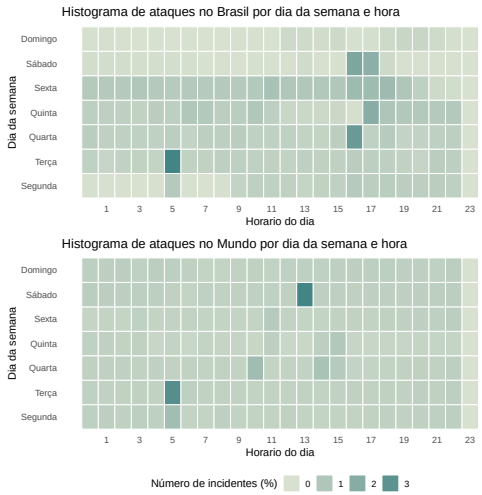


Figura 5. Incidência de ataques por dia da semana e horário

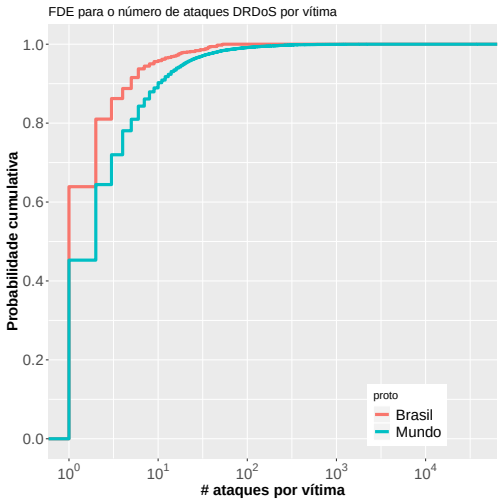


Figura 6. Número de ataques por vítima

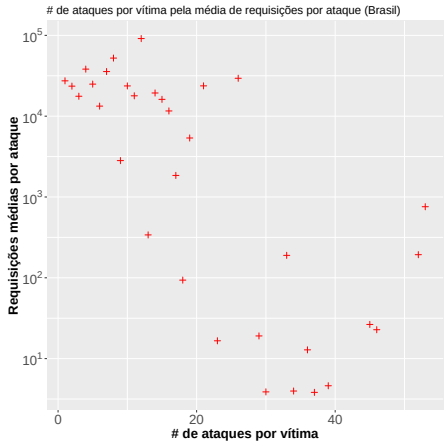


Figura 7. Número de ataques por vítima pela média de requisições por ataque para o Brasil

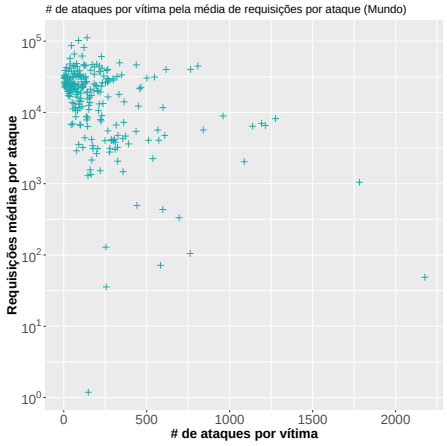


Figura 8. Número de ataques por vítima pela média de requisições por ataque para o Mundo

apenas um ataque. O número médio de ataques por vítima foi 2 (Brasil) e 8 (mundo), e o máximo foi 53 (Brasil) e 2,1 k (mundo). Para as vítimas com o valor máximo de ataques é possível destacar um valor médio de requisições baixo, com uma média de 49 (Brasil) e 758 (mundo) requisições por ataque.

As Figuras 7 e 8 mostram gráficos da média de requisições por ataque *versus* o número de ataques por vítima. As vítimas que sofreram menos ataques receberam as maiores quantidades de requisições para as vítimas que obtiveram uma menor quantidade de ataques, e há uma tendência de queda das requisições com o aumento dos ataques. Para ilustrar isso, ao avaliar todas as vítimas com mais de 45 ataques (90^o percentil para as vítimas brasileiras), tem-se uma média de requisições por ataque de 256 para o Brasil e 11,4 k para o restante do mundo, enquanto que para vítimas com até 45 ataques tem-se médias de 2 k (Brasil) e 25,9 k (mundo) requisições por ataque.

5. *Carpet Bombing*

A técnica de *carpet bombing* consiste em direcionar o tráfego para múltiplos endereços IP na mesma sub-rede, em vez de para um único endereço IP [NETSCOUT 2019]. O objetivo é saturar os enlaces de acesso das vítimas desejadas, e, ao mesmo tempo, dificultar a detecção e mitigação do ataque. Nesse caso, a detecção exige a identificação de tráfego anômalo em sub-redes inteiras em vez de identificar fluxos anômalos envolvendo um único endereço IP, enquanto a mitigação envolve desviar o tráfego das sub-redes completas para um serviço anti-DDoS.

No total foram observados 4,8 k ataques de *carpet bombing* (CB). Somente 0,05% dos ataques exploraram mais de um protocolo para realizar a amplificação de tráfego. As Figuras 9 e 10 esquematizam duas variantes típicas observadas no *honeypot*. A diferença entre elas é se os múltiplos endereços IP da sub-rede vítima são usados concomitantemente (Figura 9) ou de forma consecutiva (Figura 10), não necessariamente em ordem.

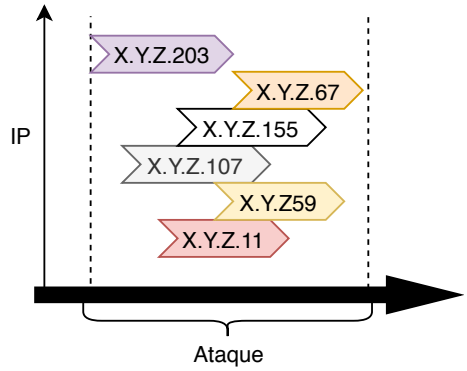


Figura 9. *Carpet bombing* com endereços IP concomitantes

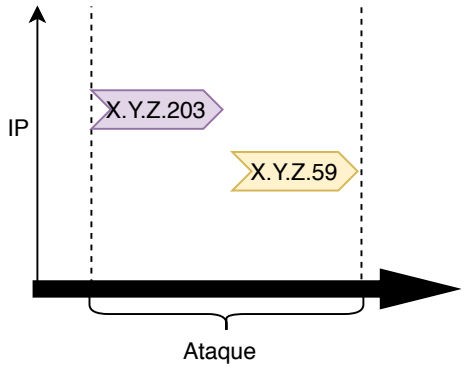


Figura 10. *Carpet bombing* com endereços IP consecutivos

A Figura 11 apresenta a FDE para a duração dos ataques CB, com médias de 52 minutos (Brasil) e 55 minutos (mundo), e máximas de 39,1 h (1,6 dias) para o Brasil e 79,7 h (3,3 dias) para o resto do mundo. As distribuições para Brasil e mundo são similares após o 10º percentil. 75% dos ataques observados têm duração de até 17 minutos (Brasil) e 30 minutos (mundo). As distribuições do número de requisições por ataque, mostradas na Figura 12, são bastante diferentes. A distribuição para o Brasil é bimodal, enquanto que a distribuição para o restante do mundo é assimétrica com cauda à direita. O número médio de requisições por ataque foi de 3,7 k (Brasil) e 76 k (mundo). O maior ataque registrado contra um alvo no Brasil teve 200 k requisições, ao passo que o maior ataque contra outros países teve 8,5 M requisições.

A Figura 13 apresenta a distribuição de ataques de acordo com os dias da semana. Ao avaliar os ataques brasileiros, é possível apontar uma maior incidência às quartas-feiras, com um destaque secundário para os finais de semana (sábado e domingo). Para os ataques no mundo a distribuição acaba apresenta dois períodos com destaque, terças às 05h e sábados às 13h. Esses dois períodos concentram 25% dos ataques, sendo que o primeiro já tinha se destacado nos ataques sem *carpet bombing* (Figura 5).

Ao considerar a fração da sub-rede que foi usada em cada ataque CB, é possível

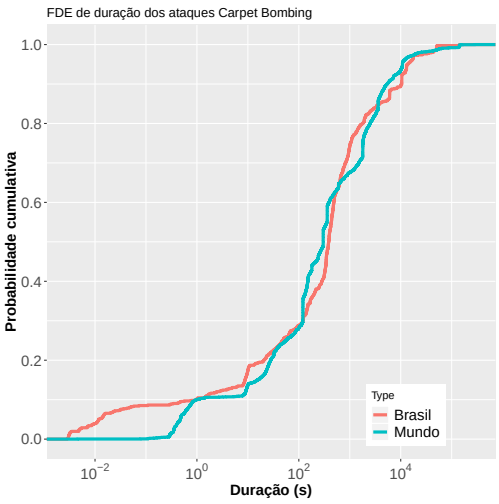


Figura 11. FDE da duração dos ataques CB

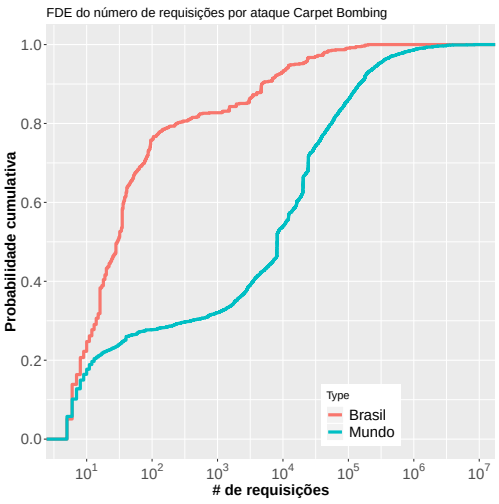


Figura 12. FDE das requisições por ataque CB

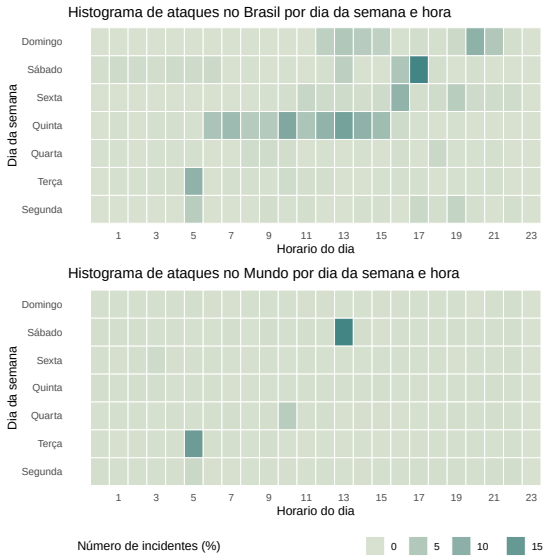


Figura 13. Incidência de ataques CB por dia da semana e horário

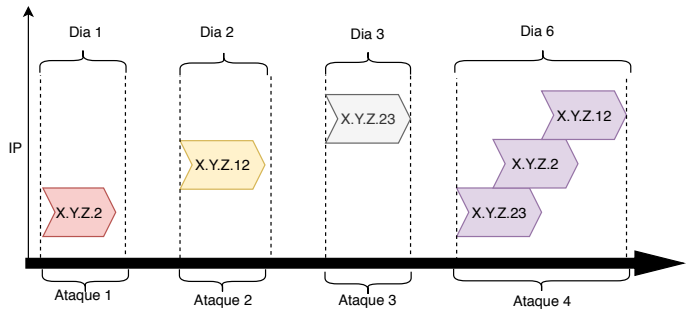


Figura 14. Ataques CB com antecedentes

identificar que 9,2% (Brasil) e 1,5% (mundo) dos ataques exploraram mais de 50% dos endereços do bloco /24. Uma ampla maioria dos ataques – 90,0% para o Brasil e 98,3% para o restante do mundo – teve cobertura de 30% ou menos da sub-rede.

A Figura 14 ilustra um tipo particular de ataque CB. Ele foi chamado de ataque com antecedentes, pois o ataque contra múltiplos endereços IP de uma sub-rede ocorre depois de alguns dias em que são observados ataques a um único endereço IP da sub-rede em cada dia. Esses ataques são considerados os antecedentes do *carpet bombing* porque, embora os endereços IP variem, as características desses ataques – protocolo (Chargen), duração, número de requisições – são parecidas entre si. No tráfego coletado pelo *honeypot*, 18,9% dos ataques *carpet bombing* observados tiveram antecedentes. Os ataques antecedentes tiveram em média um minuto de duração e 13,5 k requisições por ataque, enquanto os ataques finais tiveram em média quatro minutos de duração e 7,8 k requisições por endereço IP da sub-rede.

6. Conclusão

Ataques DRDoS são uma ameaça significativa na Internet. A facilidade de realização de ataques, a amplificação de tráfego que pode ser obtida, a disponibilidade de refletores abertos que podem ser explorados nos ataques, e a dificuldade de identificação dos seus autores são fatores que concorrem para que eles continuem acontecendo. Entender o funcionamento dos ataques DRDoS é importante para ajudar na busca de mecanismos para detectar, conter e prevenir esse tipo de ataque.

Neste estudo foi apresentada uma análise comparativa de ataques DRDoS contra vítimas no Brasil e no resto do mundo. O conjunto de dados consiste de tráfego coletado por um *honeypot* durante 190 dias. Mais de 204 k ataques DRDoS foram identificados e analisados, com diversas características sendo discutidas. No geral, é possível apontar que os ataques no Brasil estão atrás, em termos de intensidade e de *mix* de protocolos, aos observados contra vítimas em outras partes do mundo, o que indica que o cenário no país pode piorar se os atacantes se tornarem mais sofisticados e passarem a acompanhar a evolução dos ataques.

O estudo destacou uma dessas evoluções, o uso de *carpet bombing*. Foram identificados mais de 4.800 ataques desse tipo, sendo descritas e comparadas suas principais características, e introduzidos os ataques de *carpet bombing* com antecedentes.

Como trabalhos futuros, estamos dando continuidade à coleta de dados com o *honeypot* HReflector para permitir a análise da evolução dos ataques. Além disso, pretende-se

buscar parceiros de pesquisa para aumentar o número de *honeypots* e assim conseguir ampliar o escopo de nossas análises.

Agradecimentos

Os autores agradecem o apoio da UDESC e da FAPESC para a realização desta pesquisa.

Referências

Arbor (2018). Um balanço dos ataques DDoS ao Brasil no primeiro semestre deste ano. https://bit.ly/2EKEElw

CERT.br (2019a). Estatísticas de notificações de IPs e ASNs permitindo amplificação. https://www.cert.br/stats/amplificadores/.

CERT.br (2019b). Incidentes reportados ao CERT.br – janeiro a dezembro de 2018 – análise de alguns fatos de interesse observados neste período. https://www.cert.br/stats/incidentes/2018-jan-dec/analise.html.

Cymru (2019). DNS research at Team Cymru. http://dnsresearch.cymru.com/.

Czyz, J., Kallitsis, M., Gharaibeh, M., Papadopoulos, C., Bailey, M., and Karir, M. (2014). Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 435–448. ACM.

DDoSMon (2019). Insight into global DDoS threat landscape. https://ddosmon.net/insight/.

Fachkha, C., Bou-Harb, E., and Debbabi, M. (2015). Inferring distributed reflection denial of service attacks from darknet. *Computer Communications*, 62:59–71.

Heinrich, T., Longo, F. S., and Obelheiro, R. R. (2017). Experiências com um honeypot DNS: Caracterização e evolução do tráfego malicioso. In *XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*.

Jonker, M., King, A., Krupp, J., Rossow, C., Sperotto, A., and Dainotti, A. (2017). Millions of targets under attack: a macroscopic characterization of the DoS ecosystem. In *Proceedings of the 2017 Internet Measurement Conference*, pages 100–113. ACM.

Kottler, S. (2018). February 28th DDoS incident report. https://githubengineering.com/ddos-incident-report/.

Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., and Rossow, C. (2015). AmpPot: Monitoring and defending against amplification DDoS attacks. In *International Workshop on Recent Advances in Intrusion Detection*, pages 615–636. Springer.

Krupp, J., Karami, M., Rossow, C., McCoy, D., and Backes, M. (2017). Linking amplification DDoS attacks to booter services. In *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, pages 427–449.

Majkowski, M. (2018). Memcrashed – major amplification attacks from UDP port 11211. https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/.

Mansfield-Devine, S. (2015). The growth and evolution of DDoS. *Network Security*, 2015(10):13–20.

Nazario, J. (2008). DDoS attack evolution. *Network Security*, 2008(7):7–10.

NETSCOUT (2019). Dawn of the terrorbit era. Threat intelligence report 2H 2018. `https://www.netscout.com/`.

Noroozian, A., Korczyński, M., Gañan, C. H., Makita, D., Yoshioka, K., and van Eeten, M. (2016). Who gets the boot? analyzing victimization by DDoS-as-a-Service. In *International Symposium on Research in Attacks, Intrusions, and Defenses*, pages 368–389. Springer.

OpenNTP (2019). OpenNTPProject.org – NTP scanning project. `http://openntpproject.org/`.

Paxson, V. (2001). An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communication Review*, 31(3):38–47.

Rossow, C. (2014). Amplification hell: Revisiting network protocols for DDoS abuse. In *Network and Distributed System Security Symposium (NDSS)*.

Santanna, J. J., van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., and Pras, A. (2015). Booters – an analysis of DDoS-as-a-service attacks. In *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*, pages 243–251. IEEE.

Thomas, D. R., Clayton, R., and Beresford, A. R. (2017). 1000 days of UDP amplification DDoS attacks. In *APWG Symposium on Electronic Crime Research (eCrime)*, pages 79–84. IEEE.

Wang, A., Chang, W., Chen, S., and Mohaisen, A. (2018). Delving into Internet DDoS attacks by botnets: Characterization and analysis. *IEEE/ACM Trans. Netw.*, 26(6):2843–2855.

Welzel, A., Rossow, C., and Bos, H. (2014). On measuring the impact of DDoS botnets. In *Proceedings of the Seventh European Workshop on System Security*, page 3. ACM.

Zand, A., Modelo-Howard, G., Tongaonkar, A., Lee, S.-J., Kruegel, C., and Vigna, G. (2017). Demystifying DDoS as a service. *IEEE Communications Magazine*, 55(7):14–21.